Lucent Technologies
Bell Labs Innovations

APX 8000™/MAX TNT®

WAN, Routing, and Tunneling Configuration Guide

Part Number: 7820-0739-002
For software version 9.0
January 2001

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Edge Access Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

Ordering Information

You can order the most up-to-date product information and computer-based training online at `http://www.lucent.com/ins/bookstore`.

Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this manual. Please send them to `techpubs@ascend.com`.

Lucent Technologies

Customer Service

To obtain product and service information, software upgrades, and technical assistance, visit the eSight™ Service Center at `http://www.esight.com.` The center is open 24 hours a day, seven days a week.

Finding information and software

The eSight Service Center at `http://www.esight.com` provides technical information, product information, and descriptions of available services. Log in and select a service. The eSight Service Center also provides software upgrades, release notes, and addenda. Or you can visit the FTP site at `ftp://ftp.ascend.com` for this information.

Obtaining technical assistance

The eSight™ Service Center at `http://www.esight.com` provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone.

If you need to contact Lucent Technologies for assistance, make sure that you have the following information available:

- Active contract number, product name, model, and serial number
- Software version
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or eSight Live chat. Select one of these sites when you log in to `http://www.esight.com`.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information on eSight or if you have a very urgent need, contact TAC. Access the eSight Service Center at `http://www.esight.com` and click `Contact Us` below the Lucent Technologies logo for a list of telephone numbers inside and outside the United States.

You can alternatively call (800) 272-3634 for a menu of Lucent services, or call (510) 769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Contents

Chapter 6 Virtual Routers (VRouters)... 6-1

Appendix A

Appendix B Authorization Options B-1

Figures

Tables

About This Guide

What is in this guide

This guide describes how to configure an APX 8000™ and MAX TNT® for network connectivity. To use this guide, you must have already set your TAOS unit, installed the slot cards, and provisioned and tested the lines. If you have not already finished those tasks, see the hardware installation guide that came with your unit and the *APX 8000/MAX TNT Physical Interface Configuration Guide*.

Note: This manual describes the full set of features for APX 8000 and MAX TNT units running True Access™ Operating System (TAOS) software version 8.0.2 or later. Some features might not be available with earlier versions or specialty loads of the software.

This manual hereafter refers to your product as a *TAOS unit*.

Warning: Before installing your TAOS unit, be sure to read the safety instructions in the *Edge Access Safety and Compliance Guide*. For information specific to your unit, see the "Safety-Related Electrical, Physical, and Environmental Information" appendix in your unit's hardware installation guide.

What you should know

While this guide attempts to provide enough of a conceptual framework to enable an administrator who is not an expert in a particular network technology to configure the TAOS unit accurately, it does not start from the beginning with any network management topic. Following are the general areas in which it is helpful to have some existing knowledge when configuring the related network capabilities:

- Dial-in connections (both framed protocol sessions and user logins)
- Connection cost management and accounting
- Modems
- Frame Relay
- IP routing
- OSPF routing (if applicable)
- Multicast (if applicable)
- Multiprotocol routing (if applicable)
- Packet structure and formats (for defining filters)
- Network security

Documentation conventions

Following are the special characters and typographical conventions used in this manual:

Convention	**Meaning**
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
⚠ **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
⚠ **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.
⚡ **Warning:**	Warns of danger of electric shock.

Documentation set

The APX 8000/MAX TNT documentation set consists of the following manuals.

- **Read me first:**
  - *Edge Access Safety and Compliance Guide*
    Contains important safety instructions and country-specific compliance information that you must read before installing a TAOS unit.
  - *TAOS Command-Line Interface Guide*
    Introduces the TAOS command-line environment and shows how to use the command-line interface effectively. This manual describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.
- **Installation and basic configuration:**
  - *APX 8000 Hardware Installation Guide*
    Shows how to install APX 8000 hardware and includes APX 8000 technical specifications.
  - *MAX TNT Hardware Installation Guide*
    Shows how to install MAX TNT hardware and includes technical specifications for MAX TNT units.
  - *APX 8000/MAX TNT Physical Interface Configuration Guide*
    Shows how to configure the cards installed in a TAOS unit and their line attributes for such functions as framing, signaling, and channel usage. It also describes how calls are routed through the system and includes information about configuring the unit in a Signaling System 7 (SS7) environment. This guide explains shelf controller redundancy for an APX 8000 unit.
- **Configuration:**
  - *APX 8000/MAX TNT ATM Configuration Guide*
    Describes how to configure Asynchronous Transfer Mode (ATM) operations on a TAOS unit. This guide explains how to configure physical layer attributes and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) ATM interfaces. It includes information about ATM direct and ATM-Frame Relay circuits.
  - *APX 8000/MAX TNT Frame Relay Configuration Guide*
    Describes how to configure Frame Relay operations on a TAOS unit. This guide explains physical layer configuration and restrictions and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) interfaces. It includes information about Multilink Frame Relay (MFR) and link management, as well as Frame Relay and Frame Relay direct circuits.
  - *APX 8000/MAX TNT Routing and Tunneling Configuration Guide*
    Shows how to configure LAN and WAN routing for analog and digital dial-in connections on a TAOS unit. This guide includes information about IP routing, Open Shortest Path First (OSPF) routing, Internet Group Management Protocol (IGMP) routing, multiprotocol routers, Virtual Routers (VRouters), and tunneling protocols.
  - *MultiVoice™ for APX 8000/MAX TNT Configuration Guide*
    Shows how to configure the MultiVoice application to run on an APX 8000 or MAX TNT unit in both Signaling System 7 (SS7) and H.323 Voice over IP (VoIP) configurations.

- **RADIUS:** *TAOS RADIUS Guide and Reference*
  Describes how to set up a TAOS unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *APX 8000/MAX TNT Administration Guide*
  Describes how to administer a TAOS unit, including how to monitor the system and cards, troubleshoot the unit, and configure the unit to use the Simple Network Management Protocol (SNMP).
- **Reference:**
  - *APX 8000/MAX TNT Reference*
    An alphabetic reference to all commands, profiles, and parameters supported on TAOS units.
  - *TAOS Glossary*
    Defines terms used in documentation for TAOS units.

WAN Connections

1

Introduction to WAN connections

WAN connections can be established by dialing in to or out from the TAOS unit. Dial-in connections are initiated by a remote user or access router, and dial-out is initiated by the TAOS unit itself (typically for packet routing) or by a user dialing out through one of the system’s digital modems.

The far end of a WAN connection determines whether the link is synchronous or asynchronous. For example, a remote access router such as a Pipeline® unit uses a synchronous link, while an analog modem requires an asynchronous link.

A synchronous link uses HDLC encoding and connects to an access router for a network-to-network link. The call is routed as a digital call to an HDLC channel in the TAOS unit, and then to the router software. Synchronous connections use an encapsulation protocol such as Point-to-Point Protocol (PPP) or Frame Relay to deliver packets from one box to another. Synchronous connections can be multichannel.

An asynchronous link uses the kind of serial communications provided by a PC COM port, and is typically initiated by a dial-up modem or V.120 terminal adapter (TA) for a host-to-network or host-to-host connection. An asynchronous call initiated by a modem is typically routed as a voice call to a digital modem in the TAOS unit, and then to the terminal-server software. Other kinds of asynchronous calls might be routed to an HDLC channel, and from there to the terminal-server software or directly to a local host.

Types of encapsulation protocols

Encapsulation protocols enable delivery of packets from one device to another across the WAN. The TAOS unit recognizes the following encapsulation types:

- Point-to-Point Protocol (PPP)
- Multilink Protocol (MP)
- Multilink Protocol Plus (MP+ or MPP)
- Unencapsulated TCP (TCP-Clear or TCP-Raw)
- V.120
- X.75
- AppleTalk Remote Access (ARA)
- Frame-Relay, Frame-Relay-Circuit, and ATM-FR-Circuit

PPP, MP, and MP+

A PPP call uses a single channel. An MP call uses a static number of multiple channels, and can be used to communicate with any MP-compliant device. An MP+ call can add channels dynamically as needed, and can be established only between TAOS units. If you configure MP+ and the remote device does not support it, the TAOS unit attempts an MP connection. If the remote device does not support MP, the TAOS unit falls back to single-channel PPP.

Other encapsulation protocols

V.120 encapsulation is handled transparently and requires minimal configuration (for details, see “Answer-Defaults profile” on page 1-3).

AppleTalk routing and ARA connections are described in Chapter 8, “AppleTalk Routing and Remote Access.”

Frame Relay, Frame Relay circuits, and ATM-to-Frame Relay circuits are described in the *APX 8000/MAX TNT Frame Relay Configuration Guide*. For a description of an ATM connection, see the *APX 8000/MAX TNT ATM Configuration Guide*.

How the system answers and authenticates dial-in calls

When the TAOS unit receives an incoming call on one of its lines (such as a T1 line), it evaluates the call on the basis of the settings in the Answer-Defaults profile. If the call complies with the conditions in that profile, the TAOS unit answers the call, routes it to the appropriate host card (such as a modem or HDLC channel), and looks for a Connection profile or equivalent external profile to match the call’s parameters.

If it finds a local or external profile for the caller, the TAOS unit begins authentication. If it does not find a matching profile and the Answer-Defaults profile requires a profile for all callers (the default), the TAOS unit drops the call.

How the system initiates dial-out calls

When the TAOS unit receives an outbound packet destined for a remote location, it looks for a Connection profile or equivalent external profile that matches the destination address in the packet. If it finds a matching profile, it brings up the connection. This process is described in more detail in the routing chapters of this guide.

Note: To enable the TAOS unit to bring up a connection on the basis of packet routing, the profile must specify dial-out parameters, and the system must have a route that enables it to find the profile. For details, see “Configuring dial-out connections” on page 1-39.

In addition, the TAOS unit can allow users to access its 56K modems to initiate dial-out sessions. This configuration is described in “Modem dial-out connections” on page 1-43.

How the system establishes and monitors sessions

After it authenticates a call, the TAOS unit builds and maintains a session with the caller. The call’s data can be forwarded to the TAOS unit router software (for a framed-protocol session), to the terminal-server software (for an interactive login), or to a specified host, depending on the nature of the call.

The TAOS unit uses settings in the caller’s profile to monitor and, if appropriate, terminate the session. For example, it might use Idle-Timer and Call-Filter settings to terminate the session after a certain amount of idle time. (For more information, see “Specifying session time limits” on page 1-8.)

Systemwide profiles

In addition to a connection-specific profile, which specifies configuration settings and the name and password to be used in the authentication sequence, a WAN connection is also affected by the Answer-Defaults, Terminal-Server, and External-Auth profiles. The parameters in these profiles apply systemwide.

Answer-Defaults profile

The Answer-Defaults profile sets baseline values that affect all incoming calls, so you must check the Answer-Defaults values to make sure they are set properly for your site.

Answer-Defaults values are applied *before* the TAOS unit routes the call to a host card for processing, and before it locates the caller’s profile. If the caller’s profile contains a similar parameter with a different value, the TAOS unit uses the connection-specific value rather than the Answer-Defaults value to build the session.

By default, the Answer-Defaults profile enables all types of encapsulation and routing, and the basic call-setup parameters use the lowest common denominator settings. This is appropriate for many sites, but you might want to change the settings to fine-tune the criteria for accepting calls, or to constrain the amount of bandwidth accessible to multilink PPP calls.

Default RADIUS settings

When the Use-Answer-For-All-Defaults parameter is set to Yes (the default), the system creates a baseline default profile for RADIUS-authenticated calls by using the settings in the Answer-Defaults profile. It retrieves the caller’s configured profile from RADIUS and uses the attribute-value pairs in the profile. Attributes that are not specified in the profile take their values from the Answer-Defaults settings.

If Use-Answer-For-All-Defaults is set to No and a RADIUS profile does not return certain explicit values, the TAOS unit uses factory default values for RADIUS attributes instead.

Requiring authentication for PPP calls

The following Answer-Default parameters (shown with default values) affect authentication:

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

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

By default, no Calling Line ID (CLID), Dial Number Information Service (DNIS), or PPP authentication is required for incoming calls. Most sites change the Receive-Auth-Mode default, as shown in the following example, to ensure authentication of a PPP call before a session is established:

```
admin> read answer
ANSWER-DEFAULTS read

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

admin> write
ANSWER-DEFAULTS written
```

When you specify Any-PPP-Auth as the method of PPP authentication, the TAOS unit accepts incoming PPP calls that support any of the authentication methods, but it drops connections that do not offer any authentication protocols during Link Control Protocol (LCP) negotiation. For more details about PPP, CLID, and DNIS authentication, see Appendix A, “Authentication Methods.”

V.120 settings

V.120 terminal adapters (also known as ISDN modems) are asynchronous devices that use ITU-T V.120 encapsulation. After the system processes the call’s V.120 encapsulation, it forwards the call to the terminal server. Following are the Answer-Defaults parameters related to V.120 connections. The settings shown are the defaults.

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

By default, the system can answer V.120 calls. Frame-Length specifies the V.120 maximum transmit and receive frame sizes. The value should correspond to the settings in the TA software. For V.120 operation that is compatible with TAOS units, use the following terminal adapter settings (refer to the manual for the V.120 device for information about how to enter them).

- V.120 maximum transmit frame size—260 bytes
- V.120 maximum receive frame size—260 bytes
- Logical link ID (LLI)—256
- Modulo—128
- Line channel speed—Select 56K if the TAOS unit accepts calls from the V.120 device on a T1 line, or if you are not sure that you have 64-Kbps channel speed end-to-end.

- Call placement—The TAOS unit can receive V.120 calls, but cannot place them.

The following set of commands configures V.120 calls with a maximum frame size of 260 bytes:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set v120 frame-length = 260

admin> write
ANSWER-DEFAULTS written
```

Note: If the user's dial-in software supports async-to-sync conversion, the Connection profile can be set for PAP or CHAP authentication, and the user can access the terminal server by PPP automatic login. For recommended authentication settings for connections using terminal adapters, see Appendix A, "Authentication Methods."

Terminal-Server profile

The TAOS unit terminal-server software receives asynchronous calls after they have been processed by a digital modem. Such calls are typically dialed in by a modem or V.120 TA. If the caller does not send PPP packets immediately, the terminal server starts a login sequence.

For an asynchronous PPP call, the terminal server forwards the call to the router software as soon as it detects a PPP packet. For information about configuring asynchronous PPP calls, see "Example of an asynchronous PPP connection" on page 1-14.

For a login session, each user must have a Connection profile (or external profile) that specifies a name and password to be used in the terminal-server login sequence. In addition, a global Terminal-Server profile defines how these calls are authenticated and where the call is directed after authentication. For information about both of these subjects, see Appendix A, "Authentication Methods."

You must enable the terminal-server software if the TAOS unit is to handle asynchronous calls. Following is the related parameter with its default setting:

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

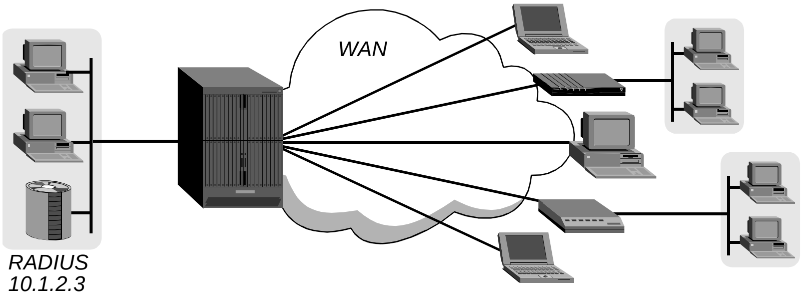
The following set of commands enables the terminal-server software:

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

admin> set enabled = yes

admin> write
TERMINAL-SERVER written
```

External-Auth profile

For external authentication and accounting, the TAOS unit supports RADIUS, Terminal Access Control Access System (TACACS) protocol, and TACACS+. In Figure 1-1, the TAOS unit answers incoming calls and forwards authentication requests to a RADIUS server on a LAN interface:

Figure 1-1. RADIUS server on a LAN interface



The following commands configure the TAOS unit to access the RADIUS authentication server at 10.1.2.3 on UDP port 5000, using the shared-secret `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
```

The following commands configure a TAOS unit to access the RADIUS accounting server at 10.1.2.3 on UDP port 512, using the shared-secret `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
```

Local and external authentication profiles

You can define WAN connections locally in Connection profiles or on a RADIUS server in user profiles. The examples in this guide show both configuration methods.

Using Connection profiles

A Connection profile contains all connection-specific information, including authentication settings, compression values, filter specifications, and telco options. To create a new Connection profile, use the following command:

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

Sharing profiles on a per-user basis

You can enable shared profiles on a per-connection basis even though they have been disallowed systemwide. In previous software releases, this functionality was only available in RADIUS profiles through the Ascend-Shared-Profile-Enable attribute. Following is the relevant parameter, shown with its default setting:

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

Parameter	Description
Shared-Prof	Enable/disable multiple callers to share the Connection profile, provided that IP address conflicts do not result. With the default setting of `no`, the setting of the Shared-Prof parameter in the IP-Global profile allows or disallows shared profiles systemwide.

If the Shared-Prof parameter is set to `yes` in the IP-Global profile, the Shared-Prof setting in a Connection profile has no effect. However, if the Shared-Prof parameter is set to `no` in the IP-Global profile and `yes` in a Connection profile, the setting in the Connection profile takes precedence. For example, with the following settings, multiple callers can call in and authenticate the Connection profile named `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
```

Using RADIUS

You can use RADIUS to externally authenticate calls answered by the TAOS unit. External authentication centralizes the management of WAN connections and concentrates user profiles into a single text file. The use of RADIUS also enables token-card authentication for secure networks, or authentication based on a UNIX password database.

RADIUS profiles are composed of the following three parts:

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

The User-Name must be left justified. It is typically the name of the caller (or calling device), but it can also be a telephone number (for CLID or DNIS authentication), a special string indicating a pseudo-user profile, or the string `DEFAULT` (for the default user profile).

Check-Items must be on the same line as the User-Name, and must be separated by white space (space or tab) from the User-Name. Check-Items includes zero or more attribute-value pairs that must match the attributes that are present in the Access-Request packet for the user to be authenticated. Check-Items typically include the password for the entry.

Reply-Items must be indented and separated from the User-Name and Check-Items by a new line. (If a Reply-Item is not indented, it is interpreted as the User-Name of a new entry.) Reply-Items includes zero or more attribute-value pairs that are returned in Access-Accept messages to authorize services for the user.

Specifying session time limits

Once the TAOS unit has answered a call and established a WAN session, it uses settings in a Connection profile or RADIUS profile to apply filters or firewalls to the session's data stream and to time out the session if it becomes inactive for a specified time period.

Time-limit settings in a Connection profile

Following are the relevant parameters for specifying session time limits in a Connection profile. The settings shown are the defaults.

```
[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
```

Parameter	**Specifies**
Call-Filter or Data-Filter	Name of a filter or firewall to apply to the connection. For details, see Chapter 9, “Packet Filters.”
Filter-Persistence	Enable/disable filter persistence across connection state changes.
Idle-Timer	Number of seconds a packetized network session can remain idle before it is terminated. The default value is 120.
TS-Idle-Mode	Direction in which active traffic is monitored during a session (Input-Only, Input-Output, or None).
TS-Idle-Timer	Number of seconds a login session can remain idle before it is terminated. The default value is 120.
Max-Call-Duration	For single-channel sessions, the maximum number of minutes a call can stay connected. For MP+ sessions, the maximum number of minutes a single call within the session can stay connected. (Each call in the bundle has a limited duration, but the session can last indefinitely as calls change status.)

Time-limit settings in a RADIUS profile

RADIUS uses the following attribute-value pairs for setting session time limits:

RADIUS Attribute	Value
Filter-ID (11)	Name of a local Filter profile that defines a data filter. The next time a TAOS unit accesses the RADIUS user profile in which this attribute appears, the referenced data filter is applied to the connection. For details, see Chapter 9, “Packet Filters.”
Idle-Timeout (28)	Maximum number of consecutive seconds of idle time allowed the user before termination of the session or prompt. This standard RADIUS attribute is very similar to the Ascend-Idle-Limit (244) vendor attribute, and TAOS units support the use of the RFC-defined attributes. The Ascend vendor attributes will be deprecated over time in favor of RFC-defined attributes.
Session-Timeout (27)	Maximum number of seconds of service to be provided to the user before termination of the session or prompt. This standard RADIUS attribute is very similar to the Ascend-Maximum-Time (194) vendor attribute, and TAOS units support the use of the RFC-defined attributes. The Ascend vendor attributes will be deprecated over time in favor of RFC-defined attributes.
Ascend-TS-Idle-Mode (170)	Direction in which active traffic is monitored during a session (TS-Idle-Input, TS-Idle-Input-Output, or TS-Idle-None).
Ascend-TS-Idle-Limit (169)	Number of seconds a login session can remain idle before it is terminated (120 by default).
Ascend-Maximum-Call-Duration (125)	For single-channel sessions, the maximum number of minutes a call can stay connected. For MP+ sessions, the maximum number of minutes a single call within the session can stay connected. (Each call in the bundle has a limited duration, but the session can last indefinitely as calls change status.)

Example of setting time limits

The following set of commands sets the idle timer to 60 seconds and specifies that only input characters reset the timer. In addition, it limits the duration of any login session to 2 hours.

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

admin> set active = yes

admin> set encaps = tcp-raw

admin> set ppp recv-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
```

Following are comparable settings in a RADIUS profile:

```
smith Password = “xyzzy”
   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
```

Using session accounting

Both RADIUS and TACACS+ enable administrators to keep track of connection statistics, usually for billing purposes. For details on session accounting attributes, see the *APX 8000/MAX TNT Reference*.

Specifying data and transmit rates in RADIUS

The Ascend-Data-Rate attribute specifies the receive rate of the connection in bits per second. The Ascend-Xmit-Rate attribute specifies the transmit rate for the connection. The Ascend-Data-Rate and Ascend-Xmit-Rate RADIUS attributes are part of an Access Request packet and can be used to provide troubleshooting information for the user.

The information that these attributes contain is sent only if you do not authenticate with CLID or DNIS. RADIUS uses the following attribute-value pairs for setting data receive rates and data transmit rates:

RADIUS attribute	Value
Ascend-Data-Rate (197)	Specifies the receive rate of the connection in bits per second. This attribute appears in Accounting-Request packets to provide troubleshooting information for the user. The TAOS unit includes Ascend-Data-Rate in an Accounting-Request packet when both of the following conditions are true: • The session has ended or has failed to authenticate because Acct-Status-Type is set to Stop. • The Auth-Type parameter is not set to `RADIUS/LOGOUT`.

RADIUS attribute	Value
Ascend-Xmit-Rate (255)	Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate specifies the transmit data rate. For analog calls, it specifies the modem baud rate at the time of the initial connection. Ascend-Xmit-Rate does not appear in a user profile. Its default value is 0 (zero). This attribute appears in Accounting-Request packets to provide troubleshooting information for the user. The TAOS unit sends the Ascend-Xmit-Rate attribute in Accounting-Request packets at the end of a session under the following two conditions (whether the unit authenticates the connection or not): • The Accounting-Request packet has Acct-Status-Type set to Stop. • The Auth-Type parameter is set to a value other than `RADIUS/LOGOUT`.

Configuring switched dial-in connections

A switched dial-in connection is a temporary WAN connection brought up by a remote device dialing into a TAOS unit. It is the most common type of WAN connection, and can be configured in a local Connection profile or in RADIUS. The following subsections contain examples of both types of configuration.

Note: For details about dial-ins that use Frame Relay, see the *APX 8000/MAX TNT Frame Relay Configuration Guide*.

Single-channel PPP connections

A single-channel PPP dial-in can be initiated by an asynchronous device, such as an analog modem, or by a synchronous network device, such as a Pipeline. For connections requiring more then 56Kbps bandwidth, see “Multilink Protocol (MP) connections” on page 1-15 or “Multilink Protocol Plus (MP+) connections” on page 1-18.

Settings in a Connection profile

To configure a single-channel PPP dial-in connection in a Connection profile, use the following parameters (shown with default settings):

```
[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
```

Parameter	Specifies
Station	Name of the caller. The value is case sensitive, and must exactly match the name the remote device presents during authentication.
Encapsulation-Protocol	Encapsulation protocol. Set to PPP for single-channel Point-to-Point Protocol.
Recv-Password	Password expected from the caller.
Link-Compression	Link-compression method to use. For details, see “Link-compression methods” on page 1-12.
MRU	Maximum number of bytes the TAOS unit can receive in a single packet (from 1 to 1524, default 1524).
LQM	Enable/disable the Link Quality Monitoring (LQM) Protocol.
LQM-Minimum-Period LQM-Maximum-Period	Maximum and minimum period for generating Link-Quality-Report packets.

Settings in a RADIUS profile

RADIUS uses the following attribute-value pairs for PPP connections:

RADIUS attribute	Value
Password (2)	Password expected from the caller for a dial-in connection.
Service-Type (6)	Type of services the link can use. Set to Framed for dial-in PPP connections that do not use a terminal-server login, or set to Login for asynchronous PPP connections. If not specified, the service type is unrestricted.
Framed-Protocol (7)	Encapsulation protocol. Set to PPP (1) to enable a user to dial in with PPP framing or dial in unframed and then change to PPP framing.
Framed-MTU (12)	Maximum number of bytes the TAOS unit can send in a single packet (from 1 to 1524, default 1524).
Ascend-Link-Compression (233)	Link-compression method to use. For details, see “Link-compression methods” on page 1-12.

Password authentication

For details about password authentication for PPP, MP, and MP+ connections, see Appendix A, “Authentication Methods.”

Link-compression methods

The link-compression setting in a Connection or RADIUS profile specifies a compression method to use for PPP-encapsulated packets transmitted and received on the connection. During the negotiation phase of the connection, both sides must agree to use the specified method. TAOS units support the following types of PPP link compression:

- Stac compression uses a modified version of draft 0 of the CCP Protocol, which predates RFC 1974. Older Ascend equipment supports this compression method. This method is not recommended for use with IPX connections. In a Connection profile, the setting is Stac. In a RADIUS profile, it is Link-Comp-Stac (1).
- Stac-9 compression uses draft 9 of the Stac LZS compression protocol, which is described in RFC 1974. Most devices, especially recent equipment, use this compression method. In a Connection profile, the setting is Stac-9. In a RADIUS profile, it is Link-Comp-Stac-Draft-9 (2).
- MS-Stac (Microsoft/Stac) compression is the method used by Windows95. Use this method for connections with Windows95 clients. In a Connection profile, the setting is MS-Stac. In a RADIUS profile, it is Link-Comp-MS-Stac (3).

Link Quality Monitoring (LQM)

Link Quality Monitoring (LQM) is the process of monitoring data loss on a point-to-point link (see RFC 1989, *PPP Link Quality Monitoring*). When you enable LQM in a Connection profile, the TAOS unit maintains counts of the number of packets transmitted and successfully received, and periodically transmits this information to the far-end device in a Link-Quality-Report packet. The following set of commands enables LQM for a connection, using the default six-second period for generating Link-Quality-Report packets:

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

admin> set ppp lqm = yes

admin> write
CONNECTION/test written
```

Nailed connections that use PPP encapsulation and Link Quality Monitoring (LQM) include magic number support to detect looped-back links and other data link layer anomalies. When the system detects anomalies, it disconnects the link.

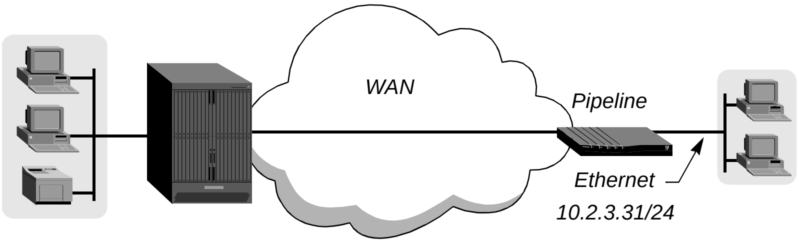
When LQM is enabled, the system selects a random number and negotiates that number with the far-end device during LCP negotiation of the link. If the far-end device does not negotiate magic numbers, the magic-number field in transmitted packets is set to zero. If the number is successfully negotiated, the local magic-number field is set to the selected random number. The WANDisplay command on an HDLC card shows information about LQM magic number negotiations, and the periodic LQM reports show the assigned local and remote magic numbers.

TAOS units inspect the magic-number field in received packets and process a packet normally if the field is equal to zero or the peer's unique magic number. If the magic-number field is equal to the local magic number, indicating a loopback link, the unit terminates the link.

Example of a synchronous PPP connection

In Figure 1-2, the caller is a Pipeline unit with the IP address 10.2.3.31/24.

Figure 1-2. Synchronous PPP connection



The following commands create the caller's Connection profile:

```
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
```

Following is a comparable RADIUS profile:

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

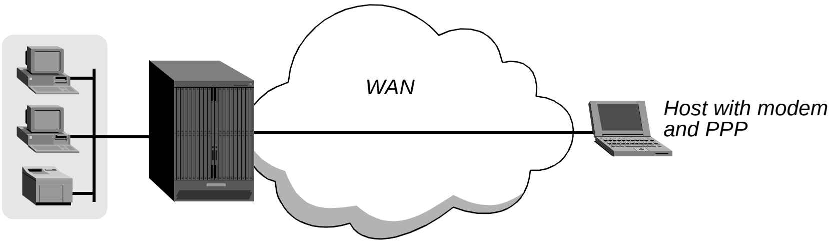
For details about enabling the TAOS unit to route packets to the Pipeline by dialing out to that destination, see “Configuring dial-out connections” on page 1-39.

Example of an asynchronous PPP connection

Asynchronous connections are authenticated first by the terminal-server software, so you must enable the terminal server to allow these connections. For details, see “Terminal-Server profile” on page 1-5. For information about terminal-server authentication, see Appendix A, “Authentication Methods.”

In Figure 1-3, the calling device is a modem, so the connection is asynchronous.

Figure 1-3. Asynchronous PPP connection



The following commands create the caller's Connection profile:

```
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
```

Following is a comparable RADIUS profile:

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

Multilink Protocol (MP) connections

Multilink Protocol (MP) uses the encapsulation defined in RFC 1990. MP enables the caller to use a static number of channels. Both sides of the connection must support MP encapsulation.

PPP Answer-Defaults and Connection profile settings also apply to MP connections. If you configure an MP connection and the TAOS unit cannot successfully negotiate the connection, it falls back to single-channel PPP (for additional information, see “Configuring dial-out connections” on page 1-39).

Note: For optimum performance, both sides of a connection should set the Base-Channel-Count parameter to the same value.

Settings in a Connection profile

Following are the parameters related to dial-in MP connections. The settings shown are the defaults.

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

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

Parameter	Specifies
Encapsulation-Protocol	Encapsulation protocol. Set to MP for Multilink Protocol connections.
Base-Channel-Count	Base number of channels to use for a multilink PPP connection. When a call is received, the TAOS unit authenticates the first (base) channels of the call and then determines the maximum and minimum settings.

Parameter	Specifies
Minimum-Channels	Minimum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.
Maximum-Channels	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.

Settings in a RADIUS profile

RADIUS uses the following attribute-value pairs for dial-in MP connections:

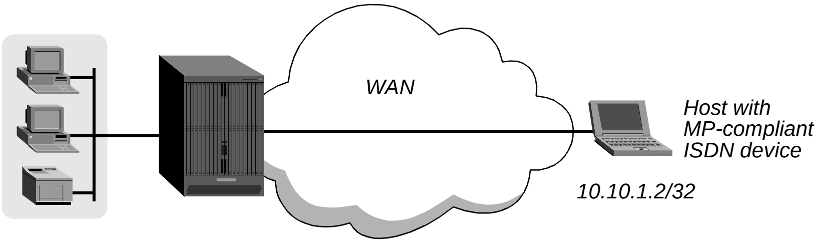
RADIUS attribute	Value
Framed-Protocol (7)	Encapsulation protocol. MP (262) indicates Multilink Protocol.
Ascend-Base-Channel-Count (172)	Base number of channels to use for a multilink PPP connection. When a call is received, the TAOS unit authenticates the first (base) channels of the call and then determines the maximum and minimum settings.
Ascend-Minimum-Channels (173)	Minimum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.
Ascend-Maximum-Channels (235)	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.

Note: If a RADIUS profile does not specify Ascend-Maximum-Channels, the default value of 1 prevents the client from establishing a multichannel call.

Examples of an MP connection

The MP connection shown in Figure 1-4 is allocated two channels.

Figure 1-4. Multilink Protocol (MP) connection



Following are the commands entered to configure a local profile, and the system’s responses:

```
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
```

Following is a comparable RADIUS profile:

```
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
```

MP bonding of analog calls

MP also operates on modem cards to bond multiple channels for analog calls. This feature enables a client with two modems to connect to the TAOS unit at a speed that is the aggregate speed of both connections. For example, a Windows NT 4.0 system with two 56Kbps modems, and Dial Up Networking (DUN) configured to use multiple lines, can set both modems to dial in to a TAOS unit.

Note: Some client modems and software packages have compatibility problems with MP channel bonding.

To enable MP bonding of analog calls, specify a standard MP connection. For example:

```
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 recv-password = localpw

admin> set mp base-channel-count = 2

admin> write
CONNECTION/baskar written
```

Or, in a RADIUS profile:

```
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
```

The first 56Kbps modem call negotiates the MP connection, and the second modem call is bundled with the first. The TAOS unit reports a single MP user with a 128Kbps connection.

Multilink Protocol Plus (MP+) connections

Multilink Protocol Plus (MP+) uses PPP encapsulation with TAOS extensions, as described in RFC 1934. MP+ enables a TAOS unit to monitor traffic on a connection with another TAOS unit and add or subtract bandwidth on demand. The criteria for adding or dropping bandwidth are part of the TAOS extensions, and are supported only by Lucent Technologies equipment.

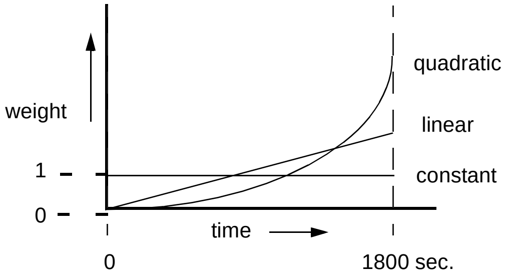
On MP+ connections, the side that makes the first call makes all subsequent calls to add bandwidth. If a remote user or access router dials in, all calls dialed to add channels are also dialed in. If the TAOS unit initiates the first call, all calls to add channels are dialed out.

PPP and MP Answer-Defaults and Connection profile settings also apply to MP+ connections. To specify the base channels of an MP+ connection, you must configure the MP-Options subprofile (as described in “Multilink Protocol (MP) connections” on page 1-15).

How TAOS units add bandwidth

Dynamic bandwidth allocation (DBA) enables a TAOS unit to add bandwidth on demand by establishing additional connections and inverse multiplexing them into the call. DBA uses one of several possible weighting algorithms to determine when to add or subtract bandwidth. The default weighting algorithm (quadratic) gives more weight to recent utilization samples than to older samples, with the weighting increasing at a quadratic rate. Linear allows the weighting to increase at a linear rate, and Constant gives equal weight to all utilization samples. Figure 1-5 is a graphical representation of the three algorithms.

Figure 1-5. Weighting line utilization samples



For information about configuring per-channel add-on numbers that enable a TAOS unit to add bandwidth on demand, see the *APX 8000/MAX TNT Physical Interface Configuration Guide*. You can add channels one at a time or, if the TAOS unit is configured for parallel dialing, in multiples. To configure the unit for parallel dialing, set the Parallel-Dialing parameter in the System profile. For example, the following command shows that Parallel-Dialing is set to 2 (the default), which enables two concurrent dial-out calls:

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

A TAOS unit can reject the request to add bandwidth if there are no more channels available at one or both ends, or if the network is congested. Under either of those conditions, the two ends enter bandwidth-addition-lockout mode, in which neither side can request bandwidth. The local restriction prevents both ends from continuing with futile attempts to add new channels. The TAOS unit and the TAOS unit at the other end of the connection automatically remove the lockout restriction when the condition that caused the lockout changes. Changes typically result from addition of a new switched-service line, reconfiguration of the line’s profile, or a switched-service congestion timeout. Once the lockout is removed, either end is free to add bandwidth.

ALU spikes

The values for Seconds-History, Add-Persistence, and Sub-Persistence should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity. Over T1 lines, the TAOS unit can add bandwidth in less than ten seconds. Over ISDN lines, the unit can add bandwidth in less than five seconds.

Telco charges

When the TAOS unit adds bandwidth, it typically incurs a minimum usage charge, after which billing is time-sensitive. The Sub-Persistence value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds.

Adding or subtracting channels too quickly (less than 10-20 seconds apart) leads to many short duration calls, each of which incurs the carrier’s minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, because the devices on either end have to retransmit data when the link speed changes.

Settings in a Connection profile

Following are the Connection profile parameters related to dial-in MP+ connections. The settings shown are the defaults.

```
[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
```

Parameter	Specifies
Encapsulation-Protocol	Encapsulation protocol. MP+ (the default) specifies Multilink Protocol Plus. The far end must be a TAOS unit.
Aux-Send-Password	Password the TAOS unit sends when it adds channels to an MP+ call that uses PAP-Token-CHAP authentication. For details, see “Token-card authentication” on page A-25.
Dynamic-Algorithm	Algorithm for calculating average line utilization (ALU) over a certain number of seconds (Seconds-History). For details, see “How TAOS units add bandwidth” on page 1-18.

Parameter	Specifies
Bandwidth-Monitor-Direction	Direction in which criteria apply, that is, whether criteria for adding or dropping links apply to traffic received across the link, transmitted across the link, or both. If both sides of the link have Bandwidth-Monitor-Direction set to None, DBA is disabled.
Increment-Channel-Count	Number of channels the TAOS unit can add at one time, subject to the setting of the Parallel-Dialing parameter in the System profile.
Decrement-Channel-Count	Number of channels the TAOS unit can subtract at one time, dropping the newest channels first.
Seconds-History	Number of seconds to use as the basis for calculating average line utilization (ALU).
Add-Persistence	Number of seconds for which ALU must persist beyond the Target-Utilization threshold before the TAOS unit adds bandwidth.
Sub-Persistence	Number of seconds for which the ALU must persist below the Target-Utilization threshold before the unit subtracts bandwidth.
Target-Utilization	Percentage of line utilization (default 70%) to use as a threshold when determining when to add or subtract bandwidth.

Settings in a RADIUS profile

A RADIUS user profile can specify the following attributes for configuring a dial-in MP+ connection's PPP options, in addition to the PPP attributes described in "Single-channel PPP connections" on page 1-11 and the MP parameters described in "Multilink Protocol (MP) connections" on page 1-15:

RADIUS attribute	Value
Framed-Protocol (7)	Encapsulation protocol. MPP (256) indicates an MP+ connection with another TAOS unit.
Ascend-History-Weigh-Type (239)	Algorithm for calculating average line utilization (ALU) over a certain number of seconds. For details, see "How TAOS units add bandwidth" on page 1-18.
Ascend-DBA-Monitor (171)	Criteria for adding or subtracting bandwidth from the connection. You can specify DBA-Transmit (0), DBA-Transmit-Recv (1), or DBA-None (3). If both sides of the link have Bandwidth-Monitor-Direction set to None, DBA is disabled.
Ascend-Inc-Channel-Count (236)	Number of channels the TAOS unit can add at one time, subject to the setting of the Parallel-Dialing parameter in the System profile.
Ascend-Dec-Channel-Count (237)	Number of channels the TAOS unit can subtract at one time, dropping the newest channels first.
Ascend-Seconds-Of-History (238)	Number of seconds to use as the basis for calculating average line utilization (ALU).
Ascend-Add-Seconds (240)	Number of seconds for which ALU must persist beyond the Target-Utilization threshold before the TAOS unit adds bandwidth.
Ascend-Remove-Seconds (241)	Number of seconds for which the ALU must persist below the Target-Utilization threshold before the unit subtracts bandwidth.

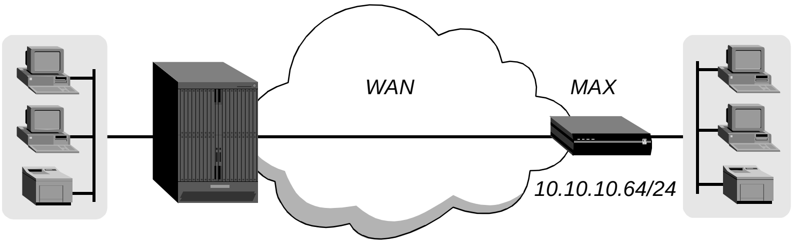
RADIUS attribute	Value
Ascend-Target-Util (234)	Percentage of line utilization (default 70%) to use as a threshold when determining when to add or subtract bandwidth.
Ascend-Maximum-Channels (235)	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.

Note: If a RADIUS profile does not specify Ascend-Maximum-Channels, the default value of 1 prevents the client from establishing a multichannel call.

Example of an MP+ configuration

In Figure 1-6, both TAOS units specify MP+ encapsulation.

Figure 1-6. Multilink Protocol Plus (MP+) connection



The following commands create a Connection profile for the far-end MAX™ unit:

```
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 recv-password = localpw

admin> set mp base-channel-count = 2

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

admin> set mpp seconds-history = 30

admin> set mpp add-persistence = 10

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

Following is a comparable RADIUS profile:

```
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
```

Note: The RADIUS profile must specify Ascend-Maximum-Channels, or the default value of 1 prevents the client from establishing a multichannel call.

Bandwidth Allocation Control Protocol (BACP)

TAOS units support BACP for PPP Multilink Protocol (MP) connections. MP is described in RFC 1990. BACP is described in RFC 2125. BACP provides dynamic bandwidth allocation based on a utilization threshold, using criteria that are very similar to those used by the bandwidth-on-demand feature in Multilink Protocol Plus (MP+). BACP can be used with digital or analog links.

For dynamic bandwidth allocation to work on an MP connection, both sides of the connection must support BACP. The following parameters (shown with sample settings) enable BACP:

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

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

Parameter	Specifies
BACP-Enable	Enable/disable BACP for MP connections. BACP is disabled by default. In the Answer-Defaults profile, the `yes` setting enables the system to accept an MP call that requests BACP bandwidth management. In a Connection profile, the `yes` setting enables a specific connection to use BACP bandwidth management.

BACP shares the parameters used by MP+ to specify criteria for adding or subtracting bandwidth. Following are the relevant parameters, shown with default settings:

```
[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
```

Details about each parameter are provided in the *APX 8000/MAX TNT Reference*. Following is an example of configuring the system to enable BACP and configuring an MP connection that uses 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
```

TCP-Clear connections

TAOS units do not process packet encapsulation for TCP-Clear connections. These connections often use a proprietary encapsulation method, or encapsulation performed by an application running on top of TCP. The TAOS unit redirects the connection's data immediately to a specified host, where encapsulation processing is assumed to occur.

You can configure TCP-Clear for a specific connection, as described in this section. Or, you can enable it globally in the Terminal-Server profile by using TCP service in *immediate mode*, as described in "Authorizing immediate-mode login service" on page B-2.

Performance enhancements for TCP-Clear calls (local profiles only)

TCP-Clear dial-in sessions that do not require V.120 processing can be buffered and transmitted as TCP packets rather than as continuous data streams, thereby increasing performance. In addition, unless V.120 processing is required, TCP-Clear WAN data is sent directly to the HDLC interface rather than to the terminal-server subsystem. The system does not collect session statistics for TCP-Clear calls that make use of these performance enhancements. If a session requires V.120 processing, the terminal server processes the call.

Settings in a Connection profile

Following are the Connection profile parameters related to dial-in TCP-Clear connections. The settings shown are the defaults.

```
[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 = “”
flush-length = 256
flush-time = 20
```

Parameter	Specifies
Encapsulation-Protocol	Encapsulation protocol. Set to TCP-Raw for a TCP-Clear connection.
Recv-Password	Password expected from the caller.
Host or Host*N*	DNS names or IP addresses of up to four hosts. If the TCP connection to the first specified host/port combination fails while the TCP-Clear session is being established, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.
Port or Port*N*	Destination TCP port on the named host. A port number of zero (the default) means any port.
Detect-End-of-Packet	Enable/disable packet buffering of incoming data. With a setting of Yes, the TAOS unit begins buffering incoming data as soon as the dial-up session has been authenticated. It continues buffering until it receives the specified End-of-Packet-Pattern, or until it reaches the specified timeout (Flush-Time) or maximum packet length (Flush-Length), whichever comes first. If Detect-End-of-Packet is set to No (the default), none of the related parameters apply.
End-of-Packet-Pattern	Character pattern that signals the end of a packet. When the TAOS unit finds this pattern in the buffered data, it immediately flushes the buffer by writing all data, up to and including the pattern, out to TCP. Note that the data is written before a match occurs if the specified timeout (Flush-Time) or maximum packet length (Flush-Length) is exceeded.
Flush-Length	Maximum number of bytes to buffer. Valid values are from 1 to 8192. The default value is 256. (Note that buffering large packets consumes more system resources.) If the system has buffered the specified number of bytes without matching the End-of-Packet-Pattern, it flushes the buffer by writing the data to TCP.
Flush-Time	Timer in milliseconds. Valid values are from 1 to 1000. The timer begins counting down upon reception of the first byte of buffered data. If the specified number of milliseconds has elapsed without the End-of-Packet-Pattern being matched, the system flushes the buffer by writing the data to TCP.

The character pattern you specify as the value of the End-of-Packet-Pattern parameter can be up to 64 characters long. It can contain both ASCII characters and binary data. To specify a binary value, use the backslash (\) as an escape mechanism. To insert a literal backslash in the pattern, escape it by entering two backslash characters (\\).

To insert a one- to three-digit octal number, escape the value by preceding it with a single backslash. (To avoid confusion between the literal ASCII characters 0 through 7 and an octal value, you can pad the octal value with leading zeros.)

For example, the following pattern represents a carriage return (octal 15):

```
\015
```

To insert a one- or two-digit hexadecimal number in the pattern, precede the number with \x. For example, the following pattern represents a carriage return (hex 0D):

```
\x0D
```

Other escape sequences are as follows:

Escape sequence	Description	Value
`\a`	Alarm	7
`\b`	Backspace	8
`\f`	Form feed	12
`\n`	New line	10
`\r`	Carriage return	13
`\t`	Tab	9
`\v`	Vertical tab	11
`\\`	Backslash	92
`\′`	Apostrophe	44
`\"`	Double quote	34
`\?`	Wildcard	Matches any single character

Settings in a RADIUS profile

A RADIUS profile can include up to four Login-IP-Host attribute settings and four Login-TCP-Port attribute settings. A TAOS unit validates the number of these settings in an Access-Accept packet returned by RADIUS. If it finds more than four, the unit logs an error in RADIF debug output and processes only the first four.

While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the unit attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.

Following are the RADIUS profile attributes related to TCP-Clear:

RADIUS Attribute	Value
Login-Service (15)	Type of login service allowed to the caller. Set to TCP-Clear (2). To suppress status messages on a per-user basis while the session is being established, set to TCP-Clear-Quiet (256).
Login-IP-Host (14)	IP address of a TCP login host.
Login-TCP-Port (16)	Destination TCP port on the specified login host (an integer from 1 to 65535). The default is 23.
Service-Type (6)	Type of service the link can use. Specify Framed or Unframed.

Examples of a TCP-Clear connection

The following set of commands specifies a TCP-Clear connection to a host Sparky on TCP port 23, or a host named Boom on TCP port 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 = sparky

admin> set tcp port = 23

admin> set tcp host1 = boom

admin> set tcp port1 = 125

admin> write
CONNECTION/tcpapp1 written
```

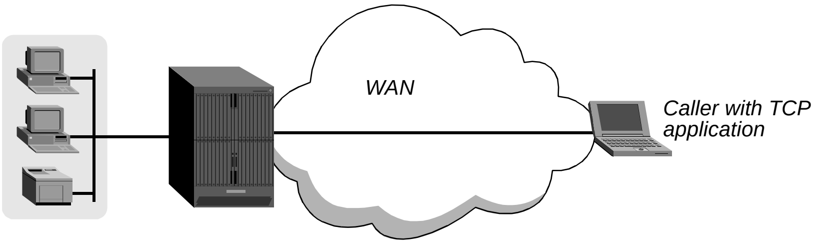
Following is a comparable RADIUS profile:

```
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
```

Example of a TCP-Clear connection with packet buffering (local profiles only)

In Figure 1-7, a caller dialing in to the TAOS unit is running an application that uses an encapsulation method that must be decoded by a local host. The TAOS unit sends the data stream from the incoming call directly to the host.

Figure 1-7. TCP-Clear connection to a local host



The following commands configure a TCP-Clear connection to a host named Sparky on TCP port 23, with the TAOS unit buffering packets before transmitting them. The End-of-Packet-Pattern is three hexadecimal numbers.

```
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
```

Applying an IPSec profile to a TCP-Clear session

RADIUS profiles use the following attribute-value pair to apply an IPSec profile to a TCP-Clear session. (For information about IPSec and creating IPSec profiles, see “Configuring IP security (IPSec) authentication” on page 5-17.)

RADIUS Attribute	Value
Ascend-IPSEC-Profile (73)	Name of an IPSec profile that describes the IPSec transforms and end points to use for this connection (a string value).

To use the attribute-value pairs in the profile specified by the Ascend-IPSEC-Profile attribute, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

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

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

For details about these settings, see the *APX 8000/MAX TNT Reference*. For details about setting up TCP-Clear connections, see “TCP-Clear connections” on page 1-23.

Tunnel mode and transport mode

The TAOS unit supports the IPSec transport mode and tunnel mode for TCP-Clear connections between gateways.

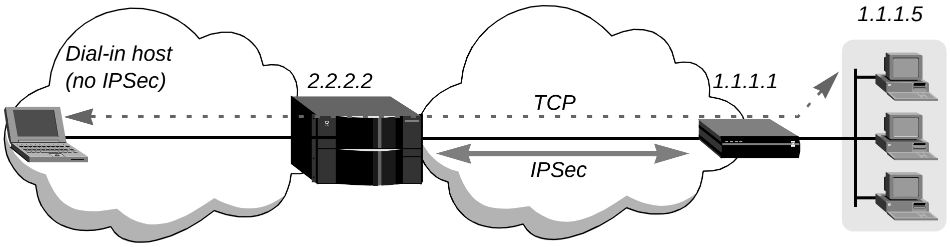
Tunnel mode is required for connections between a host that does not perform IPSec processing and a security gateway. In tunnel mode, IP packets are encapsulated in an outer IP header that specifies the IPSec processing destination (IP-in-IP encapsulation).

Transport mode operates between two hosts. Transport mode provides security services for higher-layer protocols, which can include selected portions of the IP header and other selected options.

In Figure 1-8, the IPSec end points are a TAOS unit and Pipeline 220 unit. The TCP end point is a TCP host dialing into the TAOS unit. Because the IPSec end points are different from the TCP end point, the IPSec profile for this connection must specify tunnel mode, as described in “IPSec encapsulation modes” on page 5-18. For example:

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

Figure 1-8. IPSec tunnel mode for TCP-Clear between gateways



The following sample RADIUS profile enables the dial-in host to establish a secure TCP-Clear session to a login host at 1.1.1.5:

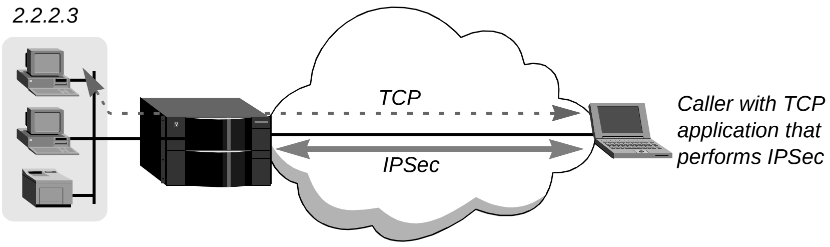
```
tcpapp-user Password = "localpw"
    Service-Type = Login,
    Login-Service = TCP-Clear,
    Login-Host = 1.1.1.5,
    Login-TCP-Port = 23,
    Ascend-IPSEC-Profile = securegw
```

The TAOS unit applies an IPSec profile named `securegw` to the session's data stream. The Pipeline 220 must have a corresponding IPSec configuration, and the two IPSec end points require Connection or RADIUS profiles for the link between them.

In Figure 1-9, the dial-in host is running a TCP application that is capable of performing IPSec encapsulation and decapsulation. In this case, the IPSec end points and the TCP-Clear end point are the same, so the IPSec profile for this connection specifies transport mode. For example:

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

Figure 1-9. IPSec transport mode for TCP-Clear with dial-in host



The following sample profile enables the dial-in user to use an IPSec profile named `dialin` to establish a secure TCP-Clear session to a login host at 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
```

Example of an IPSec ESP configuration for TCP-Clear

In the following example, an administrator creates an IPSec profile applying IPSec ESP to packets tunneled to and from an IPSec security gateway at the IP address 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
```

In the next set of commands, the TAOS unit's send configuration must match corresponding parameters in the far-end security gateway's IPSec receive configuration, and vice versa:

```
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

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
```

Following are sample RADIUS profiles that refer to the IPSec profile:

```
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
```

X.75 connections

The following parameters (shown with their default values) enable dial-in access to the terminal server from ISDN terminal adapters using the X.75 protocol. Settings in the Answer-Defaults profile apply to RADIUS-authenticated connections.

```
[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
```

Parameter	**Specifies**
Enabled	Enable/disable X.75 systemwide for incoming calls. X.75 is enabled by default.
K-Frames-Outstanding	Maximum number of data packets that can be outstanding in an X.75 connection before acknowledgment is required. The valid range is from 2 to 7. The default is 7.
N2-Retransmissions	Retry limit, which is the maximum number of times the TAOS unit can resend a frame on the X.75 connection when the T1 Retransmission Timer expires. The valid range is from 2 to 10 (default 10). Within this range, a higher value increases the probability of a correct transfer of data, and a lower value allows for quicker detection of an error condition.
T1-Retran-Timer	Maximum number of ticks the transmitter should wait for an acknowledgment before initiating a recovery procedure. The valid range is from 500 to 2000. The default value is 1000 (1 second).
Frame-Length	Maximum frame size for the link. The default is 1024 bytes. The HDLC card can support the maximum frame size of 1532 bytes. The Hybrid Access II and III (HDLC2) slot cards can support up to 2048 bytes. For X.75 connections, the maximum is 2048 bytes.

Full technical specifications for X.75 can be found in the *CCITT Blue Book Recommendation X* series 1988. Following is an example of configuring a Connection profile for X.75 when a Hybrid Access HDLC slot card is installed:

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

```
admin> set active = yes
admin> set ppp recv-password = passwd

admin> set x75-options frame-length = 1532

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

Configuring nailed and nailed MP+ connections

A nailed connection is a permanent link that is always up as long as the physical connection persists. If the unit or central switch resets, or if the link goes down, the TAOS unit attempts to restore the link at ten-second intervals. If the TAOS unit or the remote unit is powered off, the link comes back up when the device boots up again.

An unchannelized line (such as serial WAN) can be used in its entirety for a nailed connection. On an ISDN line, a nailed connection uses one or more channels that have been configured for nailed usage and assigned a group number. All channels in a group are aggregated into an indivisible, dedicated unit of bandwidth for the connection that uses it. More than one connection cannot share the same group of channels. If more than one group is assigned to a nailed connection, the sum of the channels in the multiple groups is an aggregated indivisible unit of bandwidth.

Nailed connections

For the most part, a nailed connection uses the same settings as a switched connection. If either the TAOS unit or the far-end device resets, the nailed connection must be reestablished, typically with negotiations similar to those for establishing a switched connection. The following subsections describe only the parameters that are unique to nailed connections.

Settings in a Connection profiles

The following Connection profile parameters are relevant to a nailed connection:

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

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

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

Parameter	**Specifies**
Dial-Number	Number to dial out for this connection.
Backup	Name of a profile to use if the nailed connection goes down. See “Backup interfaces for nailed connections” on page 1-36.
Answer-Originate	Enable/disable origination of the call to establish the nailed connection.
Call-Type	Type of call. Set to FT1 for a nailed connection.

Parameter	Specifies
Nailed-Groups	Group numbers of channels for the connection. You can specify multiple groups by separating the numbers with commas, in which case the bandwidth is an aggregate of all specified groups. Nailed bandwidth cannot be shared by other connections.

Settings in a RADIUS profile

The following RADIUS attribute-value pairs are relevant to nailed connections:

RADIUS Attribute	Value
Ascend-Dial-Number (227)	Number to dial out for this connection.
Ascend-Backup (176)	Name of a profile to use if the nailed connection goes down. See “Backup interfaces for nailed connections” on page 1-36.
Ascend-Call-Type (177)	Type of call. Set to Nailed (1) for a nailed connection.
Ascend-Group (178)	Group numbers of the channels dedicated to the connection. You can specify multiple groups by separating the numbers with commas, in which case the bandwidth of the connection is an aggregate of all specified groups. Nailed bandwidth cannot be shared by other connections.

When you have created or modified a nailed profile in RADIUS, you must reload the information from the RADIUS server. The following command requests a reload of all nailed profiles (permanent connections) from the RADIUS server:

```
admin> refresh -n
```

In the current software version, you can specify how nailed connections are handled after a Refresh –n. Following is the relevant parameter, shown with its default value:

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

Parameter	Specifies
Perm-Conn-Upd-Mode	Method of reloading permanent connections: Reestablish all permanent connections after a Refresh, or reestablish only changed permanent connections. With a setting of All (the default), the system behaves as in earlier versions of the software: All existing permanent connections are brought down and then brought up again (along with any new connections) after the update. This setting causes service interruption every time any nailed profile is updated or added. With a setting of Changed, only new connections are created, and only those with modified attribute values are reestablished.

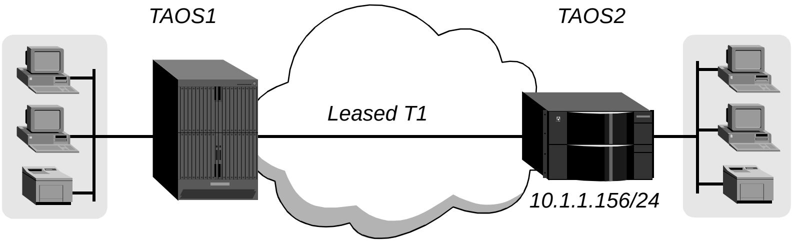
Following is an example of setting the Refresh –n command should to download only changed profiles:

```
admin> read system
SYSTEM read

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

admin> write
SYSTEM written
```

Example of a nailed connection

In Figure 1-10, the TAOS1 unit and the TAOS2 unit communicate via a leased T1 line with all of its channels assigned to group 11.

Figure 1-10. A nailed (permanent) connection



The following set of commands on the TAOS unit named TAOS1 configures a local profile for the nailed connection to 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
```

Following is a comparable RADIUS profile:

```
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”
```

Nailed MP+ connections

A connection that uses MP+ encapsulation can specify a certain number of nailed channels as the base connection, and add switched channels as needed by using the dynamic bandwidth allocation (DBA) algorithms. (For details about DBA, see “Multilink Protocol Plus (MP+) connections” on page 1-18.)

An *FT1-MPP* connection starts as a nailed connection but can use switched channels either to increase the bandwidth as needed or to provide a backup if the nailed channels go down. The maximum number of channels for the FT1-MPP connection is either the Maximum-Channel-Count for the connection or the number of nailed channels in the specified group, whichever is greater.

The base channels of an FT1-MPP connection are nailed. When a nailed channel is temporarily down, the TAOS unit polls continuously while trying to reestablish that connection. If an outbound packet arrives while the nailed connection is still down, the unit replaces the nailed channel with a switched channel, even if the call is on line with more than the minimum number of channels.

Settings in a Connection profile

In addition to the MP+ parameters described in “Multilink Protocol Plus (MP+) connections” on page 1-18, the following parameters are relevant to an FT1-MPP connection:

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

Parameter	**Specifies**
Answer-Originate	Enable/disable origination of the call to establish the nailed connection. Together, the Answer-Originate and FT1-Caller parameters specify that the TAOS unit is the designated caller for the switched part of the connection.
Call-Type	Type of call. Set to FT1-MPP for a nailed MP+ connection.
Nailed-Groups	Group numbers of the dedicated channels for the nailed part of the connection.
FT1-Caller	Enable/disable origination of the switched part of the connection. Because bandwidth is added on the basis of calculations made at both ends of the connection, only one end of the connection can originate calls for FT1-MPP.

Settings in a RADIUS profile

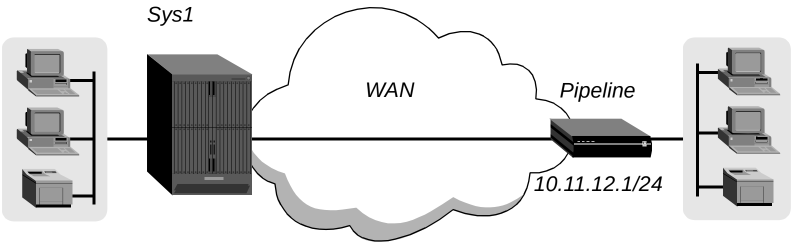
In addition to the MPP attributes, which are described in “Multilink Protocol Plus (MP+) connections” on page 1-18, RADIUS uses the following attribute-value pairs for nailed MP+ connections:

RADIUS Attribute	Value
Ascend-Call-Type (177)	Type of call. Set to Nailed/Mpp (2) for a nailed MP+ connection.
Ascend-Group (178)	Group numbers of the dedicated channels for the nailed part of the connection.
Ascend-FT1-Caller (175)	Enable/disable origination of the switched part of the connection. Specify FT1-No (0) to wait for the remote end to initiate the call, or FT1-Yes (1) for the TAOS unit to dial out to add channels. Only one end of the connection can be the FT1 caller.

Example of a nailed MP+ connection

In Figure 1-11, the TAOS unit establishes a nailed MP+ connection with a Pipeline 25 unit across the WAN.

Figure 1-11. Connection using both nailed and switched bandwidth



For the nailed MP+ connection to use nailed channels in groups 1 and 3, you would configure the local profile as follows:

```
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
```

Note: If you modify the Connection profile for an FT1-MP+ (ft1-mpp) connection, most changes become active only after the call is brought down and then back up, because the connection is primarily a nailed one. However, if you add a group number to the Nailed-Groups parameter setting and write the modified profile, the additional channels become available immediately.

Following is a comparable nailed (permanent) profile in RADIUS:

```
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”
```

Backup interfaces for nailed connections

The term *backup* refers to a set of capabilities for the system to establish and use a temporary, alternative connection to a destination when the primary connection becomes unavailable. A backup connection replaces the primary connection, which must be a nailed (permanent) connection. The backup interface can be nailed or switched.

When the TAOS unit detects that the primary interface is unavailable, it puts the primary interface in a Backup Active state. It does not remove the routes to the primary interface, but diverts traffic from the primary to the backup interface. When the unit detects that the primary interface is available again, it diverts traffic back to the primary interface. If the backup interface is a switched connection, the unit then brings it down.

One of the side effects of the data-link-layer backup interface is that, when a nailed interface specifies a backup interface, the routes to the nailed interface never go down.

You can specify a backup interface for a nailed connection in local Connection profiles or in RADIUS. Nested backups are not supported. (The profile for a backup interface cannot specify another backup interface.) The profile for a backup interface does not inherit attributes, such as filters or firewalls, from the profile for the primary nailed connection.

Settings in a Connection profile

In the Connection profile for the primary, nailed interface, the following parameter assigns a backup interface. (The value shown is the default.)

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

Parameter	Specifies
Backup	Name of a Connection profile for the backup interface. This is specified in the profile for the primary nailed interface.

Settings in a RADIUS profile

In RADIUS, a Permconn profile is a pseudo-user profile in which the first line has the following format:

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

The *name* argument is the TAOS unit’s system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the TAOS unit stops retrieving the profiles when it encounters the gap.

The following attribute can be set to specify a backup interface for a Permconn pseudo-user profile:

RADIUS Attribute	Value
Ascend-Backup (176)	Name of the profile for the backup interface.

Example of a switched backup interface

In the sample profiles that follow, the primary interface is a nailed MP+ connection defined in a profile named `nailed`, and the backup interface is a switched PPP connection defined in a profile named `p7`. In this example, the remote IP address of the primary and the backup connection are the same. (For another example of backup interfaces that use different IP addresses for the primary and backup connections, both of which are nailed, see the *APX 8000/MAX TNT Frame Relay Configuration Guide*).

The following set of commands defines the primary and backup interfaces in local Connection profiles:

```
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 recv-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 recv-password = ascend

admin> set ip remote-address = 10.168.7.9/24

admin> write
CONNECTION/pvc written
```

Following are comparable RADIUS profiles:

```
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
```

When the TAOS unit brings up the nailed connection, the routing table includes entries such as the following:

```
...
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
...
```

If the nailed connection becomes unavailable, the switched connection comes up. In this case, because the remote IP address of the primary and backup interfaces is the same, the routing table does not change. (No routes are added or deleted.)

The Ifmgr command displays the primary interface in the Backup Active state (indicated by a plus sign), as shown in the following sample output:

```
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
```

Notice that `nailed` is shown with a plus sign (+) to indicate that it is in the Backup Active state (that it is backed up by another connection). When the nailed connection comes up again, the switched connection is torn down. At that point, the Ifmgr command output shows the primary interface in the Active state, and shows the backup connection in the Down state. For example:

```
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
```

Configuring dial-out connections

Typically, the TAOS unit initiates dial-out connections on the basis of packet routing. When it receives a packet to be forwarded across a WAN interface and the WAN connection is not up, it searches its routing table for a route and dials the connection on the basis of the routing entry. If the profile for the connection is not in the local system, the route for the remote network must specify a dial-out profile, as shown in the RADIUS examples that follow. (The system can find local profiles by using only the IP address.)

Another type of dial-out occurs when users are allowed to access the TAOS unit digital modems to dial out. For details about modem dial-out, see “Modem dial-out connections” on page 1-43.

About RADIUS dial-out profiles

The name of a dial-out profile can be any convenient name (other than the name used for the dial-in profile), but the convention is to use the dial-in name followed by `–out`. For example, the following are two corresponding dial-in and dial-out profiles:

```
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"
```

All RADIUS dial-in profiles include at a minimum a username and password. When the TAOS unit wants to dial out, it uses the name and a well-known password to retrieve the dial-out profile. To eliminate the possibility that someone could make use of the well-known password and a dial-out profile to gain access to the network, all dial-out profiles should also have Service-Type set to Outbound-User. This attribute-value pair prevents anyone from using the profile for incoming authentication.

The User-Name attribute in the dial-out profile should specify the name of the dial-in profile to avoid “glare” between simultaneous dial-in and dial-out calls for the same user. This is a recommended procedure that helps to avoid possible problems.

Configurable dial-out timer

The TAOS unit uses a 20-second timer to establish a dial-out call. If the remote side is not connected within that time, the dial-out attempt fails. However, you can set the dial-out timer to allow increased flexibility for international dialing. Following is the relevant parameter, shown with its default setting:

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

Max-Dialout-Time specifies the maximum number of seconds the system waits for a Call Setup Complete packet from the remote side when dialing out. Valid values are from 0 to 255. The default is 20 seconds. If the parameter is set to zero, the TAOS unit uses its internal default of 20 seconds. In the following example, the dial-out timer is set to 60 seconds:

```
admin> read system
SYSTEM read

admin> set max-dialout-time = 60

admin> write
SYSTEM written
```

Note: The Max-Dialout-Time setting does not influence the modem timeout to detect carrier. Modems have an internal timer that counts down from dial-out to establishing carrier with the remote modem (including training), which for Rockwell modems has a default of 45 seconds.

Dial-out PPP and multichannel PPP profiles

Some callers might not require dial-out capability in a PPP, MP, or MP+ profile. The main reason to provide dial-out capability is to enable the TAOS unit to bring up the connection to forward packets.

Settings in a Connection profile

The following Connection profile parameters, shown with their default settings, enable dial-out in a PPP or multichannel PPP profile:

```
[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
```

Parameter	Specifies
Dial-Number	Number to dial out for this connection.
Send-Auth-Mode	Authentication protocol to request when the TAOS unit initiates the connection. (See “Password authentication” on page 1-12.)
Send-Password	Password sent to the remote device when the TAOS unit initiates the connection.
Remote-Address	IP address of the remote device. The TAOS unit brings up the connection to route packets on the basis of this address.

Settings in a RADIUS profile

For background information, see “About RADIUS dial-out profiles” on page 1-39. A RADIUS user profile can include the following attribute-value pairs for configuring a dial-out PPP connection:

RADIUS Attribute	Value
Service-Type (6)	Type of service. Set to Outbound-User for dial-out profiles to avoid possible security issues.
User-Name (1)	Name of the remote device. For dial-out profiles, should specify the name assigned to the corresponding dial-in profile, to avoid “glare” if there are simultaneous inbound and outbound connections.
Ascend-Dial-Number (227)	Number to dial out for this connection (a string value).
Ascend-Send-Auth (231)	Authentication protocol to use for a dial-out connection. (See “Password authentication” next).
Ascend-Send-Secret (232)	Password sent to the remote device when the TAOS unit initiates the connection. If the profile uses the Ascend-Send-Passwd (232) attribute to specify the password, the RADIUS daemon performs no encryption before sending the password across the network to the NAS. (For more information, see “Shared secrets and secure exchanges” on page A-5.)
Ascend-Remote-Addr (154)	IP address of the remote device. The TAOS unit brings up the connection to route packets on the basis of this address.

Password authentication

PPP authentication for dial-out calls uses the setting of the Send-Auth-Mode parameter in a local profile or the Ascend-Send-Auth attribute in a RADIUS profile to determine which protocol to request from the far end. It can specify the following protocols:

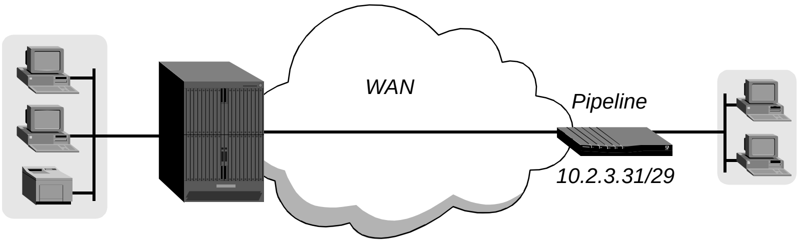
- None (the TAOS unit does not request the use of a particular protocol). This is the default, specified as No-PPP-Auth in a local profile or Send-Auth-None(0) in a RADIUS profile.
- Password Authentication Protocol (PAP). The TAOS unit requests PAP, but uses CHAP if the far end requires it. In a local profile the setting is PAP-PPP-Auth. In a RADIUS profile it is Send-Auth-PAP (1).
- Challenge Handshake Authentication Protocol (CHAP). The TAOS unit requires the use of CHAP. In a local profile the setting is CHAP-PPP-Auth. In a RADIUS profile it is Send-Auth-CHAP (2).
- Microsoft's extension of CHAP, used by Windows NT/LAN Manager (MS-CHAP). In a local profile the setting is MS-CHAP-PPP-Auth. In a RADIUS profile it is Send-Auth-MS-CHAP (3).

For details about password authentication for PPP, MP, and MP+ connections, see Appendix A, "Authentication Methods."

Examples of a dial-out PPP connection

In Figure 1-12, the far-end device is a Pipeline unit with the IP address 10.2.3.31/29.

Figure 1-12. Dial-out PPP connection



The following commands create a profile that enables the system to answer a dial-in or initiate a dial-out to the far end:

```
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 recv-password = localpw

admin> write
CONNECTION/phani written
```

Following are comparable RADIUS profiles:

```
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"
```

Modem dial-out connections

If modem Direct-Access is enabled in the Terminal-Server profile, users can dial out through the TAOS unit’s digital modems. The Direct-Access service uses the Telnet protocol, rather than a raw TCP connection, for communicating with client processes. Therefore, any client process that is to use this service to transmit or receive binary data must, at a minimum, escape outgoing IAC (0xFF) characters, handle escaped incoming IAC characters, and strip out incoming Telnet options. For a description of the Telnet protocol and how it differs from a raw TCP connection, see RFCs 854 and 855.

System reset requirement

After you configure the system to listen for dial-out modem connections on a specified port, you must reset the system to enable the feature.

Enabling modem Direct-Access

You can enable direct access to the 56Kbps modems by setting the following parameters (shown with their default values):

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

Note: To enable modem access, you must set both the Enabled and the Direct-Access parameters to Yes in the Terminal-Server profile.

Parameter	Specifies
Enabled	Enable/disable modem dial-out of any kind. With a setting of No, none of the other parameters in the Dialout-Configuration subprofile apply.
Direct-Access	Enable/disable the Direct-Access dial-out feature. With a Yes setting, users can Telnet to a particular port on the TAOS unit to get immediate dial-out service. The port number configured as the Port-for-Direct-Access tells the TAOS unit that all Telnet sessions to that port want direct access to a modem. With the No setting, the remaining parameters in the Dialout-Configuration subprofile do not apply.

Parameter	Specifies
Port-for-Direct-Access	TCP port number to use for immediate dial-out service. Must be set to an integer from 5000 (the default) to 32767 if Direct-Access is enabled.
Password-for-Direct-Access	The password (up to 64 characters) used for Global mode authentication. If Security-for-Direct-Access is not set to Global, this parameter is ignored.
Security-for-Direct-Access	Password security for Direct-Access. None (the default) means that no password is required to access the modems. If this parameter is set to Global, a single global password protects modem usage. The Password-for-Direct-Access parameter must specify the global password. When a user initiates a Telnet session to the specified port, the system prompts for the assigned Password-for-Direct-Access. If the setting is User, a user must have a dial-out profile that specifically allows modem dial-out. In that case, the PPP Recv-Password in the user's profile is required for access to the unit's modems.

Example of Direct-Access using a global password

The following commands set up Direct-Access dial-out on TCP port 5028 with a Global security setting:

```
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
```

With this configuration, a user dials out on a modem as follows:

1. Telnet to the TAOS unit, specifying the Direct-Access port number on the command line. For example:

   ```
   telnet taos01 5028
   ```

2. When prompted for a password, enter the Password-for-Direct-Access value.

   ```
   Password: pizza
   ```

3 Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to your computer. For example:

```
ATDT 555-1212
```

4 To terminate the session with the modem, terminate the Telnet session.

Dial-out modem connections that require profiles

If you set Security-for-Direct-Access to User, a user must have a dial-out profile that specifically allows modem dial-out. In that case, the Send-Password setting in the user's profile protects modem usage. For example, if you use the following settings:

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

When a user initiates a Telnet session for Direct-Access, the system prompts for a username and matches the user's input to a Connection profile (or RADIUS profile). It then password-authenticates the dial-out session, using the profile's password.

Connection profile settings

Following are the Connection profile parameters relevant to Direct Access dial-out (shown with their default setting):

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

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

Parameter	**Specifies**
Recv-Password	User's password. The system prompts for this password before allowing the user access to its modems.
Dialout-Allowed	Enable/disable modem dial-out. If the username and password match up, the system checks the Dialout-Allowed setting. If the setting is Yes, the system provides access to one of its modems.

RADIUS profile settings

Following are the RADIUS profile attributes relevant to Direct Access dial-out:

RADIUS Attribute	**Usage for a Direct-Access dial-out**
Password (2)	User's password. The system prompts for this password before allowing the user access to its modems.
Ascend-Dialout-Allowed (131)	Enable/disable modem dial-out. If the username and password match up, the system checks this attribute. If the setting is Dialout-Allowed (1), the system provides access to one of its modems.

Example of Direct-Access with user security

The following commands set up Direct-Access dial-out on TCP port 5000 with a security setting of 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
```

The following set of commands configures a Connection profile for dial-out:

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

admin> set ppp recv-password = kpassword

admin> set telco dialout-allowed = yes

admin write
CONNECTION/kevin written
```

Following is a comparable RADIUS profile:

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

With this setup, the user named Kevin dials out on a modem as follows:

1. Specify the Direct-Access port number on the Telnet command line. For example:

   `telnet taos01 5000`

2. Enter your username at the system prompt:

   `User:` **`kevin`**

3. Enter your password at the system prompt:

   `Password:` **`kpassword`**

4. Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a workstation. For example:

   `ATDT 555-1212`

5. To terminate the session with the modem, terminate the Telnet session.

IP Routing

2

Routing overview

When you power on or reset the TAOS unit, it creates an IP routing table containing all the routes it knows about, including the following:

- Routes for local active IP interfaces (configured IP-Interface profiles)
- Routes for active WAN IP connections (switched or nailed connections that are up)
- Routes for inactive switched WAN IP connections (configured Connection profiles)
- Routes defined in IP-Route profiles or RADIUS route profiles

If dynamic routing protocols are enabled on one or more interfaces, the TAOS unit adds routes it learns from routing-update packets. In addition, it is continuously updating its routing table by adding routes for links that become active and removing routes for inactive connections. If a nailed connection goes down, the TAOS unit removes the route from its routing table.

Routes and interfaces

An IP route specifies a destination address, a gateway to the network, and an interface that leads to the gateway. It can also specify metrics and other values associated with the route.

A route defined in a profile is a *static route*. A *dynamic route* is learned from Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) updates sent by other routers. Dynamic updates provide access to many more routes than those actually configured in the

TAOS unit, and are updated automatically as routes change. However, they cause additional routing overhead, so they are disabled by default.

An *interface* is a point of ingress to or egress from the system. For example, a local interface is an Ethernet port and a WAN interface is a nailed or switched connection. An *IP interface* is the logical IP address that enables IP data to be sent and received.

Displaying the routing table

To view the routing table, use the Netstat command. For example:

```
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
```

For each route in the table, the Destination and Gateway fields show the destination address and the address of the next-hop router used to reach that destination. The zero destination address is the default route. If the system does not find a route for a packet's destination, it forwards the packet to the default route rather than dropping the packet. Note that the system uses the most specific route (having the longest prefix) that matches a given destination. Direct routes do not show a gateway address.

An asterisk (*) in the flags column indicates a hidden route, which is not included in routing updates sent by the TAOS unit and is not used for forwarding packets. Hidden routes are used only for display purposes.

The IF field shows the name of the interface through which a packet addressed to the entry's destination will be sent. The route to the `mcast` interface name encapsulates the multicast forwarder for the entire class D address space. (For more information, see "Setting up multicast forwarding" on page 2-73.)

Routes to the local machine display the `local` interface name. Packets to the 224.0.0.1 and 224.0.0.2 interfaces can be multicast and received like normal multicast packets, but upon receiving such a packet, the router does not forward it to another link layer device. Effectively, these packets have a maximum transmission unit (MTU) of 1.

OSPF uses 224.0.0.5 and 224.0.0.6 for inter-router communications (instead of using broadcasts, as RIP does).

Displaying the interface table

To display the interface table, use the `–i` option on the Netstat command line:

```
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
```

The entries named `ie0` or `ie`*N-N-N[-N*] represent Ethernet interfaces. *N-N-N-N* represents the shelf number, slot number, item number, and logical-item number of the interface. When the logical-item number is zero (the physical interface), it does not appear in the interface name. The same sequence of numbers forms the address used to index the IP-Interface profile. For example, the default profile for 1-4-1 is indexed as follows:

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

When the logical-item number is *not* zero, it does appear in the interface name. Again, the sequence of numbers is identical to the profile index. For example, suppose an IP-Interface profile has the following index:

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

This profile has the following interface name:

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

The other names in the interface table have the following significance:

- The `lo0` (loopback) interface is the local loopback.
- The `rj0` (reject) and `bh0` (blackhole) interfaces are used in the Pool-Summary feature.
- The `wanabe` interface is an inactive RADIUS dial-out profile.

- The `local` interface is the local machine.
- The `mcast` interface is the multicast interface, which represents the multicast forwarder for the entire class-D address space. For details, see “Setting up multicast forwarding” on page 2-73.
- The `tunnel` interface is a pseudo-interface that is used only when the TAOS unit is configured as an ATMP Router Home Agent. In that configuration, the TAOS unit creates a route for each registered mobile client. Regardless of how many tunnels the Home Agent might terminate, there is always a single tunnel interface. (The number terminating the tunnel interface name is an internal number that can change from one software version to the next.)
- The `vr0_main` interface represents the router itself. For details, see “Configuring VRouters” on page 6-1.
- The `sip0` interface is a soft IP interface. For details, see “Setting a system source IP address” on page 2-36.
- The numbered WAN (`wan`*N*) interfaces are WAN connections, which are entered in the interface table as they become active.

IP address syntax

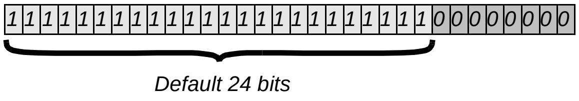
A TAOS unit uses dotted decimal format (not hexadecimal) for IP addresses. If no subnet mask is specified, the unit assumes a default mask based on the address class. Table 2-1 shows address classes and the number of network bits in the default mask for each class.

Table 2-1. IP address classes and number of network bits

Class	Address range	Default network bits
Class A	0.0.0.0–127.255.255.255	8
Class B	128.0.0.0–191.255.255.255	16
Class C	192.0.0.0–223.255.255.255	24

For example, a class C address, such as 198.5.248.40, has 24 network bits, leaving 8 bits for the host portion of the address. If no subnet mask is specified for a class C address, the TAOS unit assumes the default mask of 24 bits, as shown in Figure 2-1.

Figure 2-1. Default subnet mask for class C IP address



A subnet address includes a prefix length, which specifies the number of network bits in the address. For example, the following address specifies a 29-bit subnet:

```
ip-address = 198.5.248.40/29
```

In this address, 29 bits of the address are used to specify the network. The three remaining bits are used to specify unique hosts on the subnet. With three bits used to specify hosts on a 29-bit subnet, eight different bit combinations are possible. Of those eight possible host addresses, two are reserved:

000 — Reserved for the network (base address)
001
010
100
110
101
011
111 — Reserved for the broadcast address of the subnet

Note: Be careful with zero subnets (subnets with the same base address as a class A, B, or C network). Early implementations of TCP/IP did not allow them. For example, the subnet 192.32.8.0/30 was illegal because it had the same base address as the class C network 192.32.8.0/24, while the subnet 192.32.8.4/30 was legal. Modern implementations of TCP/IP support zero subnets, and the TAOS unit implementation of RIP treats these subnets the same as any other network. However, it is important that you treat zero subnets consistently throughout your network. Otherwise, you will encounter routing problems.

Table 2-2 shows subnet masks and prefix lengths for a class C network number.

Table 2-2. Decimal subnet masks and prefix lengths

Subnet mask	Number of host addresses	Prefix length
255.255.255.0	254 hosts + 1 broadcast, 1 network base	/24
255.255.255.128	126 hosts + 1 broadcast, 1 network base	/25
255.255.255.192	62 hosts + 1 broadcast, 1 network base	/26
255.255.255.224	30 hosts + 1 broadcast, 1 network base	/27
255.255.255.240	14 hosts + 1 broadcast, 1 network base	/28
255.255.255.248	6 hosts + 1 broadcast, 1 network base	/29
255.255.255.252	2 hosts + 1 broadcast, 1 network base	/30
255.255.255.254	invalid mask (no hosts)	/31
255.255.255.255	1 host—a host route	/32

The broadcast address of any subnet has the host portion of the IP address set to all ones. The network address (or base address) represents the network itself, because the host portion of the IP address is all zeros. For example, supposing the TAOS unit configuration assigns the following address to a remote router:

```
198.5.248.120/29
```

The Ethernet network attached to that router has the following address range:

```
198.5.248.120 — 198.5.248.127
```

A host route is a special-case IP address with a prefix length of /32. For example:

```
198.5.248.40/32
```

Host routes are to a single host, rather than to a router or subnet.

Configuring LAN IP interfaces

A LAN IP interface is an Ethernet port configured for IP. A TAOS unit creates an IP-Interface profile for an Ethernet port when it first detects the presence of the port. For example, the following output shows the default IP-Interface profiles for the shelf controller and an Ethernet-2 card installed in slot 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 }
```

The profile for the first Ethernet port on a card in shelf 1, slot 12, uses the following index:

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

This index consists of a physical address and a logical-item number in the following format:

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

The logical item addresses a specific logical interface. It is zero except when multiple (virtual) interfaces have been configured on the physical port. For more details, see “Example of defining virtual LAN interfaces” on page 2-9.

Overview of LAN interface settings

Following are the parameters in an IP-Interface profile, shown with default settings:

```
[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
```

Parameter	Specifies
Interface-Address	Shelf address of the Ethernet interface or, if the item number is not zero, the virtual interface address.
IP-Address	IP address of the LAN interface.

Parameter	Specifies
Proxy-Mode	Enable/disable proxy ARP responses for dial-in devices that are assigned local addresses.
RIP-Mode	Enable/disable RIP updates on the interface. RIP is disabled by default on LAN interfaces.
Route-Filter	Filter for RIP update packets. For details, see Chapter 9, “Packet Filters.”
RIP2-Use-Multicast	Enable/disable use of the multicast address (224.0.0.9) rather than the broadcast address for RIP updates. By default, RIP updates use the multicast address.
OSPF	OSPF routing options. See “Adding a TAOS unit to an OSPF network” on page 3-9.
Multicast-Allowed	Multicast forwarding option. See “Setting up multicast forwarding” on page 2-73.
Multicast-Rate-Limit	Multicast forwarding option. See “Setting up multicast forwarding” on page 2-73.
Multicast-Group-Leave-Delay	Multicast forwarding option. See “Setting up multicast forwarding” on page 2-73.
Directed-Broadcast-Allowed	Enable/disable forwarding of directed broadcast traffic onto the interface and its network.
VRouter	Name of a virtual router. See “Assigning interfaces to a VRouter” on page 6-7.
Management-Only-Interface	Enable/disable management-only on the IP interface.

Example of configuring a LAN IP interface

The following commands set the IP address of the leftmost shelf-controller Ethernet port:

```
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
```

In this example, the TAOS unit resides on the 10.1.2 subnet. To enable it to communicate with routers on other local subnets, it must either have a static route configuration to another router in its own subnet, or it must enable RIP. (For an example of configuring a route to a local router, see “Examples of configuring default routes” on page 2-26.)

After you assign an IP address, you can verify that the TAOS unit is a valid IP host on that network segment by pinging another host, as shown in the following example:

```
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
```

Enabling proxy ARP

When you enable proxy ARP, hosts on the local network can ARP for hosts or subnets that reside across the WAN but have an IP address on the local network. The TAOS unit responds to the ARP requests, and then routes the packets for those connections across the WAN.

You can enable Proxy-Mode by setting it to Active (respond for active WAN connections only), Inactive (respond only for inactive WAN connections), or Always (respond for all pool addresses, including those for inactive connections). If the TAOS unit is set to respond to ARP requests for inactive connections, it brings up the required WAN connection.

The following commands configure both shelf-controller LAN interfaces in an APX 8000 to respond as proxies for ARP requests for active WAN connections:

```
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
```

In this case, if controller switchover occurs, the system can continue to respond to ARP requests.

Enabling RIP

RIP is off by default, so a TAOS unit does not send out its routing table or receive routing information from other routers on the interface. Therefore, local hosts on other subnets cannot access remote hosts without static route configurations, and dial-in hosts do not have access to other routes maintained locally.

You can enable RIP to receive routing table updates, send them, or both. Receiving updates from other routers increases the size of the TAOS unit's routing table. The table then provides access to more networks, but route searches are not as fast. Sending updates propagates information about remote networks to local routers.

Note: Running RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements is not recommended. RIP-v1 guesses subnet masks, while RIP-v2 handles them explicitly. Running the two versions on the same network can result in RIP-v1 guesses overriding accurate subnet information obtained via RIP-v2.

The following commands configure a TAOS unit to receive RIP-v2 updates on the multicast address:

```
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
```

Example of defining virtual LAN interfaces

You can configure up to 16 IP-Interface profiles for each Ethernet card as a whole, with each profile specifying one IP address. The system creates the default profile for an interface and assigns it the zero logical-item number. To configure another IP address on a LAN interface, create an IP-Interface profile with a nonzero logical-item number in its interface address. For example, the following commands create a virtual interface for an Ethernet port installed in shelf 1, slot 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
```

The logical-item numbers do not have to be consecutive, but they must each be unique. The following restrictions apply to virtual LAN interfaces:

- The default IP-Interface profile (with the zero logical-item number) must have an IP address configured, or none of the other IP-Interface profiles for the same port will function. (Do not delete the default profile and expect your other configurations to work.)
- If Proxy-Mode is enabled in any of the IP-Interface profiles for a given Ethernet port, it is enabled for all ARP requests coming into the physical port.
- OSPF can be enabled on any one of a port's IP interfaces, but not on more than one interface for the same port. This is in conformance with RFC 1583.

Example of defining the soft interface

A TAOS unit supports a soft IP interface, which is an internal interface that never goes down. Therefore, as long as one of the unit's IP interfaces is up, the soft interface address is reachable.

Note: Do not use the IP address of a physical LAN interface for the soft interface address.

The IP-Interface profile with the zero index is reserved for the soft interface. If RIP is enabled, the unit advertises the interface address as a host route (with a prefix length of 32 bits) using the loopback interface. If RIP is not enabled, routers one hop away from the unit must have a static route to the soft interface address.

The following commands set the soft interface IP address to 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
```

To create an interface-independent address for a VRouter, create a new IP-Interface profile with the logical-item value greater than zero. For example:

```
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
```

The TAOS unit adds the soft address to its interface table with the name `sip#`, where # is the logical-item number from the IP-Interface profile index. For more details about VRouters, see “Assigning interfaces to a VRouter” on page 6-7.

If routing updates (RIP or OSPF) are enabled, a TAOS unit advertises the interface address as a host route with a mask of /32, using the loopback interface. If RIP or OSPF is not enabled, routers one hop away from the TAOS unit must have a static route to the soft address. To verify that other hosts in your network have a route to the soft address, execute Ping or Traceroute from the other hosts. For example:

```
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
```

Example of disabling directed broadcasts

Denial-of-service attacks known as “smurf” attacks typically use ICMP Echo Request packets with a spoofed source address and packets directed to IP broadcast addresses. These attacks are intended to degrade network performance, possibly to the point that the network becomes unusable.

To prevent the TAOS router from being used as an intermediary in this type of denial-of-service attack launched from another network, you must disable the TAOS router from forwarding directed broadcasts it receives from another network. The following example shows how to disable directed broadcasts that are not generated locally. All IP interfaces in the system must disable the feature explicitly. The sample commands configure both shelf-controller interfaces (so the broadcasts are still disabled if controller switchover occurs) and the IP interfaces of a four-port Ethernet card in shelf 1, slot 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
```

Example of defining a management-only interface

Management-only means that incoming traffic on the interface terminates in the system itself. The traffic is not forwarded on any other interface. In addition, only traffic generated by the system is forwarded on the management-only interface. Traffic generated externally is dropped on the interface. Setting the Management-Only parameter to Yes enforces these conditions on the port.

The following commands specify that a port on an installed card is a management-only interface:

```
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
```

The Ifmgr –d command displays a Management Only field to reflect the port’s status.

Configuring WAN IP interfaces

A WAN IP interface is a nailed or switched connection configured for IP. A TAOS unit creates a routing interface for local Connection profiles (if they do not use pool addresses) when the system starts up. For interfaces that use pool addresses or are defined in RADIUS user profiles, the unit creates a routing interface when a session becomes active.

Overview of WAN interface settings

You configure WAN IP interfaces in Connection profiles or RADIUS profiles. At a minimum, each profile specifies the IP address of the far-end device or a pool from which the system assigns an address. You can also set a variety of routing and service parameters.

Settings in Connection profiles

Following are the IP options (shown with default settings) in a Connection profile:

```
[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
```

Parameter	Specifies
IP-Routing-Enabled	Enable/disable IP routing for the interface. IP routing is enabled by default.
VJ-Header-Prediction	Enable/disable Van Jacobsen prediction for TCP packets on incoming calls using encapsulation protocols that support Van Jacobsen compression. The default setting is Yes.
Remote-Address	IP address of the calling device, which can include a subnet specification. If the address does not include a subnet mask, the router assumes the default subnet mask based on address class.
Local-Address	IP address assigned to the local side of a numbered-interface connection. (For details, see “Example of a numbered-interface connection” on page 2-18.)
Routing-Metric	RIP metric for the specified route (a number from 1 to 15, default 1). If preference values are equal, the higher the metric, the less likely that the TAOS unit will use the route.
Preference	Preference value for the route. Valid values are from 0 to 255. For details, see “Setting static-route preferences” on page 2-40.
Down-Preference	Preference value for the route when the interface is down.
Private-Route	Enable/disable advertisement of the route when the router sends RIP or OSPF updates. With the Yes setting, the route is excluded from update packets.
Multicast-Allowed	See “Setting up multicast forwarding” on page 2-73.
Address-Pool	Number of the address pool from which to acquire an address (see “Configuring and using address pools” on page 2-62).
IP-Direct	IP address of a host to which all IP packets received across the link will be directed (see “Example of an IP-Direct connection” on page 2-20).
RIP	Enable/disable RIP updates on the interface. RIP is disabled by default.
Route-Filter	Filter for RIP update packets. For details, see Chapter 9, “Packet Filters.”
Source-IP-Check	Enable/disable antispoofing for the session. With the Yes setting, the system does not accept packets that do not originate on the subnet to which the remote device is attached. The system determines the subnet during IPCP negotiation. If Remote-Address specifies a subnet, packets that originate on that subnet are accepted. If Remote-Address specifies a 32-bit mask, only packets from that host are accepted. Packets sent from an address that does not match are discarded.
OSPF-Options	OSPF routing options (see Chapter 3, “OSPF Routing”).
Multicast-Rate-Limit	Multicast forwarding option (see “Setting up multicast forwarding” on page 2-73).

Parameter	Specifies
Multicast-Group-Leave-Delay	Multicast forwarding option (see “Setting up multicast forwarding” on page 2-73).
Client-DNS-Primary-Addr	Client DNS option (see “Using client DNS” on page 2-58.)
Client-DNS-Secondary-Addr	Client DNS option (see “Using client DNS” on page 2-58.)
Client-DNS-Addr-Assign	Client DNS option (see “Using client DNS” on page 2-58.)
Client-Default-Gateway	Default route for traffic from this connection. For details, see “Example of client default gateways” on page 2-21.
TOS-Options:Active	Enable/disable proxy-QoS and TOS for this connection (see “Example of setting QoS and TOS policy” on page 2-22).
TOS-Options:Precedence	Priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled, you can set the bits to one of the following values (most significant bit first): • 000—Normal priority • 001—Priority level 1 • 010—Priority level 2 • 011—Priority level 3 • 100—Priority level 4 • 101—Priority level 5 • 110—Priority level 6 • 111—Priority level 7 (the highest priority)
TOS-Options:Type-of-Service	Type of Service of the data stream. The next four bits of the TOS byte are used to choose a link according to the type of service. When TOS is enabled, Type-of-Service can specify Normal (Normal service), Cost (Minimize monetary cost), Reliability (Maximize reliability), Throughput (Maximize throughput), Latency (Minimize delay).
TOS-Options:Apply-To	Direction in which TOS is enabled. With the Input setting (the default), bits are set in packets received on the interface. With the Output setting, bits are set in outbound packets only. With the Both setting, both incoming and outgoing packets are tagged.

Settings in RADIUS profiles

The following attribute-value pairs configure IP options in a RADIUS profile:

RADIUS Attribute	Value
Ascend-Route-IP (228)	Enable/disable IP routing for the interface. IP routing is enabled by default.

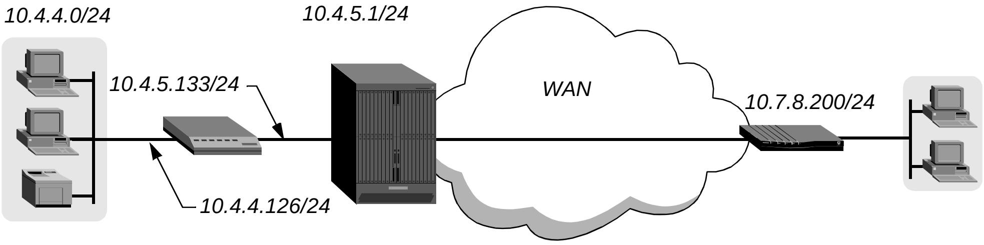
RADIUS Attribute	Value
Framed-Compression (13)	Enable/disable Van Jacobsen prediction. You can specify Van-Jacobsen-TCP-IP to turn on TCP/IP header compression. If you do not specify this value, RADIUS uses the default of no header compression.
Framed-IP-Address (8)	IP address of the calling device.
Framed-IP-Netmask (9)	Subnet mask of the caller's address. If you do not specify a subnet mask, the router assumes the default subnet mask based on address class.
Ascend-PPP-Address (253)	IP address assigned to the local side of a numbered-interface connection. For details, see "Example of a numbered-interface connection" on page 2-18.
Ascend-IF-Netmask (153)	Subnet mask in use for the local-side numbered interface.
Ascend-Metric (225)	RIP metric for the specified route (a number from 1 to 15, default 7). If preference values are equal, the higher the metric, the less likely that the TAOS unit will use the route.
Ascend-Route-Preference (126)	Preference value for the route. Valid values are from 0 to 255. A value of 255 prevents the use of the route. For details about setting preferences, see "Setting static-route preferences" on page 2-40.
Framed-Route (22)	Static route definition, which can be used to make a user profile a private route. For details, see "Configuring static IP routes" on page 2-23.
Ascend-Assign-IP-Pool (218)	Number of the address pool from which to acquire an address. For details, see "Configuring and using address pools" on page 2-62.
Ascend-Assign-IP-Global-Pool (146)	Name of a global address pool. For details, see "Global RADIUS pools (RADIPAD)" on page 2-63.
Ascend-IP-Direct (209)	IP address of a host to which all IP packets received across the link will be directed. For details, see "Example of an IP-Direct connection" on page 2-20.
Framed-Routing (10)	Enable/disable RIP updates on the interface. RIP is disabled by default. Valid values are None(0), Broadcast(1), Listen(2), Broadcast-Listen(3), Broadcast-v2(4), Listen-v2(5), and Broadcast-Listen-v2(6).
Ascend-Source-IP-Check (96)	Enable/disable antispoofing for the session. The default is Source-IP-Check-No (0). With the Source-IP-Check-Yes (1) setting, the system discards packets that do not originate on the subnet to which the remote device is attached. The system determines the subnet during IPCP negotiation. If Framed-IP-Netmask specifies a subnet, packets that originate on that subnet are accepted. If Framed-IP-Netmask specifies a 32-bit mask, only packets from a single host are accepted. Packets sent from an address that does not match are discarded.
Ascend-Multicast-Client (155)	Multicast forwarding option. For details, see "Setting up multicast forwarding" on page 2-73.
Ascend-Multicast-Rate-Limit (152)	Multicast forwarding option. For details, see "Setting up multicast forwarding" on page 2-73.

RADIUS Attribute	**Value**
Ascend-Multicast-GLeave-Delay (111)	Multicast forwarding option. For details, see “Setting up multicast forwarding” on page 2-73.
Ascend-Client-Primary-DNS (135)	Client DNS option. For details, see “Using client DNS” on page 2-58.
Ascend-Client-Secondary-DNS (136)	Client DNS option. For details, see “Using client DNS” on page 2-58.
Ascend-Client-Assign-DNS (137)	Client DNS option. For details, see “Using client DNS” on page 2-58.
Ascend-Client-Gateway (132)	Default route for traffic from this connection. For details, see “Example of client default gateways” on page 2-21.
Ascend-IP-TOS (87)	Type of Service (TOS) of the data stream. The value of this attribute sets the four bits following the three most significant bits of the TOS byte. The four bits are used to choose a link according to the type of service. Specify one of the following values: • Ascend-IP-TOS IP-TOS-Normal (0)—Normal service • Ascend-IP-TOS IP-TOS-Disabled (1)—Disable TOS • Ascend-IP-TOS IP-TOS-Cost (2)—Minimize monetary cost • Ascend-IP-TOS IP-TOS-Reliability (4)—Maximize reliability • Ascend-IP-TOS IP-TOS-Throughput (8)—Maximize throughput • Ascend-IP-TOS IP-TOS-Latency (16)—Minimize delay
Ascend-IP-TOS-Precedence (88)	Priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled, set the bits to one of the following values (most significant bit first): • IP-TOS-Precedence-Pri-Normal (0)—Normal priority • IP-TOS-Precedence-Pri-One (32)—Priority level 1 • IP-TOS-Precedence-Pri-Two (64)—Priority level 2 • IP-TOS-Precedence-Pri-Three (96)—Priority level 3 • IP-TOS-Precedence-Pri-Four (128)—Priority level 4 • IP-TOS-Precedence-Pri-Five (160)—Priority level 5 • IP-TOS-Precedence-Pri-Six (192)—Priority level 6 • IP-TOS-Precedence-Pri-Seven (224)—Priority level 7 (the highest priority)
Ascend-IP-TOS-Apply-To (89)	Direction in which TOS is enabled. With the IP-TOS-Apply-To-Incoming (1024) setting, which is the default, bits are set in packets received on the interface. With the IP-TOS-Apply-To-Outgoing (2048) setting, bits are set in outbound packets only. With the IP-TOS-Apply-To-Both (3072) setting, both incoming and outgoing packets are tagged.

Example of a connection to another IP router

Figure 2-2 shows the TAOS unit connecting to a far-end router, such as a Pipeline. This could be a telecommuting configuration, for example, in which the Pipeline is located at a branch or home office.

Figure 2-2. Router-to-router IP connection



The default settings for the IP-Options subprofile enable IP routing and Van Jacobsen header compression and turn RIP off. Those settings are appropriate for the following example, which shows configuration of a Connection profile for the Pipeline in Figure 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
```

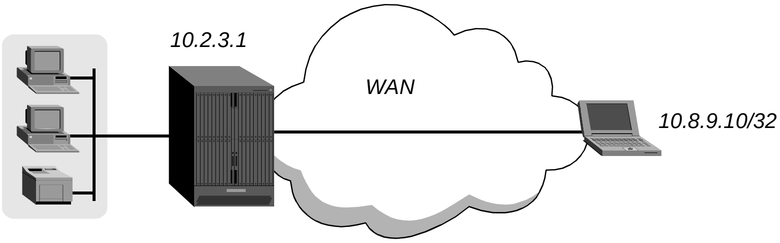
Following are comparable RADIUS profiles:

```
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"
```

Example of a host route connection

A host route is advertised as an IP address with a subnet mask of 32. It represents a single host rather than a remote router. Figure 2-3 shows a sample connection in which a dial-in host with an ISDN modem card calls into a TAOS unit.

Figure 2-3. Dial-in host requiring a static IP address (a host route)



The PPP configuration includes the host’s address. For example:

```
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
```

The default settings for the IP-Options subprofile enable IP routing and Van Jacobsen header compression and turn RIP off. Those settings are appropriate for the following example, which shows configuration of the Connection profile for the host in Figure 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
```

Following is a comparable RADIUS profile:

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

Example of a numbered-interface connection

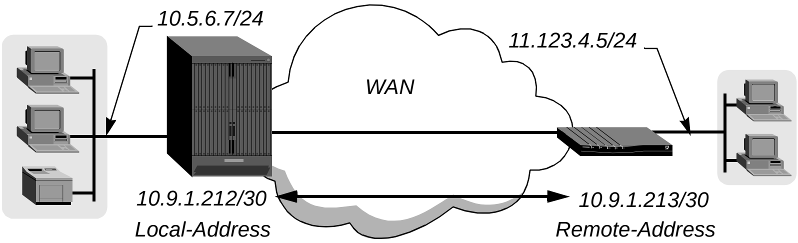
For a numbered-interface connection, each side of the connection is assigned a unique address that applies only to the connection. This is a requirement for some applications, such as SNMP.

The Local-Address value assigned to a numbered interface must be unique to the connection and to the network. You can assign a fake IP address or an IP address from one of the local subnets. A TAOS unit accepts IP packets destined for the specified address and treats them as destined for the system itself. (The packets can arrive on any interface, and the destination interface need not be in the active state.)

Note: Do not assign a local address that belongs to one of the TAOS unit's real, physical LAN interfaces. Doing so will cause routing problems.

Figure 2-4 shows a numbered-interface connection. The TAOS unit's real, physical Ethernet interface has the IP address 10.5.6.7/24. The other two addresses represent the local and remote addresses of the numbered-interface connection.

Figure 2-4. A numbered-interface connection



The following set of commands specifies a Connection profile for the numbered interface:

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

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp recv-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
```

Following is a comparable RADIUS profile:

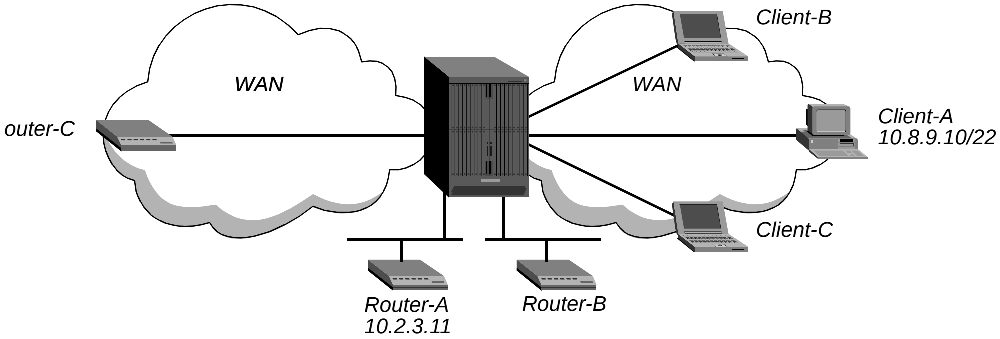
```
numbered Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Route-IP = Route-IP-Yes,
   Framed-IP-Address = 10.9.1.213,
   Framed-IP-Netmask = 255.255.255.252,
   Ascend-PPP-Addr = 10.9.1.212,
   Ascend-IF-Netmask = 255.255.255.252
```

In this example, the interface is assigned a 30-bit subnet, so four bit combinations are available for host assignments. Of the four possible host addresses, the one that is evenly divisible by 4 is the network or base address (the address that specifies zeros in the host bits). This address is added to the routing table. The other host addresses are assigned a /32 subnet mask and added as host routes. You can suppress advertisement of the host routes associated with a numbered interface by using the Suppress-Host-Routes parameter, as described in "Suppressing host-route advertisements" on page 2-44.

Example of an IP-Direct connection

Packets received on an IP-Direct connection bypass the routing tables and are redirected instead to a specified next-hop destination IP address. Outbound packets are routed as usual. Currently, the feature is implemented only for data calls. Figure 2-5 shows an example of the IP-Direct traffic flow.

Figure 2-5. IP-Direct connections



In Figure 2-5, the following conditions apply:

- Client-A’s profile redirects inbound packets to router-A on a LAN interface.
- Client-B’s profile redirects inbound packets to router-B on a LAN interface.
- Client-C’s profile redirects inbound packets to router-C through a switched connection.

Outbound packets destined for any of the three clients are routed normally by the TAOS unit, which means that these client connections can *receive* packets from any source, not just from the IP address to which their packets are sent.

The following set of commands configures an IP-Direct Connection profile for client-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
```

Following is a comparable RADIUS profile:

```
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
```

IP-Direct connections require the following special handling:

- If the profile enables the receipt or receipt-transmission of RIP updates, all RIP packets from an incoming connection are kept locally and forwarded to the IP-Direct address, so that the TAOS unit can correctly forward packets *destined* for the client.
- ARP requests received from the incoming connection are ignored.
- The caller cannot Telnet to the TAOS unit, because the connection is passed through to the IP-Direct host.

Example of making the route to a connection private

A private route is placed in the routing table but is marked with a flag that prevents routing protocols from advertising it. The following commands specify a private route in a Connection profile:

```
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
```

Following is a comparable RADIUS profile:

```
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"
```

Example of client default gateways

A client default gateway is a route that replaces the systemwide default route for a particular connection. For packets arriving on the connection, if the TAOS unit consults the routing table and finds no match for the packets' destination (if it finds only the system default route or, if there is no system default route, no match at all) it forwards the packets to the client default gateway address.

The specified address must be a legitimate next hop, that is, the TAOS unit must be able to reach the router directly in one hop. If this is not the case, the unit drops the packets it should route to the client default gateway.

Packets from other users or from the Ethernet network are handled normally. The system's routing table is not modified by use of this feature. The following commands specify a connection-specific default gateway:

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

admin> set ip-options client-default-gateway = 17.1.1.1

admin> write
CONNECTION/test written
```

Following is a comparable setting in a RADIUS profile:

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

Example of per-session source address checking

You can configure WAN IP interfaces so that the system checks the source IP address in all received packets and drops the packets if the address does not match the address negotiated for the far-end subnet. This type of configuration enables the TAOS unit to detect packets with a spoofed source IP addresses and discard them.

When the system initially detects a spoofing attempt (a mismatched source address), it logs a message that includes the port number on which the attempt occurred. For example:

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

The following commands configure a Connection profile for antispoofing:

```
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
```

Following is a comparable setting in a RADIUS profile:

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

Example of setting QoS and TOS policy

You can configure the TAOS unit to set quality of service (QoS) priority bits and type of Service (TOS) classes of service on behalf of customer applications. The TAOS unit does not implement priority queuing, but it does set information that can be used by other routers to prioritize and select links for particular data streams.

To enable service-based TOS or to set QoS precedence for the traffic on a particular WAN connection, configure the TOS options in a Connection or RADIUS profile. The settings cause the TAOS unit to set bits in the TOS byte of IP packet headers that are received (the default), transmitted, or both, on the WAN interface. Another router can then interpret the bits accordingly.

You can also specify proxy-QoS and TOS policy in a TOS filter, which can then be applied to any number of Connection or RADIUS profiles. For a Connection or RADIUS profile that has both its own local policy and an applied TOS filter, the policy defined in the TOS filter takes precedence. For example, applying a TOS filter to a TOS-enabled connection allows you to define one priority setting for incoming packets on a connection and another for incoming packets addressed to a particular destination (the destination in a TOS filter). For details, see Chapter 9, “Packet Filters.”

The following set of commands enables TOS for incoming packets on a WAN interface. It sets the priority of the packets at 6, which means that another router that implements priority queuing will not drop the packets until it has dropped all packets of a lower priority. The commands also set TOS to prefer maximum throughput, which means that the priority-queuing router will choose a high bandwidth connection if one is available, even if it has higher cost or higher latency or is less reliable than another available link.

```
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
```

Following is a comparable RADIUS profile:

```
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
```

Configuring static IP routes

Any profile that specifies how to reach an IP device or subnet (such as an IP-Interface, Connection, or RADIUS user profile) specifies a static IP route to that destination. However, sometimes administrators configure static routes in a more flexible way, to extend or fine-tune the routing table.

The default route is a special-case static route that acts as a catch-all for packets for which the TAOS unit cannot find a route. If you define a default route (with the zero destination address), the TAOS unit routes all packets with unknown destinations to the specified gateway. If no default route is defined, the TAOS unit drops those packets.

If the unit’s LAN IP addresses include subnet specifications, you must create a static route to another LAN router to enable the TAOS unit to reach local networks beyond its own subnets. You might also configure a static route to a LAN router to offload local routing overhead from the TAOS unit.

Another reason to configure static routes is to specify multipath routes, which define multiple paths to the same destination. Multipath routes, with equal metric and equal preference values, distribute traffic to a single destination across multiple interfaces.

Note: The TAOS unit does not support multipath dial-out routes from RADIUS.

Overview of static-route settings

You can define static routes in IP-Route profiles or in RADIUS.

Settings in IP-Route profiles

Following are the parameters in a local IP-Route profile (shown with default settings):

```
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 = ""
```

Parameter	**Specifies**
Name	Name of the profile (up to 31 characters).
Dest-Address	Destination IP address, which can include a subnet specification. The default value is 0.0.0.0, which represents a default route.
Gateway-Address	IP address of a router used to reach the specified destination.
Metric	RIP metric for the specified route (a number from 1 to 15, default 8). If preference values are equal, the higher the metric, the less likely that the TAOS unit will use the route.
Cost	OSPF option (see “Configuring OSPF static-route information” on page 3-16).
Preference	Preference value of the route. For details, see “Setting static-route preferences” on page 2-40.
Third-Party	OSPF option. For details, see “Configuring OSPF static-route information” on page 3-16.
ASE-Type	OSPF option. For details, see “Configuring OSPF static-route information” on page 3-16.
ASE-Tag	OSPF option. For details, see “Configuring OSPF static-route information” on page 3-16.
Private-Route	Enable/disable advertisement of the route when the router sends RIP or OSPF updates. With the Yes setting, the route is excluded from update packets.
Active-Route	Enable/disable entering the route in the routing table. (Setting the parameter to No is a useful way to make a route temporarily inactive, so you can reinstate the route later.)

Parameter	**Specifies**
ASE7-Adv	OSPF option. For details, see “Configuring OSPF static-route information” on page 3-16.
VRouter	Virtual Router option. For details, see “Defining VRouter static routes” on page 6-9.
Inter-VRouter	Virtual Router option. For details, see “Defining VRouter static routes” on page 6-9.

Settings in a RADIUS route profiles

A route profile is a pseudo-user profile in which the first line has the following format:

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

The *name* argument is the TAOS unit’s system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the TAOS unit stops retrieving the profiles when it encounters the gap.

To specify routes that can be dialed out by more than one system, eliminate the name argument. In that case, the first word of the pseudo-user profile is `route-N.`

Each pseudo-user profile specifies one or more routes with the Framed-Route (22) attribute. The RADIUS protocol limits the number of Framed-Route definitions in a single route profile. The limit varies with the exact contents of the routes. However, 25 Framed-Route definitions per profile is the recommended maximum.

The value of the Framed-Route attribute uses the following syntax:

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

Syntax element	**Specifies**
dest-addr	Destination IP address, which can include a subnet specification. The default value is 0.0.0.0, which represents a default route.
gateway-addr	IP address of the next-hop router to reach the specified destination.
metric	RIP metric for the specified route (a number from 1 to 15, default 8). If preference values are equal, the higher the metric, the less likely that the TAOS unit will use the route.
private	Enable/disable advertisement of the route when the router sends RIP or OSPF updates. The Yes setting makes the route private, excluding it from update packets.
profile	Name of the dial-out user profile for the route. The default value is null.
preference	Preference value of the route. For details, see “Setting static-route preferences” on page 2-40.
VRouter	Virtual Router option. For details, see “Defining VRouter static routes” on page 6-9.

Route settings in a RADIUS user profile

You can also include the Framed-Route (22) attribute in a RADIUS user profile to define a static route. For details about Framed-Route usage, see “Settings in a RADIUS route profiles” on page 2-25.

In a user profile, you can specify the zero address as the gateway address. In this context, the 0.0.0.0 address is a wildcard entry the TAOS unit replaces with the caller’s IP address. When RADIUS authenticates the caller and sends the TAOS unit an Access-Accept message with a value of 0.0.0.0 for the router address, the TAOS unit updates its routing tables with the Framed-Route value, but substitutes the caller’s IP address for the router address. This setting is useful when the TAOS unit assigns an IP address from an address pool and RADIUS does not have access to the IP address of the caller.

If a Framed-Route definition in a user profile duplicates a route defined in the TAOS unit’s routing table or IP-Route profile, the user profile definition takes precedence while the connection is active. For example, suppose a static route to network 10.10.10.10 is defined in a local IP-Route profile, with a metric of 10. A RADIUS user profile defines a static route to 10.10.10.10 with a metric of 7. When the RADIUS user’s route is not in use, the routing table indicates that the route has a metric of 10. When the route is in use, the TAOS unit routing table indicates that the route has a metric of 7, with an `r` in the flags column to indicate that the route came from RADIUS. Furthermore, the route with a metric of 10 remains in the routing table, with an asterisk (*) in the flags column, indicating that it is a hidden route.

Connection-specific private static routes (RADIUS only)

The following attribute-value pair configures IP options in a RADIUS profile:

RADIUS Attribute	**Value**
Ascend-Private-Route (104)	A private framed route known only to the profile in which it is specified. The value is a destination address and next-hop router address (in that order). For details, see “Examples of private static routes” on page 2-34.

Examples of configuring default routes

A route with the zero destination address is a default route. If the system does not find a route for a packet’s destination, rather than dropping the packet, it forwards it to a default route. If there is no default route in the routing table, the TAOS unit drops any packet for which it cannot find a route.

The TAOS unit creates an IP-Route profile named `default`, but the profile is not valid until you specify a gateway address, so the route is not active until you assign an address and activate the route. For example:

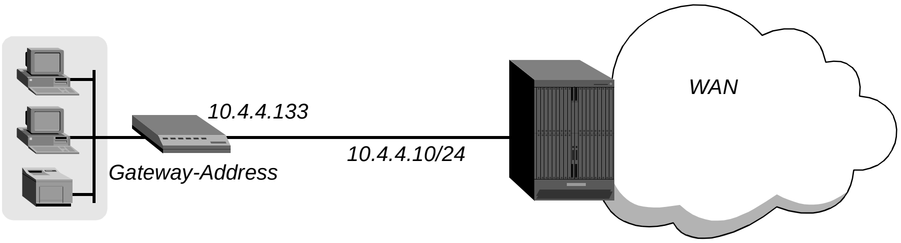
```
admin> read ip-route default
IP-ROUTE/default read

admin> set gateway-address = 10.10.10.10

admin> set active-route = yes

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

You can create a default route by modifying the `default` profile, or by creating one or more IP-Route profiles that specify a zero destination and a valid gateway address.

Example of a LAN-based default route

Figure 2-6 shows a router that resides on the same subnet as one of the TAOS unit's local IP interfaces.

Figure 2-6. Default route to a local IP router



Because the TAOS unit is located on a subnet, it needs to be informed about other backbone routers that can route beyond the subnet. In this example, the TAOS unit offloads part of its routing overhead by using a default route to the LAN router. The following commands define a default route to the local router:

```
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
```

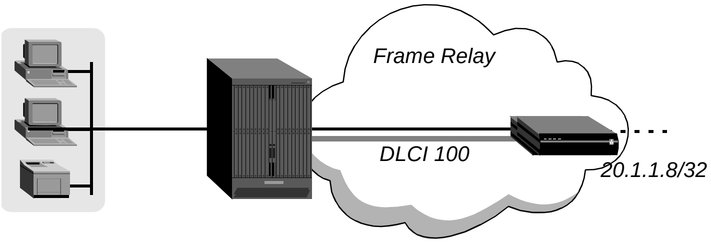
Following is a comparable RADIUS default route:

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

Example of a default route across a WAN link

Figure 2-7 shows a router that resides across a Frame Relay DLCI interface. If the WAN link to this default route goes down for any reason, the TAOS unit removes the route from its routing table.

Figure 2-7. Default route across a Frame Relay DLCI interface



In this example, the following Frame Relay settings define the data link:

```
[in FRAME-RELAY/fr1]
fr-name* = fr1
active = yes
```

```
nailed-up-group = 1
link-mgmt = ansi-t1.617d
link-type = dte
```

The following Connection profile defines the DLCI interface:

```
[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 }
```

The following commands define a default route to the remote device:

```
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
```

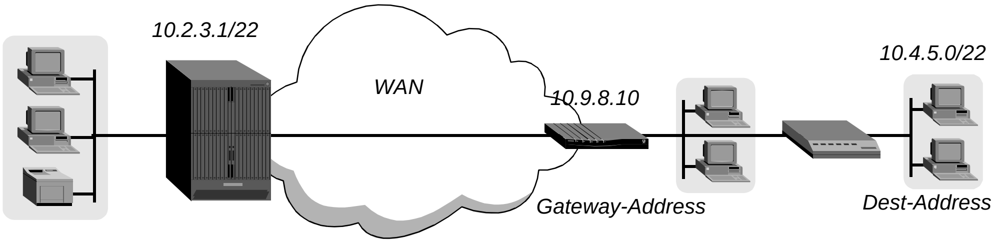
Following is a comparable RADIUS default route:

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

Example of configuring a route to a remote subnet

When RIP and OSPF are turned off on an IP interface, the router cannot reach other routers on that interface unless it has a static route. For example, if a Connection profile specifies the destination address of a host on a remote subnet, but the packets must be routed through an intermediary device to reach that host (and RIP or OSPF is not enabled), you must configure a static route specifying the intermediary device as the gateway. Figure 2-8 shows an example.

Figure 2-8. Static route to a remote subnet



The following commands configure a static route to all hosts on the remote subnet:

```
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
```

Following is a RADIUS profile that shows both the default route and a route to the remote subnet:

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

Example of configuring a multipath route

Multipath static routes distribute traffic to one destination across the aggregated bandwidth of multiple interfaces. A multipath route requires that the multiple static routes have the same destination address and subnet mask, but different gateway addresses. In addition, they must have the same route metric or OSPF cost, and the same route preference. (Otherwise, the route with the lowest values for these settings would be used exclusively.)

Note: Even the default routes can be multipath. If more than one route has a destination of 0.0.0.0, the TAOS unit creates multipath default routes.

Following is an example in which an administrator configures a multipath route to the network 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
```

The multipath routes appear in the routing table with the M (multipath) flag. For example:

```
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
```

Note: The TAOS unit does not support multipath dial-out routes from RADIUS. If a RADIUS profile defines multipath dial-out routes, such as the following:

```
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"
```

the TAOS unit adds to its routing table only the dial-out route it reads most recently (the route named `two-out` in this example).

Configuring private routing tables

In earlier versions of the software, you could define private routes through the use of the Ascend-Private-Route (104) attribute only with a RADIUS user profile. In the current software version, you can also use that attribute in private-route pseudo-user profiles, which can then be referred to by multiple RADIUS profiles, Connection profiles, or both. These externally defined private routing tables are cached locally for a configurable interval. The PrtCache command displays statistics about each cached RADIUS private-route profile, and enables you to flush profiles from the cache.

You can also define private routing tables locally, in the Private-Route-Table profile. These profiles can then be referenced by multiple RADIUS profiles, Connection profiles, or both.

Overview of local profile settings

To configure private routing tables, you set the following parameters (shown with default settings):

```
[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
```

Parameter	**Specifies**
Name	Name of the profile, up to 23 characters. This name is used to associate a RADIUS or Connection profile with the defined private routes.
Enabled	Enable/disable the specific route for use in the private routing table. A table can contain up to 24 routes.
Dest-Address	Destination IP address, which can include a subnet specification. This setting works the same as its counterpart in an IP-Route profile. For details, see the *APX 8000/MAX TNT Reference*.
Netmask	Netmask of the destination IP address, set automatically when you specify a prefix length as part of the IP address.
Gateway-Address	IP address of a router used to reach the specified destination. This setting works the same as its counterpart in an IP-Route profile. For details, see the *APX 8000/MAX TNT Reference*.

Parameter	Specifies
Metric	RIP metric for the specified route (a number from 1 to 15, with a default of `8`). This setting works the same as its counterpart in an IP-Route profile. For details, see the *APX 8000/MAX TNT Reference*.
Private-Route-Table	Name of a Private-Route-Table profile associated with the connection. The name can be that of a local profile or of a private-route pseudo-user profile in RADIUS. However, if a local Connection profile does not use authentication, it cannot point to a RADIUS private-route profile.
Private-Route-Profile-Required	Whether access to the private routing table is required for the session. With the default value of `no`, the system establishes the session even if the associated private routing table is not found. If the parameter is set to `yes`, the system disconnects the call if the specified private routing table is not found. This parameter does not apply if the profile does not refer to a private routing table by name. In the Answer-Defaults profile, this parameter is used for RADIUS user profiles that refer to a private routing table and do not specify a value for Ascend-Private-Route-Required (55).
Default-Prt-Cache-Time	Number of minutes to cache RADIUS private-route profiles that do not include a value for Ascend-Cache-Time (57). The default is `1440` (24 hours). Once the cache timer expires, cached profiles are deleted from system memory. The next time a private route is needed, the system retrieves the profile from RADIUS and stores it in cache again. Keeping a profile in cache increases the performance of route lookups, at the cost of some system memory. If this parameter is set to `0` (zero), the default timer is disabled so that only RADIUS profiles specifying a cache time are cached.

Overview of RADIUS attributes for referring to a private routing table

RADIUS user profiles can refer to private-route profiles by specifying the following vendor-specific attributes (VSAs):

RADIUS Attribute	Specifies
Ascend-Private-Route-Table-ID (54)	Name of a RADIUS private-route profile associated with the connection.
Ascend-Private-Route-Required (55)	Whether access to the private routing table is required for the session. With the default value of Required-No (0), the system establishes the session even if the associated private routing table is not found. If the attribute is set to Required-Yes (1), the system disconnects the call if the private routing table is not found. This attribute does not apply if the profile does not refer to a private routing table by name. If no value is specified for this attribute, the setting for the Private-Route-Profile-Required parameter in the Answer-Defaults profile is used.

Overview of RADIUS attributes for defining a private routing table

In RADIUS, private route tables are defined in a pseudo-user profile. A private-route profile is a pseudo-user profile in which the first two lines have the following format:

```
profile-name Password = "ascend" Service-Type = Outbound
```

The *profile-name* value is any name you assign to the profile. Private-route profile definitions can include the following VSAs:

RADIUS Attribute	Specifies
Ascend-Private-Route (104)	Destination address and next-hop router address for a private route. Each private-route profile specifies one or more private routes with this attribute, which is more fully described in the *TAOS RADIUS Guide and Reference*.
Ascend-Cache-Refresh (56)	Whether the timer for cached routes in this profile is reset each time a new session that refers to the pseudo-user profile becomes active. Refresh-No (0) does not reset the timer. Refresh-Yes (1) resets the cache timer when a session referring to the profile becomes active.
Ascend-Cache-Time (57)	Number of minutes to cache the profile. Once the cache timer expires for a RADIUS profile, the profile is deleted from system memory. The next time it is needed, the system retrieves it from RADIUS and stores it in cache again. Keeping a profile in cache increases the performance of route lookups, at the cost of some system memory. The minimum possible cache time is 0 minutes, which causes the system to retrieve the profile for every route lookup in the table. This value is usually not desirable. If no value is specified for this attribute, the setting for the Default-Prt-Cache-Time parameter in the IP-Global profile is used.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

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

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

For details about these settings, see the *APX 8000/MAX TNT Reference.*

Example of configuring a private routing table

You can configure private routing tables locally or in RADIUS. For example, the following commands define a private routing table named `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
```

Following is a comparable RADIUS private-route profile:

```
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"
```

The following commands configure the default cache time for RADIUS private-route profiles:

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

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

admin> write
IP-GLOBAL written
```

Following is a sample RADIUS private-route profile that uses of the default instead of specifying a value for 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"
```

Examples of using private routing tables

The following commands modify a Connection profile so that the session has access to the routes in the private routing table, and the system disconnects the call if the private routing table is not found:

```
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
```

The following RADIUS profile refers to the same private routing table and has the same requirements. This profile also specifies how the routes are cached for this connection.

```
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
```

The following commands configure the system to reject incoming calls when the RADIUS user profile specifies a private routing table that is not found:

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

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

admin> write
ANSWER-DEFAULTS written
```

Following is a sample RADIUS profile that uses of the default instead of specifying a value for 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"
```

Examples of private static routes

A RADIUS user profile can specify a list of private routes associated with the connection. (There is no comparable functionality in local Connection profiles.)

Private routes defined by the Ascend-Private-Route attribute in a user profile affect only packets received from the connection. The routes are not added to the global routing table. If a destination is not found in the list of private routes and there is no default private route, the global routing table is consulted for a decision on routing the packets. Otherwise, only the private routing table is consulted.

Following is an example of a user profile that creates three private routes associated with the user:

```
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"
```

With this profile, the private routing table for the connection contains the following routes, the last one of which is the default route:

```
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
```

Note: The user profile can also specify the a value for Ascend-Client-Gateway attribute, but the value will *not* modify a private default route that has been specified by the Ascend-Private-Route attribute.

When the next-hop router address specified by an Ascend-Private-Route attribute is the zero address (0.0.0.0), a lookup is performed for that route in the global routing table, providing an exit mechanism to the global table for specific private routes. For example, suppose the private routes are defined as in the following RADIUS user profile:

```
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"
```

The private routing table for this connection contains the following routes:

```
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
```

With this private routing table, a route lookup for the 20.1.0.0/16 network proceeds to the global routing table.

Setting TCP/IP routing policies

The TAOS router has many configuration settings that affect its operations. The settings that determine its routing policies include security, RIP options, IP route cache options, and other options. These settings are available only in the IP-Global profile. They have no counterpart in RADIUS.

Note: You can also configure the TAOS unit to set QoS priority bits and TOS classes of service on behalf of customer applications. These settings can then be used by other routers to prioritize and select links for particular data streams. These policies are set on WAN interfaces. For details, see “Example of setting QoS and TOS policy” on page 2-22.

Setting a system source IP address

The system IP address is the source address used for all packets generated by the system. For example, this address is used for RADIUS requests, ATMP tunnel requests, or a Telnet, Traceroute, or Ping command originating from the unit. It must be the real address of one of the unit’s LAN IP interfaces, or the interface-independent address described in “Example of defining the soft interface” on page 2-9.

Following is the parameter for specifying a system address:

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

With the default zero address, the TAOS unit uses the IP address assigned to the shelf-controller Ethernet interface as the source address for packets it generates. One reason for setting a system address other than the default is that doing so simplifies access control. For example, most RADIUS servers keep a database of known RAS clients and their authentication keys. If you do not specify a system address, the RADIUS database must include a complete list of all the system's interface addresses. If you specify a system address, it is used for all RADIUS request packets.

Another reason for setting a system address is to ensure that packets sent from an ATMP Home Agent to Foreign Agents have a single, standard source address. A system address is recommended for ATMP Home Agents that have multiple interfaces into the IP cloud that separates them from Foreign Agents, to prevent communication problems if a route changes within the IP cloud. For details, see “System IP address recommendation” on page 4-2.

Following is an example of setting the System-IP-Addr parameter to an address assigned to a port on a slot card:

```
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
```

Setting router security policies

The following parameters (shown with default settings) affect router security:

```
[in IP-GLOBAL]
must-accept-address-assign = no
shared-prof = no
telnet-password = ""
user-profile = ""
```

Parameter	Specifies
Must-Accept-Address-Assign	Enable/disable rejection of an assigned IP address by an incoming caller during PPP negotiation.
Shared-Prof	Enable/disable shared profiles. Sharing profiles is recommended only for low-security networks.
Telnet-Password	Password required for Telnet access to the TAOS unit.
User-Profile	Name of a default User profile for Telnet sessions.

Requiring acceptance of dynamic address assignment

During PPP negotiation, a calling station could reject an IP address offered by the router and present the caller's own IP address for consideration. For security purposes, many sites set Must-Accept-Address-Assign to Yes to ensure that the TAOS unit terminates such a call, as shown in the following example:

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

admin> set must-accept-address-assign = yes

admin> write
IP-GLOBAL written
```

For address assignment to occur, the TAOS unit must have an address available for assignment, the Answer-Defaults profile must enable dynamic assignment, the caller's profile must specify dynamic assignment, and the caller's PPP dial-in software must be configured to acquire its IP address dynamically. For details, see "Examples of assigning an address from a pool" on page 2-67.

Shared profiles

In low-security situations, more than one caller can share a name and password for accessing the local network. If you do not need the added security of ensuring that each connection is authenticated with its own password, you can set the Shared-Prof parameter as follows:

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

admin> set shared-prof = yes

admin> write
IP-GLOBAL written
```

If you do enable shared profiles, the profile must not result in a shared IP address (two callers at different locations sharing the same address). The profile either must not assign an IP address at all or must assign one dynamically. When the shared profile uses dynamic address assignment, each call is a separate connection that shares the same name and password, but a separate IP address is assigned dynamically to each caller. For details about dynamic IP address assignment, see “Examples of assigning an address from a pool” on page 2-67.

You can also enable shared profiles on a per-connection basis even though they have been disallowed systemwide. This functionality is also available in RADIUS profiles via the Ascend-Shared-Profile-Enable attribute. Use the following parameter (shown with its default setting) to enable or disable shared profiles on a per user basis:

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

Parameter	Specifies
Shared-Prof	Enable/disable multiple callers to share the Connection profile, provided that IP address conflicts do not result. With the default setting of `no`, the setting of the Shared-Prof parameter in the IP-Global profile allows or disallows shared profiles systemwide.

If the IP-Global profile sets Shared-Prof to `yes`, the Shared-Prof setting in a Connection profile has no effect. However, if the IP-Global profile sets Shared-Prof to `no`, and a Connection profile sets it to `yes`, the setting in a Connection profile takes precedence. For example, with the following settings, multiple callers can call in and authenticate the Connection profile named `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
```

Specifying a default User profile for Telnet access

RADIUS use the following attribute-value pair to specify a default User profile for RADIUS-authenticated Telnet access to the TAOS unit:

RADIUS Attribute	Specifies
Ascend-Telnet-Profile (91)	Name of a TAOS unit’s User profile to be used for authenticating Telnet logins.

When a user attempts to Telnet into the TAOS unit’s interface, the system first looks for a User profile matching the login name and password given by the user. If that fails, the system uses the server specified in the External-Auth profile to locate a RADIUS user profile. If the RADIUS server returns a profile that includes the Ascend-Telnet-Profile attribute, the system uses the specified User profile to authenticate and set permissions for the session. Only RADIUS profiles that specify a value for this attribute can be used to authenticate a Telnet login to the TAOS unit's interface. Following is a sample RADIUS profile that enables Telnet access to the TAOS unit with administrator permissions:

```
admin Password = "secret-pw"
    Service-Type = Framed-User,
    Ascend-Telnet-Profile = admin
```

Restricting Telnet access to the system

A user can initiate a Telnet session to the TAOS unit's command line from a local workstation or from a WAN connection. In both cases, the TAOS unit authenticates the session by means of a User profile, which defines a permission level for the user logging in. (For details about User profiles, see the *APX 8000/MAX TNT Reference*.)

In addition to the password required by a User profile, you can specify that Telnet requires its own password authentication, which occurs before any User profile authentication.

The commands in the following example set the Telnet-Password parameter and specify the Default User profile for Telnet logins. The Default profile enables minimal permissions and requires no password.

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

admin> set telnet-password = !234#@

admin> set user-profile = default

admin> write
IP-GLOBAL written
```

When users Telnet to the system, they are allowed three tries, each with a 60-second time limit, to enter the correct Telnet password. If all three attempts fail, the connection times out. If they specify the correct Telnet password, the TAOS unit prompts again for a username and password to authenticate a User profile. In the following example, a user starts a Telnet session to a TAOS unit named TAOS01, for which a Telnet password has been specified.

```
% telnet taos01
<taos01> Enter Password:

Trying 10.1.2.3 ...
Connected to taos01.abc.com.
Escape character is ‘^]’.
User:
```

After entering the correct Telnet password, the user is prompted for a username and password to authenticate a User profile.

Setting systemwide routing policies

The following parameters, (shown with default settings) specify system-wide routing policies:

```
[in IP-GLOBAL]
ignore-icmp-redirects = no
icmp-reply-directed-bcast = no
```

```
drop-source-routed-ip-packets = no
static-pref = 100
```

Parameter	Specifies
Ignore-ICMP-Redirects	Enable/disable processing of ICMP Redirect packets.
ICMP-Reply-Directed-Bcast	Enable/disable responding as a host to directed-broadcast ICMP Echo Requests.
Drop-Source-Routed-IP-Packets	Enable/disable forwarding of IP packets that have the source route option set.
Static-Pref	Default preference given to static IP routes.

Ignoring ICMP packets

ICMP Redirect packets can be counterfeited and used to change the way a device routes packets. For security purposes, many sites choose to ignore ICMP Redirects.

ICMP Echo Requests to the broadcast address have been used in denial-of-service attacks. To prevent the TAOS router from being used in a denial-of-service attack when an attacker compromises another router on the same Ethernet network as the TAOS unit, you can prevent the TAOS unit from responding to directed-broadcast ICMP Echo Requests sent to the IP broadcast address.

The following commands configure the unit to ignore both types of ICMP packets. (By default, it does not respond to ICMP Echo Requests to the broadcast address.)

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

admin> set ignore-icmp-redirects = yes

admin> write
IP-GLOBAL written
```

Dropping source-routed packets

The default setting for the Drop-Source-Routed-IP-Packets parameter is No, which causes the router to forward all source-routed packets as described in RFC1812, *Requirements For Routers*. When the parameter is set to Yes, the router drops all packets that have either a Loose or a Strict source route among their IP options. The following set of commands instructs the router to drop source-routed packets:

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

admin> set drop-source-routed-ip-packets = yes

admin> write
IP-GLOBAL written
```

Setting static-route preferences

Because RIP and OSPF metrics are incompatible, the TAOS unit supports route preferences, which provide a way to weight routes that takes precedence over route metrics. When choosing a route, the router first compares preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, and uses the route with the lowest metric. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from ICMP Redirects
- 100—Routes learned from RIP
- 100—Static routes

If a dynamic route's preference value is lower than that of the static route, the dynamic route can hide (temporarily overwrite) a static route to the same network. However, dynamic routes age, and if no updates are received, they eventually expire. In that case, the hidden static route reappears in the routing table. By default, static routes and RIP routes have the same preference value, so they are weighted equally. ICMP Redirects take precedence over both, and OSPF takes precedence over everything.

The following command decreases the preference value of static routes, instructing the router to use those routes first if they exist:

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

admin> set static-pref = 50

admin> write
IP-GLOBAL written
```

Setting routing protocol options

The following parameters (shown with default settings) define how the TAOS unit handles routing protocol updates:

```
[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
```

Parameter	Specifies
RIP-Policy	Policy for sending update packets that include routes received on the same interface.
Summarize-RIP-Routes	Enable/disable summarization of subnet information in RIP-v1 updates. This setting has no effect on RIP-v2 updates.

Parameter	Specifies
RIP-Trigger	Enable/disable RIP triggering. With a Yes setting (the default), RIP updates include only changed routes.
RIP-Pref	Preference setting for routes learned from RIP.
Dialout-Poison	Enable/disable advertisement of dial-out routes when no trunks are available. Disabling advertisement (the Yes setting) allows a redundant unit to take over.
Ignore-Def-Route	Enable/disable exclusion of advertised default routes from the routing table.
RIP-Queue-Depth	Maximum number of RIP packets to be held for processing. Valid values are 0 to 1024. The default (0) means that the TAOS unit will not drop any RIP packets, no matter how far behind it gets.
Suppress-Host-Routes	Enable/disable suppression of host routes for interfaces with a subnet mask of less than 32 bits.
OSPF-Pref	OSPF option (see "Configuring route options" on page 3-14).
OSPF-ASE-Pref	OSPF option (see "Configuring route options" on page 3-14).
RIP-Tag	OSPF option (see "Configuring route options" on page 3-14).
RIP-ASE-Type	OSPF option (see "Configuring route options" on page 3-14).
AS-Boundary-Router	OSPF option (see "Configuring route options" on page 3-14).

RIP policy for propagating updates back to the originating subnet

You can specify a split-horizon or poison-reverse policy for outgoing update packets that include routes received on the same interface on which the update is sent. Split-horizon means that the router does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received, but with a metric of 16 (infinite metric).

The following set of commands specifies the split-horizon policy:

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

admin> set rip-policy = split

admin> write
IP-GLOBAL written
```

RIP triggering

RIP triggering enables the router to tag routes that have been updated in the routing table and send updates that include only the changed routes. The result is reduced processing overhead for both the TAOS router and its neighbors.

With the default value (Yes), the router tags changes to its routing table and includes only the tagged routes in its next update. Changes occur when a call arrives or disconnects, RIP or OSPF learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates five to eight seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions.

If RIP-Trigger is set to No, the router sends full table updates every 20 to 40 seconds. To prevent RIP routers on a network from synchronizing and sending large updates in unison, the full table update is no longer broadcast at fixed 30-second intervals.

Setting the preference value for routes learned from RIP updates

For an introduction to route preferences, see “Setting static-route preferences” on page 2-40. The following command increases the preference value of routes learned from RIP updates, instructing the router to use those routes only if no other routes to the same destination exists:

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

admin> set rip-pref = 150

admin> write
IP-GLOBAL written
```

Poisoning routes to force the use of a redundant TAOS unit

If you have another TAOS unit backing up the TAOS unit in a redundant configuration on the same network, you can set the Dialout-Poison parameter to let the redundant unit take over when necessary. If you set the parameter to Yes, and for any reason the TAOS unit’s trunks experience an alarm condition, the TAOS unit stops advertising IP routes that use dial services. With a setting of No, the unit continues to advertise its dial-out routes, which prevents the redundant unit from taking over the routing load. Set the parameter as follows if you want the TAOS unit to allow a redundant unit to take over.

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

admin> set dialout-poison = yes

admin> write
IP-GLOBAL written
```

Limiting the size of UDP packet queues

When the router is very busy and receives a flood of UDP packets from SNMP requests or RIP updates, a backlog of packets waiting for processing can create enough delay in routing to cause sporadic problems with time-sensitive packets, such as LCP negotiation or Frame Relay management packets.

To prevent such problems, UDP processing runs at a lower priority than processing of routed packets. On a system busily routing packets, this could mean that UDP processing is delayed, and a backlog of UDP packets builds up. The RIP-Queue-Depth parameter in the IP-Global profile and the Queue-Depth parameter in the SNMP profile specify the maximum size of this backlog.

When you set one of these parameters to specify a queue depth, the TAOS unit is more likely to drop UDP packets when it is busy routing packets. However, time-sensitive routed packets are less likely to be delayed and system memory is used more efficiently.

In the following example, the administrator sets both queue depths to 50. Fifty of each type of packet will be held for processing, and if additional packets of either type are received when the queue is full, they will be dropped.

```
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
```

The Netstat command output shows the queue depth of various UDP ports, and the total packets received and total packets dropped on each port. The total packets received count includes dropped packets. In the following example, the SNMP queue depth was set to 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
```

Ignoring default routes when updating the routing table

Ignore-Def-Route prevents routing updates from modifying the default route in the routing table. (This configuration is recommended.) The following set of commands protects the default route from RIP updates:

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

admin> set ignore-def-route = yes

admin> write
IP-GLOBAL written
```

Suppressing host-route advertisements

If you set the Suppress-Host-Routes parameter to Yes, routes are suppressed according to the following rules:

- If a Connection profile includes a subnet mask of less than 32 bits in the Remote-Address setting, host routes for the interface are suppressed while the session is being negotiated, and after the session is established, only network routes are advertised for the interface.
- If a Connection profile includes a subnet mask of /32 in the Remote-Address setting, host routes for the interface are not suppressed. (Pool addresses also have a 32-bit mask, so they are not suppressed.)

The following set of commands configures the router to suppress host routes for connections that specify a subnet mask of less than 32 bits:

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

```
admin> set suppress-host-routes = yes

admin> write
IP-GLOBAL written
```

Setting IP route and IP port cache options

The following parameters (shown with default settings) define how the system handles intrashelf and intershelf routing and route caching:

```
[in IP-GLOBAL]
iproute-cache-enable = yes
iproute-cache-size = 0
ipport-cache-enable = yes
```

Parameter	Specifies
IProute-Cache-Enable	Enable/disable the route cache. If you must control memory usage for a card, you can restrict the cache size or disable the route cache. *Recommended settings are to leave route caches enabled at the default size.*
IProute-Cache-Size	Size of the internal route cache. The default (0) sets no limit on the size of the cache. If you set a higher number, it represents the number of cache entries. Usually, no limit is required.
IPPort-Cache-Enable	Enable/disable card-to-card IP packet forwarding based on the packet destination IP address and port. With the No setting, packets destined for the TAOS unit are routed from the receiving slot card to the destination slot card through the shelf controller, rather than being forwarded directly from the receiving slot card.

Route caches

The global routing table, maintained on the shelf controller, is used to route packets internally to the correct interface. To offload some of the routing overhead and improve performance, the TAOS unit uses route caches on each slot card. Route caches work as follows:

- When a modem or HDLC card receives an IP packet, it forwards the packet to the shelf controller, which routes it to the proper slot, such as an Ethernet card.
- When the shelf controller routes the packet, it writes a cache entry that is downloaded to the route cache of each slot card.
- When the modem or HDLC card receives another IP packet with the same destination address, it checks its route cache and forwards the packet directly to the proper slot, without involving the shelf controller.

The shelf controller retains responsibility for managing routing protocols, the global routing table, and the route caches themselves. But each slot card is able to check a small IP cache and route packets to a destination interface without involving the shelf controller. When a slot card receives an IP packet for which it has no cache entry, it forwards that packet to the shelf controller, which routes the packet and writes a cache entry to all slot cards.

Port caches

Like IP route caches, port caches offload the shelf-controller function by enabling slot cards to manage their own affairs. While route caches enable the cards to look up a destination interface for outbound traffic, port caches enable the cards to route traffic that is directed to the TAOS unit itself, but at a higher protocol layer (for example, the traffic in a TCP-Clear session).

In a TCP-Clear session, for example, a TCP connection is established between a host slot card, such as a modem card, and a local host that is accessible through one of the TAOS unit's Ethernet ports. The modem card creates TCP packets containing the client's data stream and sends them to the server. IP route caching enables the modem card to send the TCP packets directly to the Ethernet card rather than through the shelf controller. However, when the local host returns packets to the dial-in client, there is no IP route cache, because the packet is destined for the TAOS unit itself. So the packets are delivered to the router, which forwards them to the modem card by means of the destination port number.

If the IP-Port-Cache-Enable parameter is set to Yes (the default value), the slot card that receives packets destined for the TAOS unit (an Ethernet card, for example) routes them directly to the destination slot card (such as the modem card) rather than sending them through the shelf controller.

Enabling protocol options

The following parameters (shown with default settings) configure TCP/IP protocol options:

```
[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
```

Parameter	Specifies
BOOTP-Enabled	Enable/disable querying a BOOTP server.
RARP-Enabled	Enable/disable obtaining the system's IP addresses from a RARP server.
UDP-Cksum	Enable/disable UDP checksums.

Parameter	Specifies
TCP-Timeout	Interval for TCP retry attempts. Valid values are from 0 to 200 seconds.
Finger	Enable/disable response to remote Finger queries. When Finger is set to No (the default), the TAOS unit rejects queries from Finger clients and sends a message that the Finger online user list is denied.
BOOTP-Relay:Active	Enable/disable BOOTP Relay.
BOOTP-Relay:BOOTP-Servers[1]	IP address of up to two BOOTP servers. Only one address is required.
BOOTP-Relay:BOOTP-Servers[2]	
SNTP-Info:Enabled	Enable/disable the Simple Network Time Protocol (SNTP).
SNTP-Info:GMT-Offset	Current time zone as an offset from the Universal Time Configuration (UTC). UTC is in the same time zone as Greenwich Mean Time (GMT).
SNTP-Info:Host[1] SNTP-Info:Host[2] SNTP-Info:Host[3]	IP addresses for up to three SNTP servers. Only one address is required.

Enabling Boot Protocol and Reverse ARP

The Boot Protocol (BOOTP) is a UDP/IP-based protocol that enables a host to obtain its configuration dynamically from a BOOTP server. Reverse ARP (RARP) enables a host to obtain its address from a RARP server. The following commands enable both BOOTP and RARP:

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

admin> set bootp-enabled = yes

admin> set rarp-enabled = yes

admin> write
IP-GLOBAL written
```

Enabling UDP checksums

If data integrity is of the highest concern for your network, and redundant checks are important, you can turn on UDP checksums to generate a checksum whenever a UDP packet is transmitted. UDP packets are transmitted for queries and responses related to ATMP, SYSLOG, DNS, ECHOSERV, RADIUS, TACACS, RIP, SNTP, and TFTP.

The following commands enable UDP checksums for transmitted packets:

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

admin> set udp-cksum = yes

admin> write
IP-GLOBAL written
```

Setting a TCP timeout

The TCP-Timeout parameter adjusts the TCP retry timer. At the default value (0), the system attempts a fixed number of retries at escalating intervals adding up to about 170 seconds total. (Other limits in the system terminate TCP retries after about 170 seconds, even if the parameter is set to a higher number.) If you set TCP-Timeout to a nonzero value, the value specifies the number of seconds TCP retries persist. After the specified number of seconds, the retries stop and the connection is considered lost.

TCP-Timeout applies to all TCP connections initiated from the TAOS unit, including Telnet, Rlogin, TCP-Clear, and the TCP portion of DNS queries. The parameter applies to both established TCP connections and initial attempts to connect. A situation in which you might adjust the TCP retry timer would be, for example, when a user employs client software to enter a hostname in a terminal-server session, and DNS returns a list of IP addresses for the host. If the first address proves unreachable and the timeout on each attempt is long, the client software often times out before finding a good address.

The following commands set the timeout to 50 seconds:

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

admin> set tcp-timeout = 50

admin> write
IP-GLOBAL written
```

The optimal setting for the TCP-Timeout parameter depends on the characteristics of the TCP destination (server) hosts, and therefore must be based on experience. For example, if the destinations are all on a LAN under the same administrative control as the TAOS unit and are lightly loaded, a short timeout (such as a few seconds) might be reasonable, because a host that does not respond within that interval is probably down. Conversely, if the environment includes servers with longer network latency times (for example, those connected across the WAN), or load is high in the network or the router, or the characteristics of the remote hosts are not well-known, a longer timeout is appropriate. Values of 30 to 60 seconds are common in UNIX TCP implementations.

Enabling response to Finger queries

If Finger (described in RFC 1288) is enabled in the IP-Global profile, the TAOS unit can return user information to a remote Finger query. The following commands enable the TAOS unit to accept Finger queries and return the requested active session details to a remote client:

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

admin> set finger = yes

admin> write
IP-GLOBAL written
```

When the Finger parameter is set to Yes, a client (such as a UNIX client) can request session information for the system named TAOS1 by entering the following command:

```
# finger @taos1
```

The above command displays the information in narrow (80-character-wide) format. The client can request the information in wide format by using the command with the `–l` option. For example, the following command:

```
# finger -l @taos1
```

displays a wide (140-character-wide) format of session information for the system named TAOS1. The client can also request the details of all sessions or of a single session. For example, the following command would request information about a single user named Gavin:

```
# finger gavin@taos1
```

The Finger forwarding service is not supported. It uses the following hostname format:

`@host1@host2`

A remote client that uses the forwarding request format receives the following message:

```
Finger forwarding service denied.
```

Enabling BOOTP-Relay

If a host requesting an address does not reside on the same IP network as a BOOTP server, an intervening system is required to transfer messages between the client and server. The intervening host is a BOOTP Relay Agent.

The following commands enable the BOOTP Relay feature and specify the address of a BOOTP server:

```
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
```

If more than one server is specified, the TAOS unit uses the first server until it becomes unavailable. Once the unit starts using the second server, the unit continues using that server until it becomes unavailable, at which time the unit switches back to using the first server again.

Using SNTP to set and maintain the system time

The TAOS unit can use Simple Network Time Protocol (SNTP), which is described in RFC 1305, to set and maintain its system time by communicating with an SNTP server.

You specify the system’s time zone as an offset from the Universal Time Configuration (UTC). UTC is in the same time zone as Greenwich Mean Time (GMT). The offset specifies hours and minutes from UTC, using a 24-hour clock. Because some time zones, such as Newfoundland, do not have an even hour boundary, the offset includes four digits and requires half-hour increments.

For example, in Newfoundland the time is 1.5 hours earlier than UTC, so the offset is UTC-0130. For San Francisco, which is 8 hours earlier than UTC, the offset is UTC -0800. For Frankfurt, which is 1 hour later than UTC, the offset is UTC +0100.

The commands in the following example specify the time zone for San Francisco and the address of one SNTP server:

```
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
```

The TAOS unit always communicates with the first address unless it is inaccessible. In that case, the unit attempts to communicate with the second address, trying the third address only if the other two are inaccessible.

Configuring port redirection

Port redirection enables you to configure a Connection or RADIUS profile to redirect certain packet types to a specified server. For example, you could redirect Hypertext Transfer Protocol (HTTP) traffic to a Web cache server on a local network. However, port redirection is not limited to HTTP traffic. You can use the feature to redirect any TCP or UDP packet on the basis of its protocol and port information.

Overview of Connection profile settings

To configure port redirection in a Connection profile, set the following parameters (shown with default settings):

```
[in CONNECTION/"":port-redirect-options]
protocol = none
port-number = 0
redirect-address = 0.0.0.0
```

Parameter	Specifies
Protocol	Protocol type. Valid settings are `none` (the default, which disables port redirection), `udp`, and `tcp`. The specified setting, together with the Port-Number setting, defines a type of packet. For example, `tcp` with `21` represents FTP traffic, and `tcp` with `23` represents Telnet traffic. For HTTP traffic, set the parameter to `tcp`.

Parameter	Specifies
Port-Number	Port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For example, HTTP traffic uses TCP port 80. For a list of assigned port numbers, see RFC 1700, *Assigned Numbers*.
Redirect-Address	IP address to which matching packets are redirected.

Overview of RADIUS settings

RADIUS uses the following attribute-value pairs for port redirection:

RADIUS Attribute	Specifies
Ascend-Port-Redir-Protocol (82)	Protocol type. Valid values are `Ascend-Proto-TCP (6)` and `Ascend-Proto-UDP (17).` The specified value, together with the Ascend-Port-Redir-Portnum value defines a type of packet. For example, `Ascend-Proto-TCP` with `21` represents FTP traffic, and `Ascend-Proto-TCP` with 23 represents Telnet traffic. For HTTP traffic, specify `Ascend-Proto-TCP (6)`.
Ascend-Port-Redir-Portnum (83)	Port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For example, HTTP traffic uses TCP port 80. For a list of assigned port numbers, see RFC 1700, *Assigned Numbers*.
Ascend-Port-Redir-Server (84)	IP address to which matching packets are redirected.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

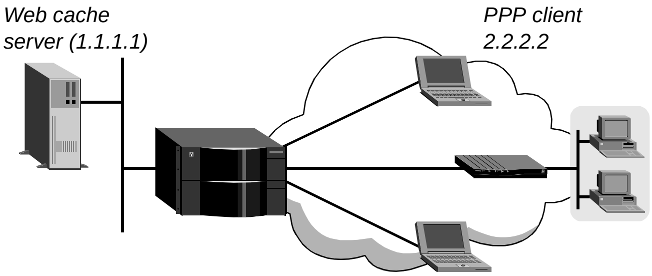
```
[in EXTERNAL-AUTH]
auth-type = radius

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

For details about these settings, see the *APX 8000/MAX TNT Reference.*

Example of configuring port redirection

In this example, the TAOS unit redirects a PPP client's browser requests to a Web cache server at 1.1.1.1. The Web cache server can respond directly if a cached entry is found, or forward the browser request to its original destination if no cache entry is found. The sample setup is shown in Figure 2-9.

Figure 2-9. Port redirection to an HTTP server



The following commands configure a local profile for the PPP client, redirecting its HTTP traffic to the server at 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
```

Following is a comparable RADIUS profile:

```
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
```

Configuring DNS

Domain Name System (DNS) is a TCP/IP service for centralized management of address resolution. Service providers can maintain multiple DNS servers, each one dedicated to a particular client or location. In that case, it might be important for security reasons to ensure that connections are always directed to the correct DNS service. With per-connection DNS access, a service provider can direct specific users to the DNS servers appropriate to their services or locations.

In the TAOS unit, DNS configuration includes settings for enabling local DNS lookups and supporting DNS list, settings for a local DNS table maintained in RAM, and client DNS for directing connections to a particular DNS service.

Configuring DNS lookups and a DNS list

Following are the parameters (shown with default settings) for configuring DNS to allow lookups and support a DNS list:

```
[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 = ""
```

Parameter	Specifies
Domain-Name	Primary domain name to use for DNS lookups. The TAOS unit appends this domain name to hostnames when performing lookups.
DNS-Primary-Server	Address of the primary local DNS server to use for lookups.
DNS-Secondary-Server	Address of the secondary local DNS server to use for lookups. Used only if the primary server is not found.
NetBIOS-Primary-NS NetBIOS-Secondary-NS	Addresses of a primary and secondary NetBIOS server.
DNS-List-Attempt	Enable/disable a DNS list.
DNS-List-Size	Maximum number of hosts in a DNS list, up to 35.
Sec-Domain-Name	Secondary domain name to use for DNS lookups if the hostname is not found in the primary domain.

Specifying domain names for lookups

When the TAOS unit receives a hostname to look up, it tries various combinations, including appending the domain name specified in the IP-Global profile. The following commands specify a primary and secondary domain name for DNS lookups:

```
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
```

If a lookup fails with the first domain name, the router tries again with the secondary domain name.

Specifying local DNS server addresses

To enable the TAOS unit to look up addresses via DNS, specify DNS server addresses as shown in the following example:

```
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
```

If the primary server is unavailable, the TAOS unit attempts a lookup on the secondary server. To execute a lookup manually, use the Nslookup command. For example:

```
admin> nslookup techpubs
Resolving host techpubs.
IP address for host techpubs is 10.6.212.19.
```

Local DNS servers provide information about the local network, and are sometimes isolated from incoming callers for security purposes. For details, see “Using client DNS” on page 2-58.

Supporting DNS list

Some DNS servers support a list feature that enables them to return multiple addresses for a hostname in response to a DNS query. However, the responses do not include information about availability of the hosts in the list. Users typically attempt to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth.

When the DNS list is used for an immediate connection by a dial-in user (for example, an immediate Telnet connection to a local host), and the first attempt fails, the physical connection is torn down. To avoid tearing down and then reestablishing the connection before attempting to access the next host in the list, enable the DNS list feature. The following example shows how to enable DNS list with a maximum of 14 hosts in the list:

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

admin> set dns-list-attempt = yes

admin> set dns-list-size = 14

admin> write
IP-GLOBAL written
```

For related information, see “Using the Auto-Update feature” on page 2-57.

Setting up a local DNS table

The TAOS unit can maintain in RAM a DNS table of up to eight hostnames and their IP addresses. It consults the table in RAM for address resolution only if requests to the DNS server fail. The local table acts as a safeguard to ensure that the TAOS unit can resolve the local set of DNS names even if all DNS servers become unreachable or go down.

The local DNS table is propagated to RAM from a configured DNS-Local-Table subprofile in the IP-Global profile. At startup, the system copies values in the profile to the table in RAM. If you subsequently modify the DNS-Local-Table subprofile, the changes are propagated to the table in RAM when the profile is written.

The DNS table in RAM has space for up to 35 IP addresses per Host-Name entry (35 is the maximum setting for DNS-List-Size). The DNS-Local-Table subprofile allows a single IP address per hostname. (For related information, see “Using the Auto-Update feature” on page 2-57.)

To set up the local DNS table, configure the following parameters (shown with their default values) in the IP-Global profile:

```
[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
```

DNS-Local Table Parameter	**Specifies**
Enabled	Whether the local DNS table in RAM will be available if DNS queries fail. With a setting of No (the default), if a DNS query times out, the request fails. With a setting of Yes, the TAOS unit attempts to resolve the query by consulting the DNS table in RAM. If the hostname in the DNS query has an entry in the table in RAM, the system returns the associated IP address(es) to the requester.
Auto-Update	Whether regular successful DNS queries update the local DNS table. For details about Auto-Update, see “Using the Auto-Update feature” on page 2-57.
Table-Config[1–8]	An array of up to eight hostnames and IP addresses for inclusion in the local DNS table.
Table-Config Host-Name	A hostname, which must be unique within the table and meet the requirements described in “Hostname matching” on page 2-56.
Table-Config IP-Address	A valid IP address for the Host-Name setting, or the zero address. If Auto-Update is enabled and IP-Address specifies the default zero address, successful DNS queries will gradually build the local table.

Hostname matching

A hostname in the local DNS table must start with an alphabetic character and must have fewer than 256 characters. Trailing periods are ignored in the comparison.

The name can be a hostname or a fully qualified domain name. If the name does not include a domain name, and you have specified one or more Domain-Name settings, the system appends the specified domain name when looking up the hostname. For example, if you have entered the settings shown in "Specifying domain names for lookups" on page 2-53, a DNS query for hostname `wheelers` results in a search for the following fully qualified domain names:

```
wheelers.eng.abc.com

wheelers.abc.com
```

Defining the local table

Following is an example of configuring a local table that specifies three 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
```

If you specify an IP address without also specifying a hostname, a message such as the following appears when you write the profile:

```
error: dns-local-table: host-name missing (#3 1.2.3.4)
```

If you enter an invalid hostname, a message such as the following appears when you write the profile:

```
error: dns-local-table: host-name must start with alpha char (#5
11foo)
```

Using the Auto-Update feature

If the Auto-Update parameter is set to No (the default), successful DNS queries do not affect the contents of the local table. With a setting of Yes, when a regular DNS query succeeds, the system performs a lookup on that hostname in the local table. If there is an entry for the hostname, the entry's IP address(es) is (are) replaced by the query response. The number of addresses added to the table depends on the DNS-List-Attempt and DNS-List-Size settings. If DNS-List-Attempt is set to No, a successful DNS query returns a single address for a given hostname. In the DNS table in RAM, that address is stored and the remaining 34 addresses are cleared (set to zero).

If DNS-List-Attempt is set to Yes, a successful DNS query returns the number of addresses it finds for the host, up to the value of DNS-List-Size. In the DNS table in RAM, those addresses are stored, overwriting the configured address or the addresses retrieved from earlier DNS queries. If the table in RAM contains more addresses than DNS-List-Size specifies, the excess addresses are cleared at each update to prevent the accumulation of stale addresses.

Note: If you modify the DNS-Local-Table subprofile, assigning a single address to a host, the newly configured address is propagated to the table in RAM. The first address of the Host-Name entry is overwritten with the configured address, and all remaining addresses are cleared. If the Auto-Update parameter is set to Yes, the next successful DNS query overwrites the configured address and restores the multiple addresses (up to DNS-List-Size).

In the following example, an administrator configures eight hostnames with null addresses and then sets Auto-Update to Yes. The changes to DNS-Local-Table will be propagated to RAM, and successful DNS queries to the specified hostnames will build the local table with up to 14 addresses for each of the hosts.

```
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
```

Using client DNS

Client DNS specifies particular servers for dial-in clients. ISPs use client DNS to direct callers to servers belonging to particular locations or customers, and to prevent those callers from accessing other clients' host information.

Client DNS can be specified systemwide to allow all dial-in clients to access one or two DNS servers. Or it can be configured on a connection basis, to allow each appropriately configured connection to access one or two specific servers. At the system level, client DNS also provides an exit mechanism to the local servers if the client servers are inaccessible.

The addresses configured for client DNS servers are presented to WAN connections during IPCP negotiation.

Overview of client DNS settings

You can configure client DNS at the system level in the IP-Global profile. At the connection level, you can specify client DNS servers in Connection or RADIUS profiles.

Settings in the IP-Global profile

The following parameters (shown with default values) specify client DNS at the system level:

```
[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
```

Parameter	Specifies
Client-DNS-Primary-Server	Address of a client DNS server for dial-in clients.
Client-DNS-Secondary-Server	Address of a secondary DNS server for dial-in clients.

Parameter	Specifies
Allow-As-Client-DNS-Info	Enable/disable an exit mechanism to local servers if the client DNS servers are not found. To isolate local network information, set to False.

Settings in Connection profiles

The following parameters (shown with default settings) specify client DNS at the connection level:

```
[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
```

Parameter	Specifies
Client-DNS-Primary-Addr	Address of a client DNS server for the connection.
Client-DNS-Secondary-Addr	Address of a secondary client DNS server for the connection.
Client-DNS-Addr-Assign	Enable/disable client DNS for the connection. With the Yes setting (the default), the system presents client DNS server addresses while negotiating the connection. The addresses it presents can be specified in the Connection profile or IP-Global profile.

Settings in a RADIUS profile

The following attribute-value pairs configure client DNS in RADIUS profiles:

RADIUS Attribute	Value
Ascend-Client-Primary-DNS (135)	Address of a client DNS server for the connection.
Ascend-Client-Secondary-DNS (136)	Address of a secondary client DNS server for the connection.
Ascend-Client-Assign-DNS (137)	Enable/disable client DNS for the connection. With the DNS-Assign-Yes (1) value, the system presents client DNS server addresses while negotiating the connection. The addresses it presents can be specified in the RADIUS profile or IP-Global profile.

Example of configuring client DNS servers at the system level

The following commands configure client DNS servers at the system level:

```
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
```

The secondary server is accessed only if the primary one is inaccessible. If neigher of these client DNS servers is accessible and the caller's profile does not specify client DNS servers, the TAOS unit does *not* allow the client to access local DNS servers.

Examples of configuring client DNS at the connection level

The following commands identify two DNS servers for this connection. The secondary server is accessed only if the primary one is inaccessible.

```
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
```

Following are comparable settings in a RADIUS profile:

```
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
```

Configuring Microsoft WINS assignment

In the current software version, you can specify a primary and secondary Windows Internet Name Service (WINS) server on a per-connection basis, either in local Connection profiles or in RADIUS.

In previous releases, the unit allowed systemwide configuration of a primary and secondary NetBIOS WINS server, to support WINS name resolution for machines connected to a NetBIOS network.

Note: The PC dialing in must have the Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings for this feature to work.

Settings in a Connection profile

Following are the local parameters (shown with default settings) for configuring client WINS servers:

```
[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
```

Parameter	Specifies
Client-WINS-Primary-Addr	Address of a client WINS server for the connection.
Client-WINS-Secondary-Addr	Address of a secondary client WINS server for the connection.
Client-WINS-Addr-Assign	Enable/disable client WINS for the connection. With the Yes setting (the default), the system presents client WINS server addresses while negotiating the connection.

For more details about these parameters, see the *TAOS RADIUS Guide and Reference*. For information about specifying NetBIOS servers in the IP-Global profile, see “Configuring DNS lookups and a DNS list” on page 2-53.

Settings in a RADIUS profile

The following attribute-value pairs configure client WINS servers in RADIUS profiles:

RADIUS attribute	Value
Ascend-Client-Primary-WINS (78)	Address of a client WINS server for the connection.
Ascend-Client-Secondary-WINS (79)	Address of a secondary client WINS server for the connection.
Ascend-Client-Assign-WINS (80)	Enable/disable the use of client WINS servers for the connection. With the WINS-Assign-Yes (1) value, the system presents client WINS server addresses while negotiating the connection.

For more details about these attributes, see the *TAOS RADIUS Guide and Reference*.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

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

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

For details about these settings, see the *APX 8000/MAX TNT Reference* that came with your unit.

Examples of configuring client WINS servers

The following commands identify two WINS servers for a configured connection. The secondary server is accessed only if the primary one is inaccessible.

```
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
```

Following are comparable settings in a RADIUS profile:

```
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
```

Configuring and using address pools

An address pool is a range of contiguous addresses on a local IP network or subnet. Pool addresses are available for assignment to incoming callers that request an address. When the call terminates, the address is returned to the pool, making it available again for assignment.

If you designate a subnet for IP address pools, you must make sure that other IP hosts on the local network know the route to that subnet. You must also make sure that the pools do not overlap (do not contain duplicate addresses).

For related information, see “Defining address pools for a VRouter” on page 6-6.

Overview of settings for defining pools

You can define up to 128 address pools locally in the IP-Global profile. Those pools can be used to assign addresses to callers authenticated locally (in Connection profiles) or by RADIUS. If you are using RADIUS authentication, you can choose to define address pools in RADIUS instead of, or in addition to, those defined locally. If you have the RADIPAD program installed, you can use it to manage address pools centrally on a single RADIUS server.

Settings in the IP-Global profiles

The following parameters (shown with default values) configure address pools locally:

```
[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 0 0+
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""+
```

Parameter	**Specifies**
Pool-Summary	Set/clear the Pool Summary flag. For details, see “Example of configuring summarized address pools” on page 2-66.
Pool-OSPF-Adv-Type	OSPF option. For details, see “Configuring route options” on page 3-14.

Parameter	**Specifies**
Pool-Base-Address	Base address of a pool of contiguous addresses on a local network or subnet.
Assign-Count	Number of addresses in the pool.
Pool-Name	A pool name, required only when TACACS+ authentication is in use. If TACACS+ authentication is not in use, the name is treated as a comment.

Settings in RADIUS pseudo-user profiles

You can define address pools in a RADIUS `pools` pseudo-user profile. The first line of `pools` pseudo-user profile uses the following format:

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

The *name* argument is the TAOS unit's system name (specified by the Name parameter in the System profile). Subsequent lines in the profile define IP address pools by using the Ascend-IP-Pool-Definition (217) attribute. The value of the Ascend-IP-Pool-Definition attribute uses the following syntax:

```
"pool-num base-addr assign-count"
```

Syntax element	**Description**
`pool-num`	Pool number. If you use the same number to designate two pools, one locally and one in RADIUS, the RADIUS definition takes precedence. So if you have defined some pools in the IP-Global profile and do not wish to override them, start numbering the pools at the next number. For example, if you defined 10 pools in the IP-Global profile, start with number 11 in RADIUS. Otherwise, start with 1.
`base-addr`	The base address in a pool of contiguous addresses on the local network or subnet.
`assign-count`	Number of addresses included in the pool.

Global RADIUS pools (RADIPAD)

RADIUS IP Address Daemon (RADIPAD) is a program that works with RADIUS authentication to manage IP address pools centrally, so that connections can all acquire an address from a global pool, regardless of which system answers the call.

RADIPAD runs on one RADIUS server on the network. A TAOS unit sends an authentication request to RADIUS, and if the user profile contains an attribute to allocate an IP address from the global pool, RADIUS sends a request to RADIPAD to acquire the address.

The TAOS unit does not talk directly to RADIPAD, so it does not require additional configuration to use RADIPAD. To configure RADIPAD, you define the global pools of addresses, specify which RADIUS server is running RADIPAD, and (optionally) specify which TAOS unit can obtain addresses from those pools. You can then create RADIUS user profiles that acquire an IP address from the global pool.

At startup, Syslog notes RADIUS requests to release RADIUS-allocated IP addresses. Some versions of the RADIUS server might time out the request, resulting in log messages indicating the release of global-pool addresses.

Defining global pools

Global address pools are defined in a `global-pools` pseudo-user profile on the server running RADIPAD. The first line of a `global-pools` pseudo-user profile uses the following format:

```
global-pools-name Password = "ascend", Service-Type = Outbound-User
```

The *name* argument is a designation for any class of users. You can create multiple global pool profiles for multiple user classes. For example, you could create profiles named Global-Pool-PPP, Global-Pool-SLIP, and so forth. Subsequent lines in the profile define IP address pools by using the Ascend-IP-Pool-Definition (217) attribute. This is the same attribute described in “Settings in RADIUS pseudo-user profiles” on page 2-63, and it follows the same rules for global pools. In addition, when the TAOS unit assigns an address from a pool managed by the RADIPAD daemon, RADIPAD tries to allocate an address from the pools in order, by pool number, and chooses an address from the first pool with an available IP address.

Specifying the RADIPAD host

Each RADIUS server must specify the host running RADIPAD and (optionally) the TAOS units that can access the global pools. These settings are defined in a `radipa-hosts` pseudo-user profile, which uses the following format in the first line of the profile:

```
radipa-hosts Password = "ascend", Service-Type = Outbound-User
```

Subsequent lines in the profile use the following attribute value pairs to define which TAOS units can assign addresses from the pools managed by RADIPAD:

RADIUS Attribute	Value
Ascend-Assign-IP-Client (144)	Address of a TAOS unit that is allowed to access the global address pools managed by RADIPAD. You can specify multiple instances of this attribute. If no client addresses are specified, all units listed in the RADIUS clients file can access RADIPAD pools.
Ascend-Assign-IP-Server (145)	Address of the server running RADIPAD. Only one instance of this attribute can appear in the profile, and it must specify the correct IP address.

For example:

```
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
```

You can specify only one RADIPAD server, but you can include multiple clients. The sample profile indicates that two TAOS units (10.31.4.10 and 10.31.4.11) can access RADIPAD pools as clients.

Preventing the use of class boundary addresses

If you define address pools that contain more than 254 addresses, be aware that the system allocates the class boundary addresses (x.y.z.0 and x.y.z.255) as valid caller addresses. According to CIDR, this is permitted because the pool is not a /24 network. However, some client systems, such as Windows, do not tolerate the class boundary addresses well. For example, because Windows assumes a /24 network, it broadcasts NetBIOS over IP name service to the .255 address, which could swamp a connection assigned the .255 host address.

To prevent client software from using a host address for broadcasts, you must explicitly apply a filter that prevents the system from using the class boundary addresses. For example, if you are using RADIUS authentication, you can apply a data filter, in the Answer-Defaults profile, that drops packets from any source to pool address x.y.z.0 or x.y.z.255.

Examples of configuring address pools

For a pool that is not summarized, each assigned address is advertised as its own host route. Such a pool can start at any base address. Addresses do not accept a subnet mask component, because they are always advertised as host routes.

The following commands define three address pools, each containing 50 addresses. Pool 1 contains 10.2.3.4 through 10.2.3.54. Pool 2 contains 11.5.7.51 through 11.5.7.101. Pool 3 contains 12.7.112.15 through 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
```

Following is a comparable RADIUS `pools` profile (for use by a single RADIUS server):

```
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"
```

Following is a comparable global pools definition (for use with 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"
```

Although some client software assumes a default subnet mask of 255.255.255.0 for PPP interfaces, you can define pools on submets wider than /24. For example, the following commands define an address pool on a /23 subnet:

```
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
```

This pool definition translates to 10.55.178.0/23 (a subnet mask of 255.255.254.0). Following are comparable RADIUS definitions:

```
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"
```

Example of configuring summarized address pools

The Pool-Summary feature reduces routing overhead associated with address pools. Instead of advertising each address assigned from a pool as a host route, the TAOS unit suppresses the host route advertisements and instead advertises a static route to the pool itself.

To use summarized pools locally or in RADIUS, you must set the Pool-Summary flag to Yes in the IP-Global profile. When Pool-Summary is set to Yes, all pools should be network-aligned.

Setting the Pool-Summary flag

The following commands enable the Pool-Summary flag:

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

admin> set pool-summary = yes

admin> write
IP-GLOBAL written
```

Defining network-aligned pools

Following are the rules for network-aligned address pools:

- The specified number of addresses in the pool must be two less than the total number of addresses in the pool. (Add 2 to the Assign-Count value for the total number of addresses in the subnet, and calculate the mask for the subnet on the basis of this total.)

  `assign-count` + 2 = number of subnet hosts

- The specified base address of the pool must be the first host address. (Subtract 1 from the Pool-Base-Address value for the base address for the subnet.)

  `pool-base-address` - 1 = network-aligned subnet address

The following commands enable the Pool-Summary flag and define a network-aligned pool:

```
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
```

In the preceding sample configurations, the Assign-Count parameter is set to 62. When you add 2 to this value, you get 64. The subnet mask for 64 addresses is 255.255.255.192 (256–64 = 192). The prefix length for a 255.255.255.192 mask is /26.

The Pool-Base-Address parameter is set to 10.12.253.1. When you subtract 1 from this value, you get 10.12.253.0, which is a valid network-aligned base address for the 255.255.255.192 subnet mask. (Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same mask.) The resulting address pool subnet is 10.12.253.0/26.

Following is a comparable RADIUS pools profile (for use by a single RADIUS server):

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User
   Ascend-IP-Pool-Definition = "1 10.12.253.1 62"
```

Following is a comparable global pools definition (for use with RADIPAD):

```
global-pool-ppp Password ="ascend", Service-Type = Outbound-User
   Ascend-IP-Pool-Definition = "1 10.12.253.1 62"
```

The TAOS unit still creates (but does not advertise) a host route for each assigned address in the pool. Host routes take precedence over subnet routes, so packets whose destination matches an assigned IP address from the pool are routed properly. However, because the TAOS unit advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network might improperly send the TAOS unit a packet for an inactive IP address. If that occurs, the packets are routed to the Reject (rj0) interface (127.0.0.2). Packets routed to the Reject interface are bounced back to the sender with an `ICMP unreachable` message.

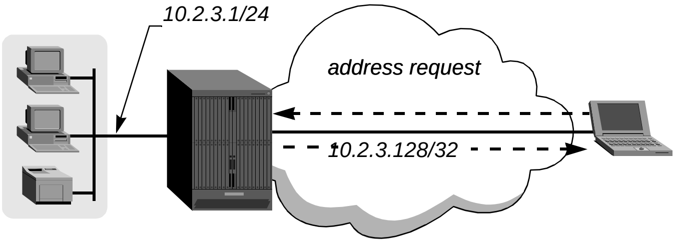
Examples of assigning an address from a pool

When an incoming call requests an IP address, the TAOS unit assigns one from a pool. A host requests an address if its client software has settings such as the following:

```
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
```

Figure 2-10 shows a dial-in host requesting and being assigned an IP address.

Figure 2-10. Dial-in host requiring assigned IP address



The following commands enable dynamic address assignment systemwide:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ip-answer assign = yes

admin> write
ANSWER-DEFAULTS written
```

For information about ensuring that connections must accept the address offered, see “Requiring acceptance of dynamic address assignment” on page 2-37.

The following commands configure a profile to acquire an address from the first pool that has available addresses:

```
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
```

Following is a comparable RADIUS profile:

```
victor Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 0
```

Following is a comparable RADIUS profile that acquires an address from any global pool managed by the RADIPAD daemon:

```
victor Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 65535
   Ascend-Assign-IP-Global-Pool = "global-pool-ppp"
```

IP pool chaining

Because the addresses within a pool must be contiguous, many sites have defined a large number of pools, with each pool containing only a small range of addresses. For example, the following RADIUS profile defines six pools, each containing 10 addresses:

```
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"
```

In earlier versions of the software, you could allow a caller to acquire an address from any pool (by assigning the pool number 0 in the caller’s profile) or from a single specified pool, such as pool 1. IP pool chaining enables you to allow a caller to acquire an address from any pool within a chain.

When IP pool chaining is enabled, contiguous pools are treated as one *pool space* with shared addresses. When the system assigns an address to an end user, it begins searching for an available address in the first pool of the chain and stops when it either finds an available address or encounters a null pool definition. So, the pools within a chain must be defined in a contiguous sequence. For example, the following profile contains two IP pool chains (pools 1, 2, 3 and pools 7, 8, 9), with each pool chain containing 30 addresses:

```
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"
```

Note: To support IP pool chaining in RADIUS profiles, the RADIUS server must support vendor-specific attributes (VSA) and the TAOS unit must be configured in VSA compatibility mode. For details, see “Pool chaining in RADIUS” on page 2-71.

IP pool chaining is supported both for RADIUS-defined address pools and for pools defined locally in the IP-Global profile. For example, the following settings in the IP-Global profile enable pool chaining and define a pool chain (pools 1 and 2) that contains 252 addresses:

```
[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 0 0+
```

Pool chaining in local profiles

Whether pool chains are defined locally or in RADIUS, the pool addresses are available for dynamic assignment regardless of where the caller’s profile is authenticated.

Overview of local profile settings

Following are the parameters, shown with default settings, relevant to IP pool chaining:

```
[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 0 0 0+
```

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

Parameter	Specifies
Pool-Chaining	Enable/disable IP pool chaining. With the `yes` setting, the system treats contiguous IP address pools as a single extended pool space when searching for an available address to assign to a caller.
Pool-Base-Address	An array of up to 128 IP addresses to be used as the first address in a pool. These values are used with the Assign-Count values to define address pools locally. A pool chain contains all of the pools defined in sequence within the array, such as 1, 2, 3. To end a pool chain, leave a null value in the array.
Assign-Count	An array of up to 128 numbers that specify the number of addresses in a pool that starts with the corresponding Pool-Base-Address.
Address-Pool	Number of an address pool from which to acquire an address. When pool chaining is enabled, a pool number within a chain includes addresses defined in all other pools within the chain. For example, if pools 1, 2, and 3 are in a pool chain, setting this parameter to `1` has the same effect as setting it to `2` or `3`.

Example of local pool chain definition

The following commands define five address pools, which form two pool chains. Notice that the pool numbers (their indexes in the Pool-Base-Address and Assign-Count arrays) are contiguous within a chain.

```
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
```

The following commands enable dynamic address assignment systemwide:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ip-answer assign = yes

admin> write
ANSWER-DEFAULTS written
```

The following commands configure profiles to acquire an address from the first pool chain. When the end users dial in, they can acquire an address from 10.1.1.1 to 10.1.1.51, from 11.1.1.1 to 11.1.1.51, or from 12.1.1.1 to 12.1.1.51. If no addresses are available within those ranges, the connection is refused.

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

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp-options recv-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 recv-password = localpw

admin> set ip-options address-pool = 1

admin> write
CONNECTION/ravi written
```

Following are comparable RADIUS profiles:

```
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
```

Pool chaining in RADIUS

Whether pool chains are defined locally or in a RADIUS pool’s pseudo-user profile, the pool addresses are available for dynamic assignment regardless of where the caller’s profile is authenticated.

Overview of RADIUS profile settings

RADIUS servers use the following attribute-value pairs to define and apply pool chains:

RADIUS Attribute	Value
Ascend-IP-Pool-Chaining (85)	Enable/disable IP pool chaining in a pseudo-user profile that defines address pools. If this attribute is set to `IP-Pool-Chaining-Yes (1)`, the system treats contiguous IP address pools as a single extended pool space when searching for an available address to assign to a caller. With a value of `IP-Pool-Chaining-No (0)`, the system treats each address pool as a separate space. **Note:** When this attribute is specified in a RADIUS profile, its value overrides the Pool-Chaining setting in the IP-Global profile.
Ascend-IP-Pool-Definition (217)	Address pool definition in a pseudo-user profile. The value has the following syntax: *`pool-number base-addr assign-count`* The *`pool-number`* value is an integer that identifies the pool. A pool chain contains all of the pools defined in sequence, such as 1, 2, 3. To end a pool chain, leave a gap in the sequence of *`pool-number`* values. The *`base-addr`* value is an IP address to be used as the first address in a pool, and the *`assign-count`* value specifies the number of addresses in a pool.
Ascend-Assign-IP-Pool (218)	Number of the address pool from which the RADIUS user profile should acquire an address. When pool chaining is enabled, a pool number within a chain includes addresses defined in all other pools within the chain. For example, if pools 1, 2, and 3 are in a pool chain, setting this value to 1 has the same effect as setting it to 2 or 3.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

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

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

For details about these settings, see the *APX 8000/MAX TNT Reference*.

Example of pool chaining in RADIUS

The following pseudo-user profile defines five address pools, which form two pool chains. Notice that the pool numbers are contiguous within a chain.

```
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"
```

The following commands configure local Connection profiles to acquire an address from the first pool chain. When the end users dial in, they can acquire an address from 13.1.1.1 to 13.1.1.51, or from 14.1.1.1 to 14.1.1.51. If no addresses are available within those ranges, the connection is refused.

```
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
```

Following are comparable RADIUS user profiles:

```
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
```

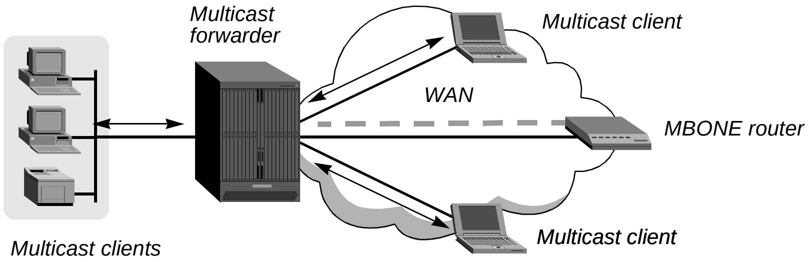
Setting up multicast forwarding

The IP Multicast Backbone (MBONE) provides one-to-many and many-to-many communication, rather than the point-to-point communication used by many other types of network applications. Video and audio transmissions use the MBONE as a much cheaper and faster way to communicate the same information to multiple hosts.

MBONE routers maintain multicast groups, in which hosts must register to receive a multicast transmission. Multicast group functions are handled with the Internet Group Management Protocol (IGMP). The TAOS unit forwards IGMP version-1 or version-2 packets, including IGMP MTRACE (multicast trace).

Figure 2-11 shows a TAOS unit forwarding multicast traffic from an MBONE router across the WAN to two WAN multicast client interfaces and a LAN multicast client interface.

Figure 2-11. TAOS unit forwarding multicast traffic to LAN and WAN clients



The interface to the MBONE router is the MBONE interface. The TAOS unit can have one and only one MBONE interface, which can be either a LAN or WAN IP interface.

To MBONE routers, the TAOS unit appears to be a multicast client, because it responds as a client to IGMP packets. To multicast clients, the TAOS unit appears to be an MBONE router, because it forwards IGMP queries to those clients, receives their responses, and forwards multicast traffic.

Global settings for enabling multicast forwarding

The following parameters (shown with default settings) initiate multicast forwarding at the system level:

```
[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
```

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Parameter	Specifies
Multicast-Forwarding	Enable/disable multicast forwarding in the TAOS unit. When you change the value to Yes and write the profile, the multicast subsystem reads the values in the IP-Global profile and initiates the forwarding function.
MBONE-Profile	Name of a local Connection profile for an MBONE router on a WAN interface. This paremeter and the MBONE-LAN-Interface parameter are mutually exclusive. For details, see “Configuring the MBONE interface” on page 2-77.

Parameter	Specifies
MBONE-LAN-Interface	Interface address (shelf, slot, and port) to MBONE router on a LAN interface. This paremeter and the MBONE-Profile parameter are mutually exclusive. For details, see "Configuring the MBONE interface" on page 2-77.
Multicast-Hbeat-Addr	Multicast address to be monitored for determining a minimal level of traffic (heartbeat).
Multicast-Hbeat-Port	UDP port number to be monitored. The TAOS unit counts only packets received on this port.
Multicast-Hbeat-Slot-Time	Polling interval (in seconds) during which the TAOS unit polls for multicast traffic.
Multicast-Hbeat-Number-Slot	Number of times to poll for the specified interval before comparing the number of heartbeat packets received to the alarmthreshold.
Multicast-Hbeat-Src-Addr	Source IP address to be ignored. Packets received from that address are ignored for heartbeat monitoring purposes.
Multicast-Hbeat-Src-Addr-Mask	Subnet mask to be applied to Multicast-Hbeat-Src-Addr value before comparing it to the source address in a packet.
Multicast-Hbeat-Alarm-Threshold	Number of packets that represents normal multicast traffic. If the number of monitored packets falls below this number, the SNMP alarm trap is sent.
Multicast-Member-Timeout	Timeout (in seconds) for client responses to multicast polling messages. If it does not receive responses on a client interface in the specified number of seconds, the TAOS unit stops forwarding multicast traffic on the interface.

Specifying a timeout for group memberships

The Multicast-Member-Timeout parameter specifies the timeout (in seconds) for client responses to multicast polling messages. If no client responds to the polling messages within the amount of time you specify for Multicast-Member-Timeout, the TAOS unit stops forwarding multicast traffic on the interface. The following commands set the timeout value to 60 seconds:

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

admin> set multicast-member-timeout = 60

admin> write
IP-GLOBAL written
```

Monitoring the multicast traffic heartbeat

Heartbeat monitoring is optional. It enables administrators to monitor possible multicast connectivity problems by continuously polling for a certain level of multicast traffic and generating the following SNMP alarm trap in the event of a traffic breakdown:

```
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).
```

Enabling heartbeat monitoring

To enable multicast heartbeat monitoring, you specify a polling frequency and the threshold below which the alarm is generated.

With the following sample configuration, the TAOS unit polls 10 times at 10-second intervals and then compares the total traffic count to the threshold value. If fewer than 30 packets have been received, the unit generates the SNMP alarm.

```
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
```

Specifying which packets to monitor

To fine-tune heartbeat monitoring, you can specify which packets the system should count as multicast traffic. You can do this in one or more of the following ways:

- Specify a particular multicast address to be used for monitoring.
- Specify a UDP port number (all packets received on that port will be used for monitoring).
- Specify a source address (all packets from that host will be ignored for monitoring purposes).
- Specify a subnet mask to be applied to the source address (all packets from the subnet or network will be ignored for monitoring purposes).

The following example shows how to monitor only packets forwarded to and received from the 224.1.1.1 multicast address:

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

admin> set multicast-hbeat-addr = 224.1.1.1

admin> write
IP-GLOBAL/ written
```

The next sample configuration limits monitoring to packets forwarded to and received from the multicast address 224.1.1.1 on UDP port 16387:

```
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
```

The following example shows how to specify that multicast packets from the 10.1.0.0 subnet will be ignored for heartbeat-monitoring purposes:

```
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
```

Configuring the MBONE interface

The MBONE interface is the single LAN or WAN IP interface on which an MBONE router resides. The MBONE interface cannot support multicast clients.

To enable a TAOS unit to forward traffic to and from an MBONE router, you must configure both the IP-Global settings and the appropriate settings in an IP-Interface or Connection profile.

Overview of MBONE interface settings

The following parameter (shown with its default setting) is used on the MBONE interface:

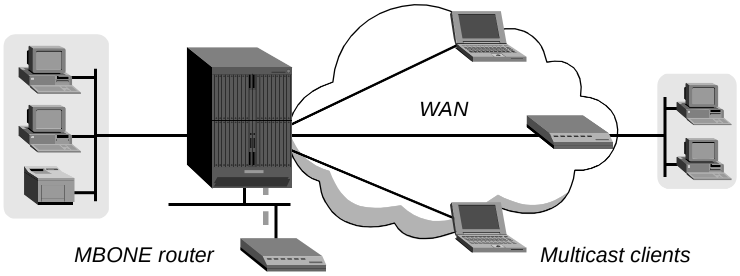
```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }  ]
multicast-allowed = no

[in CONNECTION/"":ip-options]
multicast-allowed = no
```

Parameter	Specifies
Multicast-Allowed	Enable/disable handling of IGMP requests and responses on the interface. The TAOS unit does *not* forward multicast traffic on the basis of this setting.

Example of a local MBONE router

Figure 2-12 shows an MBONE router on one of the system's LAN IP interfaces.

Figure 2-12. MBONE router on a LAN interface



The following commands configure the leftmost shelf-controller Ethernet port as the MBONE interface:

```
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
```

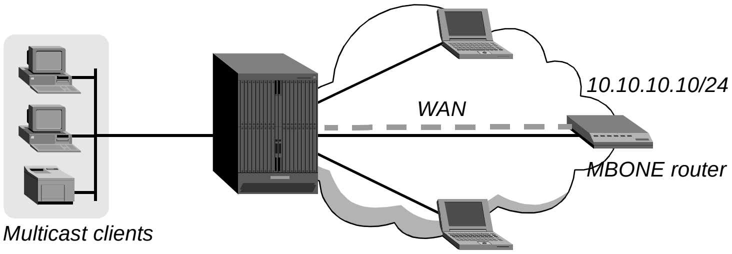
```
admin> set multicast-allowed = yes
```

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

Example of an MBONE router on a WAN interface

Figure 2-13 shows an MBONE router on a WAN interface.

Figure 2-13. MBONE router on a WAN interface



The following commands configure a switched WAN IP interface to the MBONE router:

```
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
```

Configuring multicast client interfaces

The TAOS unit can forward multicast transmissions to any interface except the MBONE interface. To communicate with multicast clients, which are typically running Video Audio Tools (VAT) or Windows, the TAOS unit handles IGMP queries and responses and forwards the MBONE transmission it receives from the MBONE router.

Settings in local IP-Interface and Connection profiles

The following parameters (shown with default settings) are used to set up a multicast client interface:

```
[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
```

Parameter	Specifies
Multicast-Allowed	Enable/disable handling of IGMP requests and responses on the interface. The TAOS unit does *not* forward multicast traffic on the basis of this setting.
Multicast-Rate-Limit	Rate at which the TAOS unit accepts multicast packets from clients on the interface. The default setting (100) disables forwarding of multicast transmissions. For details, see "Setting the multicast rate limit" on page 2-80.
Multicast-Group-Leave-Delay	Number of seconds the TAOS unit waits before forwarding an IGMP-v2 Leave Group message from a multicast client to the MBONE router. For details, see "Specifying a delay for clearing IGMP groups" on page 2-80.

Settings in RADIUS profiles

The following attribute-value pairs can be specified in RADIUS profiles for WAN multicast client interfaces:

RADIUS Attribute	Value
Ascend-Multicast-Client (155)	Enable/disable handling of IGMP requests and responses on the interface. The TAOS unit does *not* forward multicast traffic on the basis of this value.
Ascend-Multicast-Rate-Limit (152)	Rate at which the TAOS unit accepts multicast packets from clients on the interface. The default value (100) disables forwarding of multicast transmissions. For details, see “Setting the multicast rate limit” on page 2-80.
Ascend-Multicast-GRP-Leave-Delay(111)	Number of seconds the TAOS unit waits before forwarding an IGMP-v2 Leave Group message from a multicast client to the MBONE router. For details, see “Specifying a delay for clearing IGMP groups” on page 2-80.

Setting the multicast rate limit

Multicast-Rate-Limit specifies the rate at which the TAOS unit accepts multicast packets from clients on the interface.

Note: By default, Multicast-Rate-Limit is set to 100. This setting disables multicast forwarding on the interface. (The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.) To enable multicast forwarding on the interface, you must set the Multicast-Rate-Limit parameter to a number *less than* 100.

For example, if you set Multicast-Rate-Limit to 5, the TAOS unit accepts one packet every five seconds from multicast clients on the interface. Any subsequent packets received within that 5-second window are discarded.

In addition to multicast rate limiting, the TAOS unit also supports prioritized packet dropping for high-bandwidth data, voice, and audio multicast applications. If the TAOS unit is the receiving device under extremely high loads, it drops packets according to a priority ranking, which is determined by the following UDP port ranges:

- Traffic on ports 0–16384 (unclassified traffic) has the lowest priority (50).
- Traffic on ports 16385–32768 (audio traffic) has the highest priority (70).
- Traffic on ports 32769–49152 (whiteboard traffic) has medium priority (60).
- Traffic on ports 49153–65536 (video traffic) has low priority (55).

Specifying a delay for clearing IGMP groups

Multicast-Group-Leave-Delay specifies the number of seconds the TAOS unit waits before forwarding to the MBONE router an IGMP version-2 Leave Group message it receives across a multicast client interface. Typically, these messages indicate that the IGMP group session can be cleared. However, a multicast interface in the TAOS unit can support many clients, some of which might establish multiple multicast sessions for identical groups, in which case a Leave Group message from a single client must be treated in a special way.

If Multicast-Group-Leave-Delay is set to zero (the default), the TAOS unit forwards the Leave Group messages immediately.

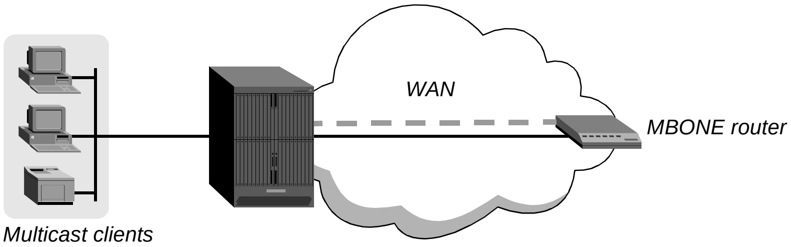
If you set Multicast-Group-Leave-Delay to a nonzero value, the TAOS unit does not immediately forward a Leave Group message it receives from a client on the interface. Instead, it sends back a query to make sure there are no clients on the interface with active multicast sessions for that group. If the TAOS unit receives a response before the specified Multicast-Group-Leave-Delay interval expires, it does not forward the Leave Group message. If the unit does not receive a response, it forwards the message and clears the IGMP group session from its tables after the specified interval.

If users might establish multiple multicast sessions for identical groups, you should set this parameter to a value from 10 to 20.

Example of configuring a LAN multicast client interface

Figure 2-14 shows multicast clients on a LAN interface.

Figure 2-14. LAN multicast client interface



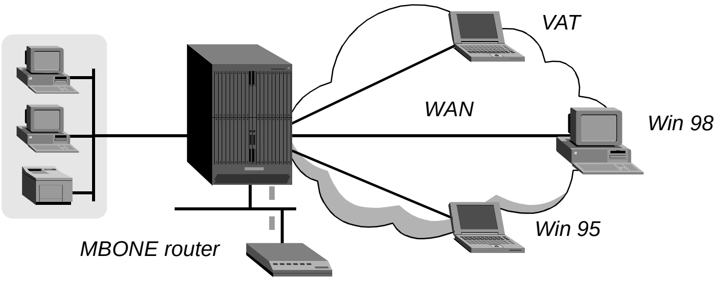
The following commands configure the LAN IP interface to forward multicast transmissions to subscribed multicast clients:

```
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
```

Example of configuring WAN multicast client interfaces

Figure 2-15 shows multicast clients on WAN interfaces.

Figure 2-15. WAN multicast client interfaces



The following commands enable multicast forwarding on the WAN multicast client interfaces in Connection profiles named VAT-1, W98-1, and 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

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
```

Following are comparable settings in RADIUS profiles:

```
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
```

OSPF Routing

3

Introduction to OSPF

Open Shortest Path First (OSPF) is a next-generation Internet routing protocol. The *Open* in its name refers to the fact that OSPF was developed in the public domain as an open specification. *Shortest Path First* refers to an algorithm developed by Dijkstra in 1978 for building a self-rooted shortest-path tree from which routing tables can be derived. (For a description of the algorithm, see “Link-state routing algorithm” on page 3-7.)

RIP limitations solved by OSPF

The rapid growth of the Internet has pushed Routing Information Protocol (RIP) beyond its capabilities, particularly in the areas of distance-vector metrics, the 15-hop limitation, and slow convergence due to excessive routing traffic.

Distance-vector metrics

RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regardless of the speed or reliability of a link.

OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network.

15-hop limitation

With RIP, a destination that requires more than 15 consecutive hops is considered unreachable, and this limitation inhibits the maximum size of a network. OSPF has no hop limitation. You can add as many routers to a network as you want.

Excessive routing traffic and slow convergence

RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. The time it takes for all routers to receive information about a topology change is called *convergence*. Slow convergence can result in routing loops and errors.

A RIP router broadcasts its routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In addition, a large table can require multiple broadcasts for each update, which consumes a lot of bandwidth. OSPF uses a topological database to represent the network and propagates only changes to the database. (For more information about propagation, see “Exchange of routing information” on page 3-4.)

TAOS implementation of OSPF

The primary goal of the OSPF implementation is to allow the TAOS unit to communicate with other routers within a single autonomous system (AS).

Limited border router capability

A TAOS unit acts as an OSPF internal router with limited border router capability.

The TAOS unit does not currently function as an IGP gateway, although it performs autonomous system border router (ASBR) calculations for external routes (such as WAN links that do not support OSPF). The TAOS unit imports external routes into its OSPF database and flags them as autonomous system external (ASE). It redistributes these routes via OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers running RIP.

Authentication

The TAOS unit supports null, simple password, and MD5 cryptographic authentication. For details, see “Security” on page 3-3.

One active IP interface per port

The TAOS OSPF implementation conforms with RFC 1583. It does not support virtual IP interfaces. That is, if more than one IP address is assigned to the same physical port, only one of the logical interfaces can have OSPF enabled. For example, in the following listing the first port on the Ethernet card in slot 15 (shelf 1, slot 15, port 1) has three virtual interfaces:

```
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 can be enabled on any one of the port’s IP interfaces, but not on more than one interface for the same port.

OSPF diagnostic commands

The OSPF diagnostic-level commands enable an administrator to display information related to OSPF routing, including the Link-State Advertisements (LSAs), border router information, and the OSPF areas, interfaces, statistics, and routing table. For information about using these commands, see the *APX 8000/MAX TNT Reference* or the *APX 8000/MAX TNT Administration Guide*.

OSPF traps

The TAOS unit supports OSPF traps as defined in RFC 1850, *OSPF Version 2 Management Information Base*. For an OSPF trap to be generated when the trap condition occurs, OSPF traps must be enabled, either in the Trap profile or by setting the corresponding bit in the `ospfSetTrap` MIB object, which is defined in RFC 1850. In addition, the individual trap that represents the trap condition must be enabled. For detailed information about OSPF traps, see the *APX 8000/MAX TNT Administration Guide*.

OSPF features

This section provides a brief overview of OSPF routing to help you configure the TAOS unit properly. (For details about how OSPF works, see RFC 1583, *OSPF Version 2*.)

An autonomous system is a group of OSPF routers exchanging information, typically under the control of one company. An autonomous system can include a large number of networks, all of which are assigned the same autonomous system number. All information exchanged within the autonomous system is *interior.*

Exterior protocols are used to exchange routing information between autonomous systems. They are referred to by the acronym EGP (exterior gateway protocol). The autonomous system number can be used by border routers to filter out certain EGP routing information. OSPF can make use of EGP data generated by other border routers and added into the OSPF system as ASE information, as well as static routes configured locally or in RADIUS.

Security

All OSPF protocol exchanges are authenticated. Only trusted routers can participate in the autonomous system's routing. A variety of authentication schemes can be used. In fact, different authentication types can be configured for each area. For a discussion of areas, see "Hierarchical routing (areas)" on page 3-6.

Authentication provides added security for the routers that are on the network. Routers that do not have the password are not able to gain access to the routing information, because authentication failure prevents a router from forming adjacencies. (For a discussion of adjacencies, see "Exchange of routing information" on page 3-4.) If both sides of a connection do not support the same authentication method, packet error messages can result.

In addition to null and simple authentication, TAOS units support the MD5 cryptographic authentication method for OSPF, making them compliant with RFC 2328. For details about MD5 encryption, see RFC 2328.

Support for variable-length subnet masks

OSPF routers handle variable-length subnet masks (VLSMs). Each route distributed by OSPF has a destination address and subnet mask, and two different subnets of the same IP network can use different size subnet masks. A packet is routed to the best (longest or most specific) match. Host routes are considered to be subnets whose masks are all ones (0xFFFFFFFF).

Note: Although OSPF is very useful for networks that make use of VLSM, you should attempt to assign subnets that are as contiguous as possible in order to prevent excessive link-state calculations by all OSPF routers on the network.

Exchange of routing information

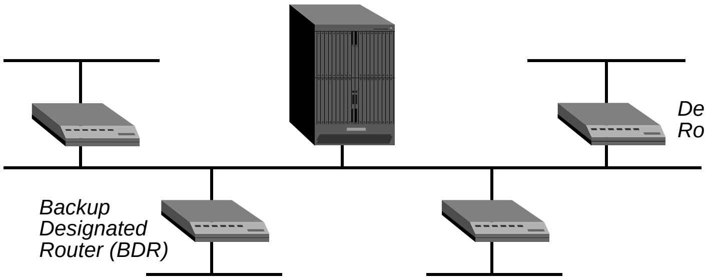
OSPF stores its information about the network in a topological database and propagates only changes to the database. Selected neighboring routers form relationships, referred to as *adjacencies*, for the purpose of exchanging routing information. Not every pair of neighboring routers become adjacent. Routers connected by point-to-point networks and virtual links always become adjacent. On multiaccess networks, all routers become adjacent to routers identified as the designated router (DR) and the backup designated router (BDR).

As the adjacency is established, the neighbors exchange databases and build a consistent, synchronized database between them. When an OSPF router detects a change on one of its interfaces, it modifies its topological database and multicasts the change to its adjacent neighbors, which in turn propagate the change to their adjacent neighbors, until all routers within an area have synchronized topological databases. This process provides quick convergence among routers.

Designated and backup designated routers

In OSPF terminology, a broadcast network is any network that has more than two OSPF routers attached and supports the capability to address a single physical message to all of the attached routers. Figure 3-1 shows such a network.

Figure 3-1. OSPF broadcast network



To reduce the number of adjacencies each router must form, OSPF calls one of the routers the designated router. As routers begin to form adjacencies, they elect a designated router and then all other routers on the network establish adjacencies primarily with the designated router. This simplifies the routing table update procedure and reduces the number of link-state records in the database. The designated router plays other important roles as well to reduce the overhead of OSPF link-state procedures. For example, other routers send LSAs to only the designated router by using the All-Designated-Routers multicast address of 224.0.0.6.

To prevent the designated router from becoming a serious liability to the network if it fails, OSPF routers also elect a backup designated router at the same time. Other routers maintain adjacencies with both the designated router and its backup, but the backup router leaves as many of the processing tasks as possible to the designated router. If the designated router fails, the backup immediately becomes the designated router and a new backup is elected.

You choose the designated router on the basis of the processing power, speed, and memory of the system, then assign priorities to other routers on the network in case the backup designated router is also down at the same time.

Note: The TAOS unit can function as a designated router or backup designated router. However, many sites choose to assign a LAN-based router for these roles in order to dedicate the TAOS unit to WAN processing.

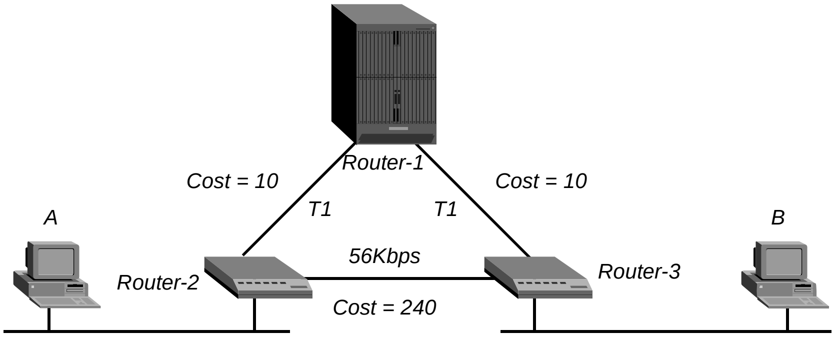
Configurable cost metrics

You assign a cost to the output side of each router interface. The lower the cost, the more likely the interface is to be used to forward data traffic. Costs can also be associated with the externally derived routing data.

The OSPF cost can also be used for preferred-path selection. If two paths to a destination have equal costs, you can assign a higher cost to one of the paths to configure it as a backup to be used only when the primary path is not available.

Figure 3-2 shows how costs are used to direct traffic over high-speed links. For example, if Router-2 in Figure 3-2 receives packets destined for Host B, it routes them through Router-1 across two T1 links (Cost=20) rather than across one 56Kbps B-channel to Router-3 (Cost=240).

Figure 3-2. OSPF costs for different types of links



The TAOS unit has a default cost of 1 for a connected route (Ethernet) and 10 for a WAN link. If you have two paths to the same destination, the one with the lower cost will be used unless route preferences change the equation. (For information about route preferences, see Chapter 2, “IP Routing.”) When assigning costs, you should account for the bandwidth of a connection. For example, for a single B-channel connection, the cost would be 24 times greater than for a T1 link.

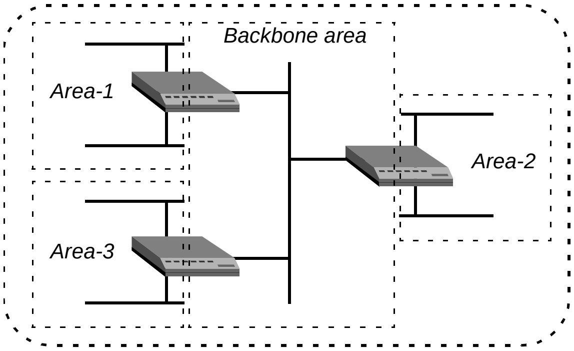
Note: Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network.

Hierarchical routing (areas)

If a network becomes too large, the size of the database, time required for route computation, and related network traffic become excessive. You can partition an AS into areas to provide hierarchical routing, with a backbone area connecting the other areas. The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the autonomous system.

Each area acts as its own network: All area-specific routing information stays within the area, and all routers within an area must have a synchronized topological database. To tie the areas together, some routers belong to the backbone area and also to one of the other areas. These routers are area border routers (ABRs). In Figure 3-3, all of the routers are ABRs.

Figure 3-3. Dividing an OSPF autonomous system into areas



With the ABRs and area boundaries set up correctly, link-state databases are unique to an area. You can configure the TAOS unit to route in three kinds of areas, which differ in their handling of external routes. That is, AS External (ASE) routes, which are originated by ASBRs as Type-5 LSAs, are handled differently in each of the following types of areas:

- Normal
- Stub
- not-so-stubby-area (NSSA)

Normal areas

An OSPF normal area allows Type-5 LSAs to be flooded throughout the area.

Stub areas

For areas that are connected only to the backbone by one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. To reduce the cost of routing, OSPF supports stub areas, in which a default route summarizes all external routes. A stub area allows no Type-5 LSAs to be propagated into or throughout the area, and instead depends on default routing to external destinations.

NSSAs

NSSAs are like stub areas in that they do not receive or originate Type-5 LSAs. However, NSSAs rely solely on default routing for external routes. They employ Type-7 LSAs for carrying ASE route information within the area. Type 7 LSAs use a propagate (P) bit to flag the NSSA border router to translate the Type-7 LSA into a Type-5 LSA, which can then be propagated into other areas.

When the TAOS unit is routing OSPF in an NSSA, it imports ASE routes defined in local or RADIUS profiles as Type-7 LSAs. These imported ASE LSAs always have the P bit enabled, which flags border routers to translate them into Type-5 LSAs.

You can list the router IDs of NSSA border routers (which are performing the Type-7 to Type-5 LSA translation), by entering the OSPF Translators command. For example:

```
admin> ospf translators

Area ID     Router ID
0.0.0.1     10.105.0.13
0.0.0.2     12.1.1.1
```

Note: For details about the NSSA specification, see RFC 1587.

Link-state routing algorithm

The link-state routing algorithms require that all routers within a domain maintain synchronized (identical) topological databases, and that the databases describe the complete topology of the domain. An OSPF router's domain can be an autonomous system or an area within an autonomous system.

OSPF routers create and update a link-state database from information exchanged with other routers. Link-state databases are synchronized between pairs of adjacent routers (as described in "Exchange of routing information" on page 3-4). In addition, each OSPF router uses its link-state database to calculate a self-rooted tree of shortest paths to all destinations. The routing table is built from these calculated shortest-path trees. For example, consider the network topology in Figure 3-4.

Figure 3-4. Sample OSPF topology

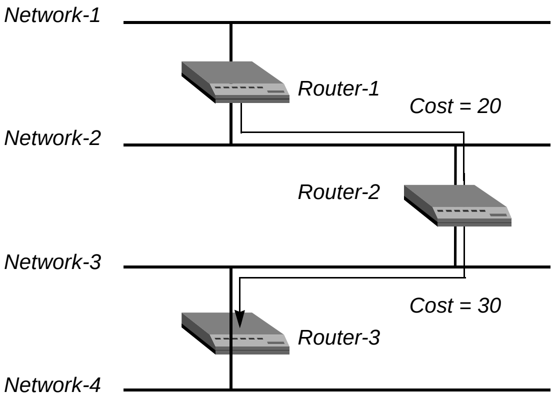


Table 3-1 shows the relevant information in the routers' link-state databases.

Table 3-1. Link-state databases for OSPF topology in Figure 3-4

Router-1	Router-2	Router-3
Network-1/Cost 0	Network-2/Cost 0	Network-3/Cost 0

Table 3-1. Link-state databases for OSPF topology in Figure 3-4 (continued)

Router-1	**Router-2**	**Router-3**
Network-2/Cost 0	Network-3/Cost 0	Network-4/Cost 0
Router-2/Cost 20	Router-1/Cost 20	Router-2/Cost 30
	Router-3/Cost 30	

From the link-state database, each router builds a self-rooted shortest-path tree, and then calculates a routing table stating the shortest path to each destination in the autonomous system. (The table also includes externally derived routing information.)

All of the routers calculate a routing table of shortest paths, based on the link-state database. Externally derived routing data is advertised throughout the autonomous system but is kept separate from the link-state data. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the autonomous system.

Table 3-2. Shortest-path tree and resulting routing table for Router-1

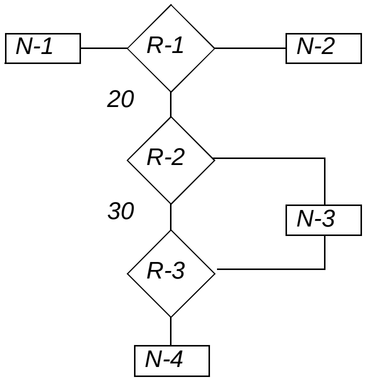
<table>
<tr><td rowspan="5"> </td><td><i>Destination</i></td><td><i>Next hop</i></td><td><i>Metric</i></td></tr>
<tr><td>Network-1</td><td>Direct</td><td>0</td></tr>
<tr><td>Network-2</td><td>Direct</td><td>0</td></tr>
<tr><td>Network-3</td><td>Router-2</td><td>20</td></tr>
<tr><td>Network-4</td><td>Router-2</td><td>50</td></tr>
</table>

Table 3-3. Shortest-path tree and resulting routing table for Router-2

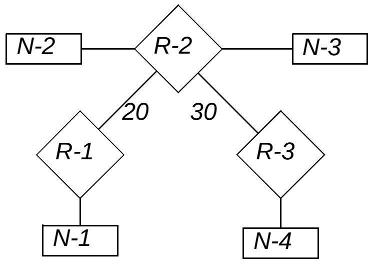
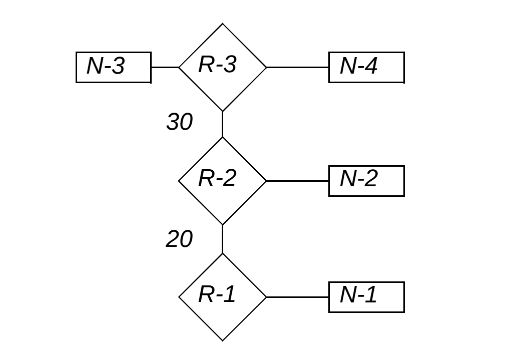
<table>
<tr><td rowspan="5"> </td><td><i>Destination</i></td><td><i>Next hop</i></td><td><i>Metric</i></td></tr>
<tr><td>Network-1</td><td>Router-1</td><td>20</td></tr>
<tr><td>Network-2</td><td>Direct</td><td>0</td></tr>
<tr><td>Network-3</td><td>Direct</td><td>0</td></tr>
<tr><td>Network-4</td><td>Router-2</td><td>30</td></tr>
</table>

Table 3-4. Shortest-path tree and resulting routing table for Router-3



Destination	*Next hop*	*Metric*
Network-1	Router-2	50
Network-2	Router-2	30
Network-3	Direct	0
Network-4	Direct	0

Adding a TAOS unit to an OSPF network

Before it can run OSPF, a TAOS unit must be configured for IP routing, as described in Chapter 2, “IP Routing.”

Overview of LAN and WAN OSPF settings

The OSPF subprofiles of the IP-Interface and Connection profiles (for configuring local and WAN interfaces, respectively) both contain the same parameters. Following are the OSPF parameters, shown with their default values:

```
[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 = *******
```

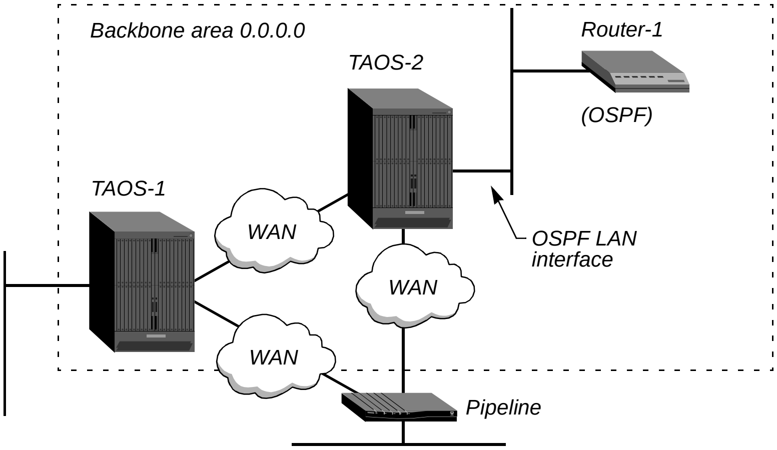
Parameter	**Specifies**
Active	Enable/disable OSPF on an interface.
Area	Area number in dotted-decimal format. The default area number is 0.0.0.0, which represents the OSPF backbone. Note that area numbers are not IP addresses, although they use a similar format. For a discussion of areas, see “Hierarchical routing (areas)” on page 3-6.
Area-Type	Type of area. The default is the Normal area type, in which external routes are advertised throughout the autonomous system.
Hello-Interval	Number of seconds between Hello packets. The default value for the Hello-Interval parameter is 30. For information about how the router uses these packets, see “Exchange of routing information” on page 3-4.
Dead-Interval	Number of elapsed seconds without receiving a Hello packet the router will wait before considering its neighbor dead and instituting a link-state change. For details, see “Exchange of routing information” on page 3-4.
Priority	Priority value, used to elect a designated router and backup designated router. A setting of 1 or greater places the TAOS unit on the list of possible designated routers. A setting of 0 excludes the TAOS unit from becoming a designated router or backup designated router. The higher the priority value of the TAOS unit relative to other OSPF routers on the network, the better the chances that it will become one of these routers. For details, see “Designated and backup designated routers” on page 3-4.
Authen-Type	Type of authentication to use for validating OSPF packet exchanges. Specify one of the following values: • None—No authentication is required. • Simple (the default)—The router uses the password supplied in the Auth-Key parameter to validate OSPF packet exchanges. • MD5— The router uses MD5 encryption and the authentication Key ID supplied by the Key-ID parameter to validate OSPF packet exchanges. For related information, see “Security” on page 3-3.
Auth-Key	Secret key for authenticating traffic in the router’s area. When Authen-Type is set to `md5`, you must set the MD5-Auth-Key parameter to specify a key.

Parameter	Specifies
MD5-Auth-Key	Secret key to be used for the MD5 cryptographic authentication method, up to 16 characters. The default value is `ascend0`.
MD5-Authen-Key	Secret key to be used for the MD5 cryptographic authentication method, up to 16 characters. The default value is `ascend0`. When Authen-Type is set to `md5`, you must supply a key in the new field because the Auth-Key setting used previously no longer applies.
Key-ID	Number from 0 to 255, used to encrypt the secret key when Authen-Type is set to MD5.
Cost	Cost of routing to the interface. The lower the cost assigned to a route, the more likely it is to be used to forward traffic. For details, see “Configurable cost metrics” on page 3-5.
Down-Cost	Cost to be applied to the interface when it is down.
ASE-Type	Type of metric to apply to routes learned from RIP. Type-1 expresses the metric in the same units as the interface cost. Type-2 is considered larger than any link-state path. This parameter applies in a Connection profile only when OSPF is *not* active
ASE-Tag	Hexadecimal number that shows up in management utilities and flags the route as external. It can also be used by border routers to filter a record. It is active in a Connection profile only when OSPF is *not* active.
Transit-Delay	Estimated number of seconds it takes to transmit a Link State Update packet over this interface, taking into account transmission and propagation delays. On a connected route, you can leave the default of 1.
Retransmit-Interval	Number of seconds between Link-State Advertisement retransmissions for adjacencies belonging to this interface. Its value is also used when retransmitting database description and link-state request packets. On a connected route, you should typically leave the default of 5.
Non-Multicast	Enable/disable a TAOS unit to run OSPF over a Frame Relay link to a GRF® switch. GRF models Frame Relay as a nonbroadcast multiaccess (NBMA) network, while the TAOS unit models Frame Relay as a serial (point-to-point) network. If Non-Multicast is set to Yes, all multicast packets are remapped to a directed neighbor address, which enables adjacencies to form between neighbors. This setting is ignored on an Ethernet broadcast network. Its use is not recommended for unnumbered interfaces. If it is specified on an unnumbered interface, the packets will be dropped.

Example of configuring a LAN OSPF interface

Figure 3-5 shows three OSPF routers in the backbone area of an autonomous system. Because all OSPF routers are in the same area, the units form adjacencies and synchronize their databases. This example shows how to configure the LAN interface of the unit labeled TAOS-2 in Figure 3-5.

Figure 3-5. OSPF on a LAN interface



All OSPF routers in Figure 3-5 have RIP turned off. Running both RIP and OSPF is unnecessary, and turning RIP off reduces processor overhead. OSPF can learn routes from RIP interfaces, incorporate them in the routing table, assign them an external metric, and tag them as external routes.

Although the RFC does not specify a limitation about the number of routers in the backbone area, you should keep the number of routers relatively small, because changes that occur in area zero are propagated throughout the autonomous system. Another way to configure the same units would be to create a second area (such as 0.0.0.1) in one of the existing OSPF routers, and add the TAOS unit to that area. You could then assign the same area number (0.0.0.1) to all OSPF routers reached through the TAOS unit across a WAN link.

Following is an example that shows how to configure TAOS-2 in Figure 3-5. The commands assign the IP address 10.168.8.17/24 to the local interface and configure the OSPF router in the backbone area:

```
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
```

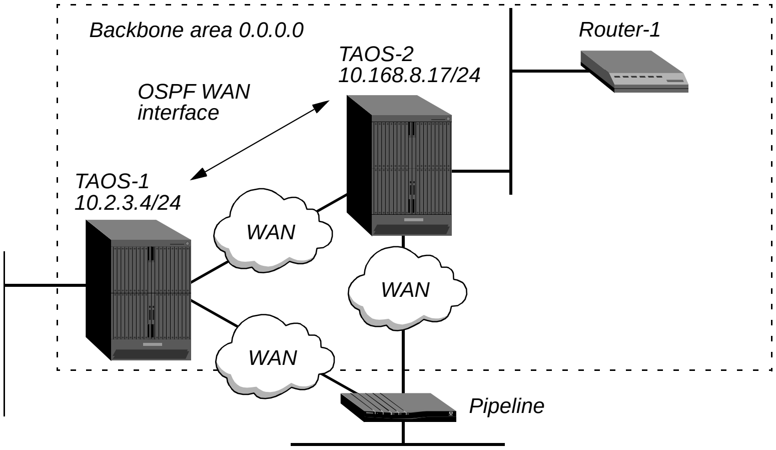
The following example shows how to configure the IP interface for MD5 authentication:

```
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
```

Example of configuring WAN OSPF interfaces

This example shows how to configure Connection profiles in the TAOS units shown in Figure 3-6, to enable them to route OSPF across the WAN that separates them. In this example, the unit labeled TAOS-1 has the IP address 10.2.3.4/24, and the unit labeled TAOS-2 has the address 10.168.8.17/24.

Figure 3-6. OSPF on a WAN interface



The WAN interfaces of the TAOS unit form point-to-point networks. That is, each link joins a single pair of routers. Point-to-point networks typically do not provide a broadcasting or multicasting service, so all advertisements are sent point to point.

The following commands configure the OSPF WAN link in TAOS-1 in Figure 3-6:

```
admin> read conn taos2ink
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
```

The following commands configure the OSPF WAN link in TAOS-2 in Figure 3-6:

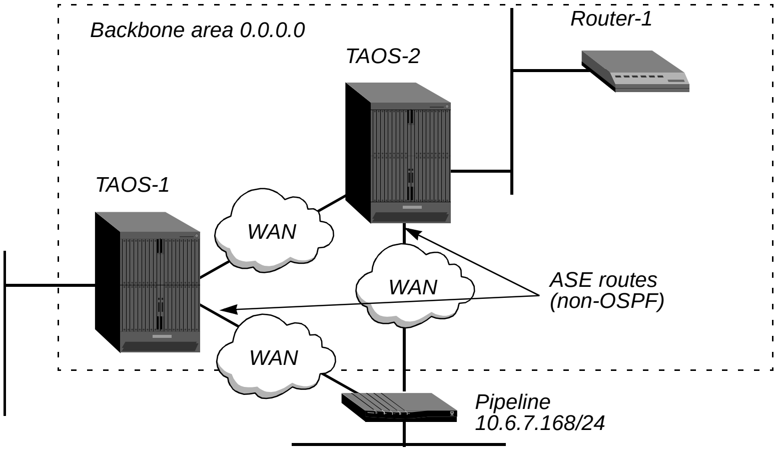
```
admin> read conn taos1link
CONNECTION/taos1link read

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
```

Example of integrating a RIP-v2 interface

In Figure 3-7, each TAOS unit has a WAN interface to a remote Pipeline unit. The Pipeline is an IP router that supports RIP-v2, and has the IP address 10.6.7.168/24. The route to the

Pipeline LAN, and any routes the TAOS unit learns about from the remote Pipeline, are ASE routes (external to the OSPF autonomous system).

Figure 3-7. Including ASE routes in the OSPF environment



To enable OSPF to add routes learned from RIP-v2 to the routing table, you can configure RIP-v2 normally in the Connection profiles. The global RIP-ASE-Type parameter in the IP-Global profile determines the ASE metric applied when the routes are imported to OSPF. For details about RIP-ASE-Type, see “Configuring route options” on page 3-14.

However, in the following example, RIP is turned off on the link, so the TAOS unit does not forward or receive routing updates on the interface. The following commands specify a cost of 240 for the link to the Pipeline, disable RIP, and specify ASE information for the Connection profile’s static route:

```
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
```

The ASE-Type and ASE-Tag information causes the OSPF router to import the route to 10.6.7.168/24 as a Type-2 LSA and tag it with the specified hexadecimal number. The cost assigned is appropriate for the bandwidth of a single B-channel connection and the cost is 24 times greater than for a T1 link.

Configuring route options

The IP-Global profile contains several settings that apply only when OSPF routing is in use. Following are the relevant parameters (shown here with their default settings):

```
[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
```

Parameter	**Specifies**
Pool-OSPF-Adv-Type	Type of ASE metric applied to summarized pools imported into OSPF as external routes. Pool-Summary must be set to Yes and OSPF must be enabled for this setting to have any effect. Type-1 (the default) expresses the metric in the same units as the interface cost. Type-2 is considered larger than any link-state path. Internal imports pool routes as intra-area routes, which enables them to work with stub areas.
OSPF-Pref	Preference value for routes learned from OSPF. Valid values are 0 to 255 (default 10).
OSPF-ASE-Pref	Preference value for routes learned from RIP, ICMP, or another non-OSPF protocol. Valid values are from 0 to 255. By default, routes learned dynamically from another routing protocol are assigned a preference value of 150.
RIP-Tag	Hexadecimal number associated with routes learned from RIP. OSPF border routers can use the tag to filter a record.
RIP-ASE-Type	Type of ASE metric applied to routes learned from RIP. Type-1 (the default) expresses the metric in the same units as the interface cost. Type-2 is considered larger than any link-state path.
AS-Boundary-Router	Enable/disable autonomous system border router (ASBR) calculations related to external routes. Normally, when the TAOS unit imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) it performs the ASBR calculations for those routes. If necessary, you can prevent the TAOS unit from performing ASBR calculations by setting AS-Boundary-Router to No.

Example of importing a summarized pool as an ASE

For information about defining summarized address pools, see “Example of configuring summarized address pools” on page 2-66. The following commands configure a summarized pool and import it to OSPF with a Type-1 OSPF metric:

```
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
```

When Pool-Summary is set to Yes and OSPF is enabled, the OSPF subsystem looks at the Pool-OSPF-Adv-Type parameter to decide how to import summarized routes into OSPF. If it is set to Type-1, the metric for the route to a summarized pool is expressed in the same units as the link-state metric (interface cost).

If Pool-OSPF-Adv-Type is set to Type-2, the assumption is that routing between autonomous systems is the major cost of routing a packet, and there is no need for conversion of external costs to internal link-state metrics. If the parameter is set to Internal, the summarized pool addresses are imported into OSPF as intra-area routes, which enables them to work properly with stub areas.

Example of setting ASE preferences

The OSPF-Pref and OSPF-ASE-Pref settings determine the preference values assigned to routes learned from other OSPF routers and those imported from other dynamic routing protocols. The default settings place a much lower preference on OSPF routes, which means that those routes are more likely to be used. The following commands decrease the preference assigned to ASE routes to 100 (the default is 150):

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

admin> set ospf-ase-pref = 100

admin> write
IP-GLOBAL written
```

Configuring OSPF static-route information

The following IP-Route parameters (shown with sample settings) apply only when OSPF is enabled:

```
in IP-ROUTE/"" (new)]
cost = 1
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
ase7-adv = N/A
```

Parameter	Specifies
Cost	Cost of routing to the interface. The lower the cost assigned to a route, the more likely that it will be used to forward traffic. See “Configurable cost metrics” on page 3-5.
Third-Party	Enable/disable advertisement of routes to external destinations on behalf of another gateway (a third party). See “Example of specifying a third-party route” on page 3-18.
Ase-Type	Type of metric to apply to routes learned from RIP. Type-1 expresses the metric in the same units as the interface cost. Type-2 is considered larger than any link-state path. This parameter applies in a Connection profile only when OSPF is *not* active

Parameter	Specifies
Ase-Tag	Hexadecimal number that shows up in management utilities and flags this route as external. It can also be used by border routers to filter this record. It is active in a Connection profile only when OSPF is *not* active.
ASE7-Adv	In earlier versions of the software, this parameter provided a way to disable the P-bit for static routes imported to OSPF in an NSSA, to prevent those routes from being propagated to the backbone. This is no longer the case. The P-bit is now always enabled for ASE routes, so the TAOS unit disregards the setting of this parameter.

Example of configuring a Type-7 LSA in an NSSA

For background information about NSSAs, see “Hierarchical routing (areas)” on page 3-6. To configure the TAOS unit to route OSPF in an NSSA, *all* OSPF interfaces in the TAOS unit must specify the NSSA area-type.

To configure a Type-7 LSA, you must specify a static route in an IP-Route profile. Following are the related parameters (shown with sample settings):

```
[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
```

The following procedure configures the TAOS unit to route in an NSSA and import a Type-7 LSA that specifies an external route across the WAN link:

1 Assign an NSSA area type to each IP interface that is running OSPF. For example:

```
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 the WAN link that represents an ASE route. For example:

```
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 a static route to the remote site. For example:

```
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
```

Example of assigning a cost to a static route

The lower the cost assigned to a route, the more likely that the router will choose the route to forward traffic. Typically, you should account for the bandwidth of a connection when assigning costs. For example, the cost for a single-channel connection would be 24 times greater than for a T1 link.

The TAOS unit has a default cost of 1 for a connected route (Ethernet) and 10 for a WAN link. If you have two paths to the same destination, the one with the lower cost is used. Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network. In the following example, an administrator assigns a cost of 25 to a static route:

```
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
```

Example of specifying a third-party route

OSPF can advertise routes to external destinations on behalf of another gateway (a third party). This function is commonly known as advertising a forwarding address. If third-party routing is disabled, the TAOS unit advertises itself as the forwarding address to an external destination. When third-party routing is enabled, the TAOS unit advertises the IP address of another gateway.

Depending on the topology of the network, other routers might be able to use this type of third-party LSA to route directly to the forwarding address without involving the advertising router, thus increasing the total network throughput. This feature can be used only if all OSPF routers know how to route to the forwarding address. For the route to be known, the forwarding address must be on a local network that has an OSPF router acting as the forwarding router, or a designated router must send LSAs for that Ethernet network to any area that sees the static route’s forwarding-address LSAs. Note that third-party routing cannot be used when ASE Type-7s are advertised (as specified in RFC 1587).

In the following sample route, the TAOS unit will advertise a third-party route (a forwarding address) for the destination 10.1.2.0. The forwarding address is 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
```

OSPF nonbroadcast multiaccess (NBMA) support

An OSPF nonbroadcast multiaccess (NBMA) network is any network that has multiple points of access (more than two routers) and does not support broadcast capability. Frame Relay and X.25 are typically NBMA networks.

OSPF routers operate on an NBMA network much as they do on a broadcast network, by using the Hello protocol to form adjacencies and identify the designated router. However, because the routers cannot discover their neighboring routers dynamically by means of broadcasts, you must specify some additional parameters.

The TAOS unit forms adjacencies with other OSPF routers on an NBMA network. Adjacencies enable the unit to route OSPF over Frame Relay networks, and to interoperate with the switches that do not support the serial (point-to-point) model over Frame Relay.

Note: The Non-Multicast parameter in the OSPF-Options subprofiles for IP interfaces causes the translation of the multicast traffic to directed traffic. This parameter is typically used with a serial link, such as a point-to-point connection over Frame Relay, and is not intended for use with NBMA. Non-Multicast must not be enabled for NBMA configurations.

Overview of OSPF NBMA settings

Following are the OSPF parameters (shown with default settings) related to 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
```

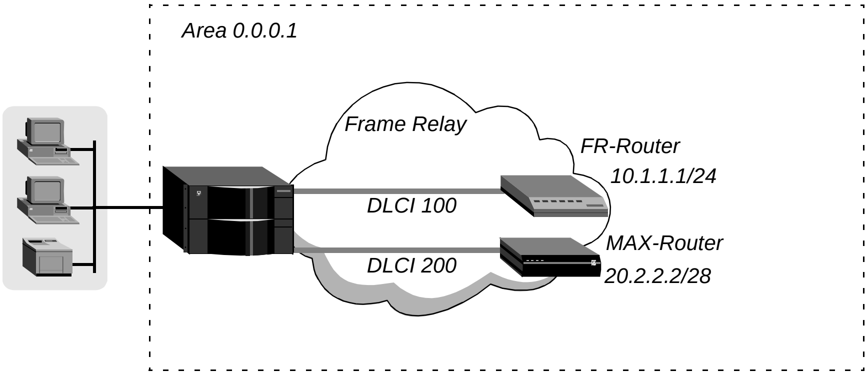
Parameter	Specifies
Network-Type	Type of network to which the interface connects: Broadcast, NonBroadcast (multiaccess), or Point-to-Point. Broadcast specifies any broadcast-capable network, such as Ethernet. NonBroadcast (multiaccess) is used for networks that have more than two OSPF routers and no broadcast capability, such as Frame Relay or X.25. Point-to-Point (the default), is used for interfaces connected to one other node on the other far end.
Poll-Interval	Interval, in seconds, at which to send Hello packets to a neighboring router that has become inactive. The default 0 (zero) means that no Hello packets are sent to a neighboring router from which no Hello packets have been received for the number of seconds specified by the Dead-Interval setting. If you specify a nonzero value, use a larger value than the Hello-Interval default of 10 seconds (for example, 120 seconds).
Name	Name of the OSPF-NBMA-Neighbor profile.
Host-Name	Station name of a local Connection profile that defines the connection to the neighboring router.
IP-Address	IP address of the neighboring router.
DR-Capable	Whether the neighboring router can be the designated router. Values are `yes` and `no` (the default).

Example of an OSPF NBMA configuration

On an NBMA network, a router that is eligible to become the designated router is configured with a list of all other OSPF routers connected to the network. At startup, these routers send Hello packets to each other to discover the designated router. The designated router then begins sending Hello packets to the entire list of routers on the network. When an NBMA interface becomes active on the TAOS unit, the unit sends Hello packets only to neighboring routers that are eligible to become the DR, until it is notified about which router is the designated router.

Figure 3-8 shows an OSPF NBMA network using Frame Relay. For the purposes of this example, assume that the unit named FR-Router is eligible to become the designated router, and that the MAX-Router unit is not eligible.

Figure 3-8. OSPF nonbroadcast multiaccess (NBMA) network



Example of configuring a designated router-capable neighboring router

The following set of commands defines a sample Frame-Relay profile for the interface to FR-Router in Figure 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
```

The next set of commands defines a Connection profile for connection to 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
```

The next set of commands enables the TAOS unit to form an adjacency with MAX-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
```

Example of configuring a non-DR-capable neighbor

The following set of commands defines a Frame-Relay profile for link operations on the interface to the unit named MAX-Router in Figure 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
```

The next set of commands defines a Connection profile for connection to 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
```

The next set of commands enables the TAOS unit to form an adjacency with 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
```

Disabling OSPF

To globally disable the OSPF protocol, set the following parameter (shown with its default value):

```
[in IP-GLOBAL:ospf-global]
enable = yes
```

Parameter	Specifies
Enable	Enable/disable the OSPF protocol. A change to the setting takes effect immediately upon writing the profile.

Although you can also deactivate OSPF manually on each OSPF interface, this parameter provides a global mechanism for disabling the protocol. It can also be used to prevent OSPF from reinitializing several times if you are modifying many OSPF-related profiles. In that case, set the parameter to `no`, write the OSPF changes, and then set the parameter to `yes` again.

Ascend Tunnel Management Protocol (ATMP) 4

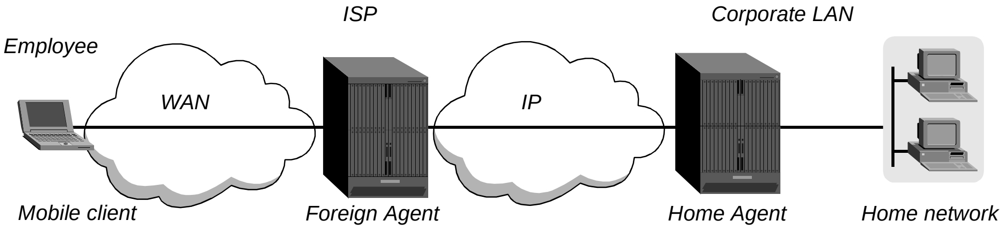
TAOS units support Ascend Tunnel Management Protocol (ATMP) for virtual private network (VPN) connectivity. For information about using other tunneling protocols for VPN connectivity, see Chapter 5, “L2TP, L2F, PPTP, and IP-in-IP Tunneling.”

Introduction to ATMP

ATMP is a UDP/IP-based protocol for tunneling between two TAOS units across an IP network. Data is transported through the tunnel in Generic Routing Encapsulation (GRE), as described in RFC 1701. (For a complete description of ATMP, see RFC 2107, K. Hamzeh, *Ascend Tunnel Management Protocol - ATMP.*)

Figure 4-1 shows one use for ATMP tunneling: Mobile clients dial in to a local ISP to log in to a distant LAN across the Internet. ATMP creates and tears down a cross-Internet tunnel between the two TAOS units. In effect, the tunnel collapses the IP cloud and provides what looks like direct access to a home network.

Figure 4-1. ATMP tunnel from an ISP to a corporate home network



A mobile client dials in to the Foreign Agent, which authenticates the Connection profile (or RADIUS profile) and initiates an IP connection to the specified Home Agent.

The Foreign Agent then requests a tunnel for the connected mobile client. The Home Agent authenticates the tunnel request (by password), and then registers the tunnel and assigns it an ID. If the Home Agent refuses the tunnel, the Foreign Agent disconnects the mobile client.

If the tunnel is successfully established, the Home Agent forwards or routes tunneled data to the home network. If the mobile client has a multichannel MP+ or MP connection, the tunnel remains active when the connection adds or subtracts channels, and is not torn down until the final channel of the call is disconnected.

The Home Agent must be able to access the home network either as an ATMP gateway or by routing the packets. For a description of how the Home Agent operates as a gateway or router, see “Home Agent ATMP profile settings” on page 4-17.

If an ATMP client disconnects because of an ATMP error, ATMP disconnect codes can help you diagnose the exact cause of the problem. Each code can appear in a Syslog record or as the value of Ascend-Disconnect-Cause (195) in a RADIUS accounting record. For additional information about disconnect codes, see the *TAOS RADIUS Guide and Reference*.

Network settings for ATMP

Network settings for ATMP include settings related to the IP connection between TAOS units, settings related to the UDP communication required to establish tunnels, and settings related to packet fragmentation and reassembly.

System reset requirement

When you change the setting of the UDP-Port parameter in the ATMP profile of a Home Agent, a system reset is required for the ATMP subsystem to recognize the new UDP port number.

When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, a system reset is required for the new value to take effect.

All other parameter settings in the ATMP profile take effect as soon as possible after writing the profile.

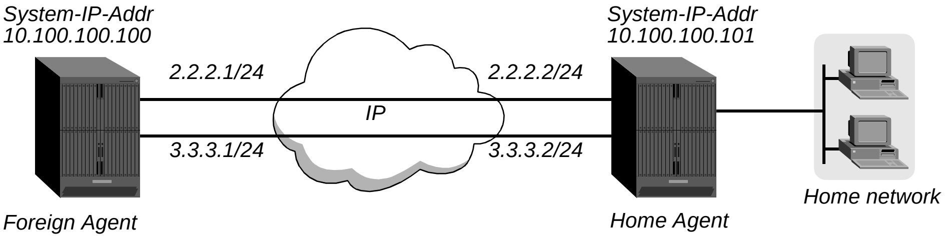
System IP address recommendation

Lucent Technologies recommends that you set the System-IP-Addr parameter in the IP-Global profile, on a TAOS unit that is operating as an ATMP agent, particularly if the unit has multiple interfaces into the IP cloud that separates it from other ATMP agents. This recommendation has two aspects:

- On a Foreign Agent, in the Connection profile for mobile clients, specify the system IP address of a Home Agent rather than the interface address on which the Home Agent accepts tunneled data. This setting helps to avoid communication problems if a route changes within the IP cloud.
- On both a Foreign Agent and a Home Agent, the link to the other agent can specify the unit’s system IP address. This setting is not required if RIP is enabled on the interfaces between the two agents, but it is recommended, because it helps to simplify configurations.

Figure 4-2 shows a Home Agent and Foreign Agent, with two Ethernet interfaces connecting them. (The principle is the same as if there were two WAN connections between the units.)

Figure 4-2. System IP addresses and routes between ATMP agents



When RIP is enabled on the IP interfaces between the two units, it advertises the system address on both ports. For example, suppose a Foreign Agent has the following system IP address and IP interface configuration:

```
[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
```

Supposing a Home Agent has the following system IP address and IP interface configuration:

```
[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
```

With this configuration, the Foreign Agent advertises, on both of its Ethernet ports, a route to its own system address, 10.100.100.100. Similarly, the Home Agent advertises, on both of its Ethernet ports, a route to its own system address, 10.100.100.101.

When the Home Agent receives the advertisements for 10.100.100.100, it selects one of the ports advertising the route and adds that route to its routing table. The next time the Home Agent establishes a connection with the Foreign Agent, it uses the port indicated in the routing table. If that port becomes unavailable (for example, if the cable is disconnected), the Home Agent soon updates its routing table to use the other port to connect to the Foreign Agent.

Setting the UDP port

By default, ATMP agents use UDP port 5150 to exchange control information while establishing a tunnel. If the Home Agent ATMP profile specifies a different UDP port number, all tunnel requests to that Home Agent must specify the same UDP port.

Note: A system reset is required for the ATMP subsystem to recognize the new UDP port number.

Specifying tunnel retry limits

The Retry-Timeout and Retry-Limit parameters in the ATMP profile work together to limit how many tunnel RegisterRequest messages (to open a tunnel) and DeregisterRequest messages (to close a tunnel) are sent and the number of seconds between each message. If a tunnel request fails, the Foreign Agent times out, logs a message, and disconnects the mobile client. When a tunnel request succeeds, the Home Agent assigns a tunnel ID, and the UDP port is no longer used for that tunnel. The actual data transfer uses the IP connection with GRE.

The Retry-Timeout and Retry-Limit parameters have default settings that are appropriate for most sites, but you might want to increase or decrease the values on the basis of what type of link connects the Foreign Agent and Home Agent. For example, if the link is a switched dial-out connection, you might want to increase the values to allow sufficient time to establish the connection. Or, if the Foreign Agent and the Home Agent are on the same Ethernet segment, you might want to reduce the values to provide a quicker response to the mobile client when the Home Agent is unavailable.

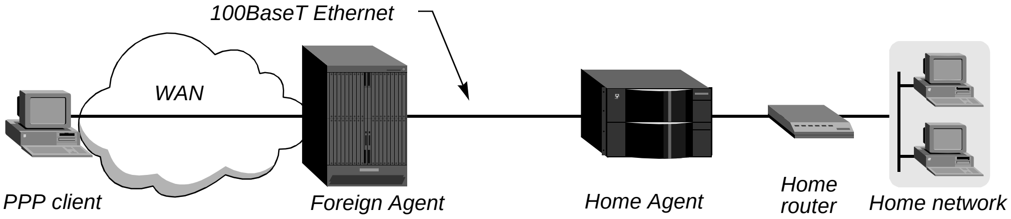
If you increase the Retry-Timeout and Retry-Limit values, keep in mind that the values determine response time to mobile clients when the Home Agent is unavailable. If a tunnel request reaches a secondary Home Agent that is also unavailable, the mobile client waits for twice the specified period before being informed that the connection failed.

Setting an MTU limit

The type of link that connects a Foreign Agent and Home Agent determines the maximum transmission unit (MTU). The link can be on a switched dial-out connection, a Frame Relay connection, or an Ethernet link, and it can be a local network or routed through multiple hops. If the link between devices is multihop (if it traverses more than one network segment), the path MTU is the *minimum* MTU of the intervening segments.

Figure 4-3 shows an ATMP setup across a 100BaseT Ethernet segment, which limits the path MTU to 1500 bytes.

Figure 4-3. Path MTU on an Ethernet segment



If any segment of the link between the agents has an MTU smaller than 1528, some packet fragmentation and reassembly will occur. You can push fragmentation and reassembly tasks to connection end points (a mobile client and a device on the home network) by setting an MTU limit. Client software then uses MTU discovery mechanisms to determine the maximum packet size, and fragments packets before sending them.

How link compression affects the MTU

Compression affects which packets must be fragmented, because compressed packets are shorter than their original counterparts. If any kind of compression is on (such as VJ header or link compression), the connection can transfer larger packets without exceeding a link's maximum receive unit (MRU). If compressing a packet makes it smaller than the MRU, it can be sent across the connection, whereas the same packet without compression could not.

How ATMP tunneling causes fragmentation

To transmit packets through an ATMP tunnel, the TAOS unit adds an 8-byte GRE header and a 20-byte IP header to the frames it receives. The addition of these packet headers can make the packet larger than the MTU of the tunneled link, in which case the unit must either fragment the packet after encapsulating it or reject the packet.

Fragmenting packets after encapsulating them has several disadvantages for the Foreign Agent and Home Agent. For example, it causes a performance degradation, because both agents have extra overhead. It also means that the Home Agent device cannot be a GRF switch. (To maintain its very high aggregate throughput, a GRF switch does not perform reassembly.)

Pushing the fragmentation task to connection end points

To avoid the extra overhead incurred when ATMP agents perform fragmentation, you can either set up a link between the two units that has an MTU greater than 1528 (which means it cannot include Ethernet segments), or you can set the MTU-Limit parameter in the ATMP profile to a value that is 28 bytes less than the path MTU.

If MTU-Limit is set to zero (the default), the TAOS unit might have to fragment encapsulated packets before transmission. The other ATMP agent must then reassemble the packets.

If MTU-Limit is set to a nonzero value, the unit reports that value to the client software as the path MTU, causing the client to send packets of the specified size. This pushes the task of fragmentation and reassembly out to the connection end points, lowering the overhead of the ATMP agents.

For example, if the TAOS unit is communicating with another ATMP agent across an Ethernet segment, you can set the MTU-Limit parameter to a value 28 bytes smaller than 1500 bytes, as shown in the following example, to enable the unit to send unfragmented packets that include the 8-byte GRE header and a 20-byte IP header:

```
admin> read atmp
ATMP read

admin> set mtu-limit = 1472

admin> write
ATMP written
```

With this setting, the connection end point sends packets with a maximum size of 1472 bytes. When the TAOS unit encapsulates them, adding 28 bytes to the size, the packets still do not violate the 1500-byte Ethernet MTU.

Forcing fragmentation for interoperation with outdated clients

To discover the path MTU, some clients normally send packets that are larger than the negotiated maximum receive unit (MRU) and that have the Don't Fragment (DF) bit set. Such packets are returned to the client with an ICMP message informing the client that the host is unreachable without fragmentation. This standard, expected behavior improves end-to-end performance by enabling the connection end points to perform any required fragmentation and reassembly.

However, some outdated client software does not handle this process correctly and continues to send packets that are larger than the specified MTU-Limit. To enable the TAOS unit to interoperate with these clients, you can configure the unit to ignore the DF bit and perform the fragmentation that normally should be performed by the client software. This function is referred to as *prefragmentation*.

When the MTU-Limit parameter is set to a nonzero value, you can set the Force-Fragmentation parameter to Yes to enable the TAOS unit to prefragment packets it receives that are larger than the negotiated MRU with the DF bit set. It prefragments those packets, and then adds the GRE and IP headers.

Note: Setting the Force-Fragmentation parameter to Yes causes the TAOS unit to bypass the standard MTU discovery mechanism and fragment larger packets before encapsulating them in GRE. Because this changes expected behavior, it is not recommended except for interoperation with outdated client software that does not handle fragmentation properly.

Mobile clients with duplicate IP addresses

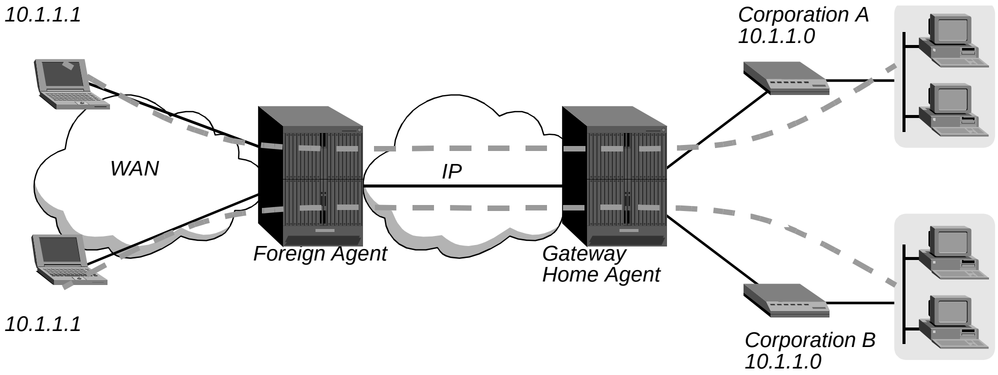
A Foreign Agent accepts multiple mobile-client connections with duplicate IP addresses, as long as they request different Home Agents or home networks. This behavior allows the use of unregistered IP addresses by multiple independent private networks.

A Home Agent does not accept multiple mobile-client connections to the same home network with duplicate IP addresses or overlapping subnet ranges. If a mobile client attempts to connect to a Home Agent with an address that duplicates or is within the same subnet of an established mobile-client connection, the Home Agent immediately terminates the *existing* client connection. This behavior allows a mobile client to reconnect if its connection is lost because a Foreign Agent became unavailable.

Network isolation and duplicate IP addresses

ATMP isolates home networks from each other as well as from other IP networks between the Foreign and Home Agents. A Foreign Agent can therefore accept multiple client connections that have the same IP address. For example, Figure 4-4 shows two mobile clients with the same IP address tunneling to two different home networks. The home networks are isolated from each other and from the IP cloud between the tunnel end points.

Figure 4-4. Foreign Agent supporting duplicate client IP addresses



To provide network isolation, a Foreign Agent does not create routes for mobile clients. Similarly, Gateway Home Agents do not create routes for ATMP gateway connections or for registered mobile clients. (However, Router Home Agents *do* create routes for registered mobile clients.) Network isolation is also the reason why a mobile client or a home network router does not receive a response when attempting to Ping a Foreign Agent or Home Agent.

Duplicate addresses connecting to the same home network

If a mobile client attempts to connect to a home network with an address that duplicates or is within the same subnet of an established mobile-client connection, the Home Agent immediately terminates the established connection and negotiates the incoming request. This behavior is required to enable a mobile client to reconnect if its connection is terminated when a Foreign Agent becomes unavailable.

For example, supposing a mobile client is connected to a home network with the following address:

```
10.10.10.10/24
```

The client's subnet range includes the addresses from 10.10.10.0 to 10.10.10.255. Supposing a second mobile client attempts to connect with the following address, which occupies the same subnet range as the first client:

```
10.10.10.199/24
```

The Home Agent terminates the first connection and allows the second mobile client to connect.

Configuring the agent-to-agent connection

The link between a Foreign Agent and Home Agent can be any kind of connection (switched, nailed, Frame Relay, and so forth) or an Ethernet link. It can be on a local network or routed through multiple hops. The only requirement is that the two units can communicate over an IP network.

For example, the following commands on a Home Agent configure an IP connection to a Foreign Agent. In this case, the Home Agent uses the `atmpfa` profile to authenticate the Foreign Agent dialing in.

```
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
```

For details about IP connections, see Chapter 2, "IP Routing."

Note: If the Foreign Agent and Home Agent reside on the same Ethernet and use RADIUS authentication, you must use separate RADIUS servers for the tunnel end points to avoid session loopbacks.

Configuring a Foreign Agent

To configure a Foreign Agent, you must set parameters in the ATMP profile, configure a Connection or RADIUS profile for the connection to the Home Agent, and configure mobile-client Connection or RADIUS profiles.

For information about configuring a connection to the Home Agent, see "Configuring the agent-to-agent connection" on page 4-7.

Foreign Agent ATMP profile settings

The ATMP profile contains the following parameters (shown with sample values) related to a Foreign Agent configuration:

```
[in ATMP]
agent-mode = foreign-agent
retry-timeout = 3
retry-limit = 10
mtu-limit = 0
force-fragmentation = no
```

Parameter	Usage for Foreign Agent configuration
Agent-Mode	Must specify Foreign-Agent.
Retry-Timeout Retry-Limit	Together, these parameters specify how many tunnel RegisterRequest and DeregisterRequest messages are sent and the number of seconds between each message. They have default settings that are appropriate for most sites. For details, see "Specifying tunnel retry limits" on page 4-4.
MTU-Limit	Specifies the maximum transmission unit (MTU) for the path between the Foreign and Home Agents. For details, see "Setting an MTU limit" on page 4-4.

Parameter	Usage for Foreign Agent configuration
Force-Fragmentation	If outdated client software sends large packets with the DF bit set, you can set this parameter to force the TAOS unit to fragment the packets anyway. For details, see “Forcing fragmentation for interoperation with outdated clients” on page 4-6.

Mobile client profile settings

All mobile-client profiles reside on the Foreign Agent side of the ATMP tunnel. A Foreign Agent can authenticate a mobile client locally in a Connection profile or externally in a RADIUS profile.

Settings in Connection profiles

The Tunnel-Options subprofile of a local Connection profile contains the following parameters (shown with sample values) related to a mobile-client connection:

```
[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 = ""
```

Parameter	Usage for mobile client configuration
Profile-Type	Must specify Mobile-Client.
Primary-Tunnel-Server	Must specify the system IP address or hostname of a Home Agent.
Secondary-Tunnel-Server	Specifies the system IP address or hostname of a secondary Home Agent. If a tunnel request to the first Home Agent fails, the Foreign Agent tries again with this host.
UDP-Port	Specifies a UDP port for one or both of the specified Home Agents. If the Home Agent specification includes a port number, that value overrides this parameter.
Password	Must specify the password, if any, that is in the ATMP profile of the Home Agent (up to 21 characters).
Home-Network-Name	If the Home Agent is operating in gateway mode, must specify the name of the gateway profile that defines the connection to the home network.

Settings in RADIUS profiles

RADIUS uses the following attribute-value pairs to specify mobile-client connections:

RADIUS Attribute	Value
Tunnel-Type (64)	Type of protocol used for the tunnel. To ensure forward compatibility, the TAOS-specific Tunneling-Protocol (127) attribute is converted into Tunnel-Type (value 4 means ATMP). To maintain backward compatibility, RADIUS accounting still generates the Tunneling-Protocol attribute.
Tunnel-Server-Endpoint (67)	System IP address or hostname of a Home Agent. The string can be followed by a colon and the UDP port number used on the ATMP Home Agent. To ensure forward compatibility, the Ascend-specific Ascend-Primary-Home-Agent (129) attribute is converted into Tunnel-Server-Endpoint.
Ascend-Secondary-Home-Agent (130)	System IP address or hostname of a secondary Home Agent. If a tunnel request fails with the first Home Agent, the Foreign Agent tries again with this host.
Ascend-Home-Agent-UDP-Port (186)	UDP port for one or both of the specified Home Agents. If the Home Agent specification includes a port number, that value overrides this parameter.
Tunnel-Password (69)	Password, if any, in the ATMP profile of the Home Agent, if any (up to 21 characters). To ensure forward compatibility, the Ascend-specific Home-Agent-Password (184) attribute is converted into Tunnel-Password. For more details, see “Tunnel authentication” on page A-33.
Tunnel-Private-Group-ID (81)	If the Home Agent is operating in gateway mode, you must use this attribute or the vendor-specific Ascend-Home-Network-Name (185) attribute to specify the name of the gateway profile that defines the connection to the home network.

When a standard RADIUS attribute for tunneling is available, you can specify either the standard attribute or the Ascend vendor attribute. For example, the following RADIUS profiles are equivalent:

```
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"
```

Specifying Home Agent addresses and port numbers

When a mobile client connects to a Foreign Agent, the Foreign Agent sends an ATMP RegisterRequest message to the IP address of the primary Home Agent. (If the Home Agent is specified as a hostname, the Foreign Agent first performs a DNS lookup.) Depending on the network configuration, the Foreign Agent might dial a connection to reach the Home Agent.

If the Foreign Agent does not receive a response to its request, it tries again. The number of retries is controlled by the Retry-Limit setting in the Foreign Agent's ATMP profile.

If the Foreign Agent still does not receive a response or if it receives a negative response (such as Home Network Unreachable), it attempts to repeat the procedure with the secondary Home Agent address. If there is no secondary Home Agent address specified or if the registration with the secondary Home Agent also fails, the mobile client is disconnected.

If the Home Agent ATMP profile specifies a UDP port number other than the default of 5150, you can specify that port number as part of the Home Agent address by appending a colon character (:) followed by the port number. The following commands specify the system IP address followed by a UDP port number for a primary and secondary Home Agent:

```
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
```

Or, in a RADIUS profile:

```
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
```

In this case, the Foreign Agent dials the connection to the primary Home Agent and requests a tunnel on port 8877. If that attempt fails, it dials the connection to the secondary Home Agent and requests a tunnel on port 4000. (If the address does not specify a port number, the Foreign Agent uses the value of the UDP-Port parameter in the mobile client Connection profile.) For example, with the following settings, the Foreign Agent dials the connection to the Primary tunnel server and requests a tunnel on port 8877:

```
admin> set primary-tunnel-server = 2.2.2.2

admin> set secondary-tunnel-server = ha2.company.com:6789

admin> set udp-port = 8877
```

If that attempt fails, the Foreign Agent dials the connection to the secondary tunnel server and requests a tunnel on port 6789.

Specifying the home network name

For definitions of Gateway and Router Home Agents, see “Home Agent ATMP profile settings” on page 4-17. For a mobile client tunnel to a *Gateway* Home Agent, you must specify the name of the gateway profile for connection to the home network. For example, suppose you are creating the following gateway profile on a Home Agent:

```
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
```

In the mobile client’s profile, you would specify the following home network name:

```
admin> set home-network-name = homenet
```

Or you would include one of the following settings in a RADIUS profile:

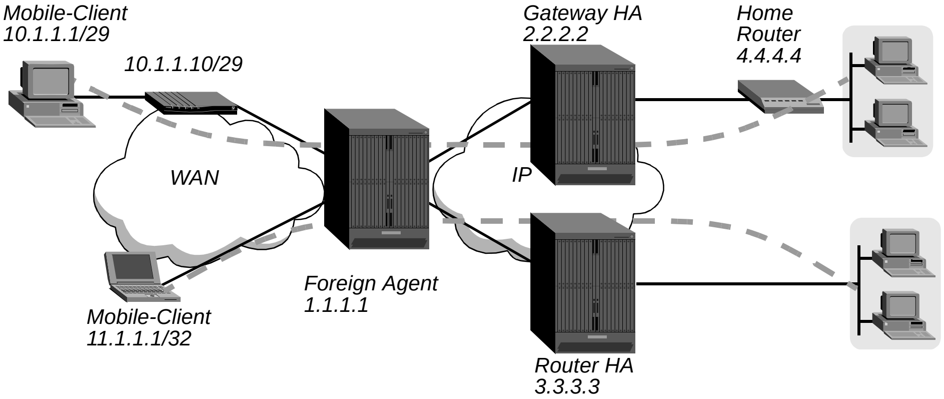
```
   Tunnel-Private-Group-ID = "homenet"

   Ascend-Home-Network-Name = "homenet"
```

Note: If the mobile client tunnels to a *Router* Home Agent, you must, in the mobile-client profiles, leave the Home-Network parameter blank or omit the Tunnel-Private-Group-ID or Ascend-Home-Network-Name attributes.

Example of a Foreign Agent configuration

Figure 4-5 shows a Foreign Agent that connects to two Home Agents across IP WAN connections. One is a Gateway Home Agent and the other is a Router Home Agent. The illustration also shows two mobile-client connections, one to each of the Home Agents.

Figure 4-5. Foreign Agent tunneling to two Home Agents



In this example, the WAN connections are multichannel PPP connections, which typically negotiate a path MTU of 1500 bytes. The agents set the MTU-Limit to 1472, to enable the connection end points to fragment packets at that size. For background information, see "Setting an MTU limit" on page 4-4.

Setting the Foreign Agent system address

The following commands set the Foreign Agent's system IP address:

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

admin> set system-ip-addr = 1.1.1.1

admin> write
IP-GLOBAL written
```

Configuring the Foreign Agent ATMP profile

The following commands configure a minimal ATMP profile:

```
admin> read atmp
ATMP read

admin> set agent-mode = foreign-agent

admin> set mtu-limit = 1472

admin> write
ATMP written

admin> reset
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

Configuring a connection to the Gateway Home Agent

In this example, the Gateway Home Agent has the following System-IP-Addr setting:

```
[in IP-GLOBAL]
system-ip-addr = 2.2.2.2
```

The following commands configure a Connection profile to the Gateway Home Agent:

```
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
```

Following are comparable RADIUS profiles:

```
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"
```

Configuring a connection to the Router Home Agent

In this example, the Router Home Agent has the following System-IP-Addr setting:

```
[in IP-GLOBAL]
system-ip-addr = 3.3.3.3
```

The following commands configure a Connection profile for the connection to the Router Home Agent:

```
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
```

Following are comparable RADIUS profiles:

```
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"
```

Configuring a mobile-client connection to the Gateway Home Agent

For the purposes of this example, the Gateway Home Agent has a nailed profile named Home-Router for connection to the home network. It also has the following settings in its ATMP profile:

```
[in ATMP]
agent-mode = home-agent
agent-type = gateway-home-agent
udp-port = 1555
password = tunnel-password
```

The following set of commands, entered on the Foreign Agent, configures a mobile-client connection to the Gateway Home Agent:

```
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
```

Following is a comparable RADIUS profile:

```
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"
```

Configuring a mobile-client connection to the Router Home Agent

For the purposes of this example, the Router Home Agent has the following settings in its ATMP profile:

```
[in ATMP]
agent-mode = home-agent
agent-type = router-home-agent
udp-port = 8877
password = tunnel-password
```

The next set of commands, entered on the Foreign Agent, configures a mobile-client connection to the Router Home Agent:

```
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
```

Following is a comparable RADIUS profile:

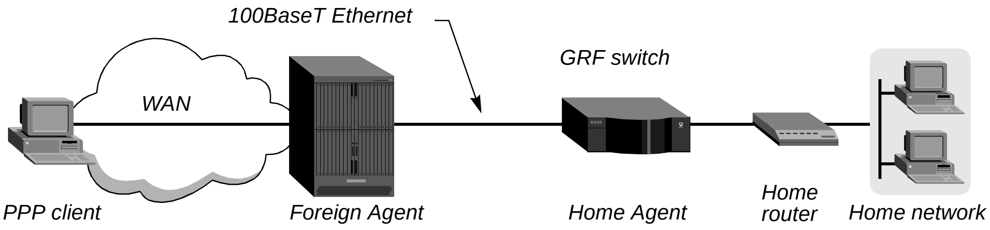
```
mobile-client-2 Password = "my-password", Service-Type= Framed-User
   Framed-Protocol = MPP,
   Ascend-IP-Route = Route-IP-Yes,
   Framed-IP-Address = 11.1.1.1,
   Framed-IP-Netmask = 255.255.255.255,
   Tunnel-Type = ATMP,
   Tunnel-Server-Endpoint = "3.3.3.3:8877",
   Tunnel-Password = "tunnel-password"
```

Example of a Foreign Agent that tunnels to a GRF switch

When a TAOS unit is operating as a Foreign Agent tunneling to a GRF switch Home Agent, setting the MTU-Limit parameter becomes a requirement rather than a recommendation. To maintain its very high throughput, the GRF does not perform packet reassembly. If an MTU-Limit value is not specified and a mobile client sends a large packet, the Foreign Agent might be forced to fragment the packet before sending it to the Home Agent. The GRF switch Home Agent drops such packets.

Figure 4-6 shows a Foreign Agent tunneling to a GRF Home Agent across a 100BaseT Ethernet segment.

Figure 4-6. Foreign Agent tunneling to a GRF switch



The following commands configure the Foreign Agent ATMP profile for the TAOS unit in Figure 4-6:

```
admin> read atmp
ATMP read

admin> set agent-mode = foreign-agent

admin> set mtu-limit = 1472

admin> write
ATMP written
```

Note: The GRF switch ATMP configuration must specify the same MTU-Limit value.

Configuring Home Agents

To configure an ATMP Home Agent, you must set parameters in the ATMP profile, configure an IP connection to the Foreign Agent, and configure the connection to the home network.

For information about configuring a connection to the Foreign Agent, see “Configuring the agent-to-agent connection” on page 4-7.

Home Agent ATMP profile settings

The ATMP profile contains the following parameters (shown with sample values) related to a Home Agent:

```
[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
```

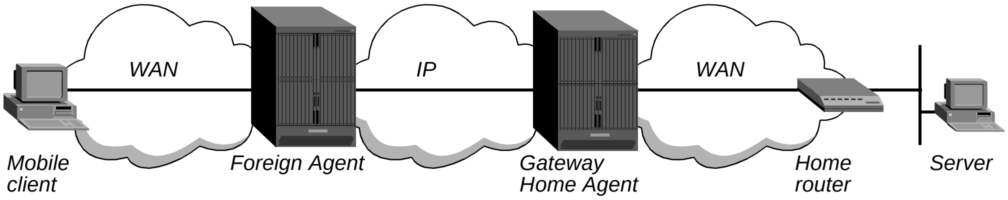
Parameter	Usage for Home Agent configuration
Agent-Mode	Must specify Home-Agent.
Agent-Type	Specifies Gateway-Home-Agent (the default) or Router-Home-Agent, depending on how the Home Agent accesses the home network.
UDP-Port	Specifies the UDP port Foreign Agents must use to establish tunnels with the Home Agent, as described in “Setting the UDP port” on page 4-3.
Password	Specifies the password Foreign Agents must supply to establish a tunnel with this unit. You can specify up to 21 characters.
Retry-Timeout Retry-Limit	Together, these parameters specify how many tunnel RegisterRequest and DeregisterRequest messages are sent and the number of seconds between each message. The default settings are appropriate for most sites, as described in “Specifying tunnel retry limits” on page 4-4.
Idle-Timer	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.
MTU-Limit	Specifies the maximum transmission unit (MTU) for the path between the Foreign and Home Agents, as described in “Setting an MTU limit” on page 4-4.
Force-Fragmentation	Enables/disables prefragmentation of packets that have the DF bit set, as described in “Forcing fragmentation for interoperation with outdated clients” on page 4-6.

Specifying a Gateway Home Agent

A Gateway Home Agent delivers tunneled data to the home network without routing. A Gateway Home Agent cannot ping or otherwise communicate with the home router. (The same restriction applies in the other direction.)

When the Gateway Home Agent receives tunneled data, it removes the GRE header and forwards the packets to the home router, as shown in Figure 4-7.

Figure 4-7. How a Gateway Home Agent works



The link to the home network cannot be a regular switched dial-out connection, because the Home Agent will not dial the connection upon receipt of tunneled data. If the gateway connection is down when the Home Agent receives a tunnel request, it rejects the request. For more details about the gateway connection to the home network, see “Home network gateway profile settings” on page 4-19.

Following is an example of specifying a Gateway Home Agent:

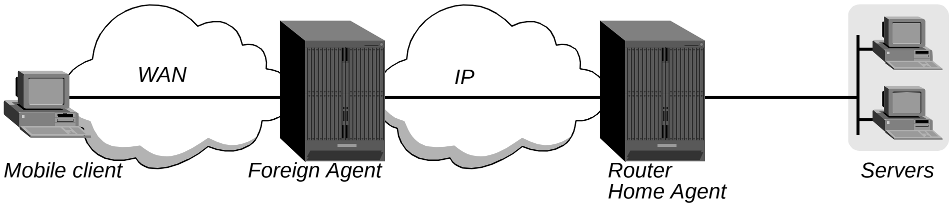
```
admin> read atmp
ATMP read

admin> set agent-mode = home-agent

admin> set agent-type = gateway-home-agent

admin> write
ATMP written

admin> reset
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

Specifying a Router Home Agent

A Router Home Agent relies on packet routing to reach the home network, as shown in Figure 4-8.

Figure 4-8. How a Router Home Agent works



When the Router Home Agent receives tunneled data, it removes the GRE encapsulation, passes the packets to its router software, and adds a route to the mobile client. If the mobile client is a PPP client, it adds a host route. If the mobile client is a router, such as a Pipeline unit, the Router Home Agent adds a regular route to the subnet addresses assigned to that router.

Following is an example of specifying a Router Home Agent:

```
admin> read atmp
ATMP read

admin> set agent-mode = home-agent
admin> set agent-type = router-home-agent

admin> write
ATMP written

admin> reset
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

Specifying the tunnel password

The Home Agent typically requests a password before establishing a tunnel. The Foreign Agent returns an encrypted version of the password found in the mobile-client profile. For details, see “Tunnel authentication” on page A-33.

Setting an idle timer for unused tunnels

When a mobile client disconnects normally, the Foreign Agent sends a request to the Home Agent to close down the tunnel. However, when a Foreign Agent restarts, tunnels that were established to a Home Agent are not normally cleared, because the Home Agent is not informed that the mobile clients are no longer connected. The unused tunnels continue to occupy memory on the Home Agent. To enable the Home Agent to reclaim the memory held by unused tunnels, you can now set an inactivity timer on a Home Agent by changing the default value of the following parameter:

```
[in ATMP]
idle-timer = 0
```

The inactivity timer runs only on the Home Agent side. Its value specifies the number of minutes (1 to 65535) that the Home Agent maintains an idle tunnel before disconnecting it. A value of 0 disables the timer, which means that idle tunnels remain connected forever. The setting affects only tunnels created after the timer was set. Tunnels that existed before the timer was set are not affected by it.

Home network gateway profile settings

When a Gateway Home Agent receives a tunnel RegisterRequest message from the Foreign Agent, it checks the status of the connection to the home network. If the connection is down, the Home Agent rejects the tunnel request and does not attempt to dial the connection. If the connection goes down after a tunnel is established, all mobile clients that were using it are disconnected.

The gateway connection to the home network can be a nailed connection or a regular dial-in switched connection. Using an incoming connection from the home router enables the administrator of the home network to regulate when mobile clients can access the network. For example, the administrator of the home network could configure an access router to dial the Home Agent every weekday at 8:00 a.m. and disconnect at 5:00 p.m., thereby limiting mobile client access to those hours. In that case, the gateway connection must be up before mobile clients dial in, or their tunnel requests will fail.

To configure a gateway profile, set up a nailed or dial-in connection and specify the following parameters (shown with sample settings) in the Connection profile:

```
[in CONNECTION/gwprofile]
station* = gwprofile

[in CONNECTION/gwprofile:tunnel-options]
profile-type = gateway-profile
max-tunnels = 0
atmp-ha-rip = rip-send-v2
```

Parameter	Usage for gateway profile configuration
Station	Specifies the name of the home router. The Home-Network-Name value specified in the mobile-client profile on the Foreign Agent must specify the same name.
Profile-Type	Must specify Gateway-Profile.
Max-Tunnels	Specifies the maximum number of mobile clients that can use the connection, all at the same time, to tunnel into the home network. The default value of 0 sets no limit.
ATMP-HA-RIP	Enables/disables construction of mobile-client routes in RIP-v2 responses to the home router. This parameter does not apply unless Profile-Type is set to Gateway-Profile. The parameter operates independently of the RIP parameter in the IP-Options subprofile. For gateway profiles, the IP-Options RIP parameter must be Off.

Limiting the maximum number of tunnels

If you decide to limit the maximum number of tunnels a gateway will support, you should consider the expected traffic per mobile-client connection, the bandwidth of the connection to the home network, and the availability of alternative Home Agents (if any). For example, the lower the amount of traffic generated by each mobile-client connection, the more tunnels a gateway connection will be able to handle.

Enabling RIP on the interface to the home router

ATMP-HA-RIP enables the Gateway Home Agent to inform the home router about routes to its mobile clients. This eliminates the requirement for the home router to maintain a static route for each ATMP mobile client. It also provides the basis for a resilient configuration, in which a secondary Home Agent can take over for a primary Home Agent if the primary agent becomes unavailable.

Informing the home router about routes to mobile clients

The router at the far end of the connection defined by the gateway profile must be able to route back to mobile clients. The easiest way to accomplish this is by setting the ATMP-HA-RIP parameter to RIP-Send-v2. With this setting, the Gateway Home Agent constructs a RIP-v2 Response(2) packet at every RIP interval and sends it to the home network from all tunnels using the gateway profile. For each tunnel, the Response packet contains the mobile-client IP address, the subnet mask, a next hop of 0.0.0.0, and a metric of 1. RIP-v2 authentication and route tags are not supported.

The following commands enable ATMP-HA-RIP in the gateway profile for the connection to the home router:

```
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
```

Note: The Home Agent will not inspect RIP updates coming from the home network, regardless of the RIP setting in the IP-Options subprofile. If the Home Agent receives RIP updates from the home network, it forwards the update packets to the mobile clients, as it would any other type of packet.

The alternative: Maintaining static routes in the home router

If the gateway profile does *not* set ATMP-HA-RIP to RIP-Send-v2, the administrator of the home network must configure a static route to each mobile client. A static route to a mobile client can be specific to the client, in which case the route's destination is the mobile-client IP address and the next-hop router is the Home Agent address. For example, in the following route the mobile client is a router (this is not a host route), and the Home Agent address is 2.2.2.2:

```
[in IP-ROUTE/mobile-client]
destination = 10.1.1.10/29
gateway = 2.2.2.2
```

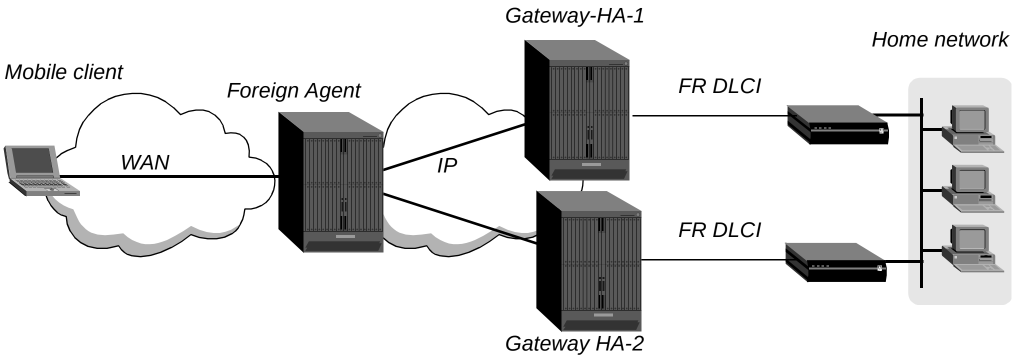
Or, if the mobile clients have addresses allocated from the same address block (including router mobile-client addresses with subnet masks of less than 32 bits) and no addresses from that block are assigned to other hosts, the home network administrator can specify a single static route that encompasses all mobile clients that use the same Home Agent. For example, in the following route all mobile clients are allocated addresses from the 10.4.*n.n* block (and no other hosts are allocated addresses from that block), and the Home Agent address is 2.2.2.2:

```
[in IP-ROUTE/mobile-clients]
destination = 10.4.0.0/16
gateway = 2.2.2.2
```

Routing in a resilient installation

A resilient ATMP installation supports multiple ATMP paths to the same home network, providing resiliency in the event of Home Agent failure or failure of the link between a Home Agent and home router. The two Home Agents might connect to two home routers, as shown in Figure 4-9, or the Home Agents might connect to the same home router.

Figure 4-9. Resilient ATMP installation



Mobile clients access the home network through one of the Home Agents, but not always the same Home Agent. Therefore, a static route maintained by the home router would not allow hosts on the home network to reliably send packets back to mobile clients. ATMP-HA-RIP resolves the routing problems that could occur in a resilient configuration.

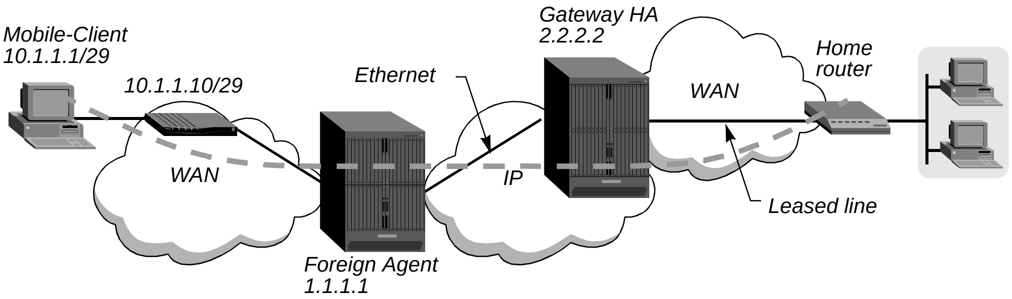
The following example shows a gateway profile that could reside in both of the Home Agents shown in Figure 4-9:

```
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
```

Example of a Gateway Home Agent configuration

Figure 4-10 shows a Gateway Home Agent with a fractional T1 connection to the home network. For details about fractional T1, see the *APX 8000/MAX TNT Physical Interface Configuration Guide*.

Figure 4-10. Gateway Home Agent with leased line to home network



Note: In this example, the ATMP Foreign Agent and Home Agent are on the same Ethernet segment, so no Connection profiles are required for communication.

Setting the Home Agent's system address

The following commands set the Home Agent's system IP address:

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

admin> set system-ip-addr = 2.2.2.2

admin> write
IP-GLOBAL written
```

Configuring the Home Agent ATMP profile

The following commands configure the Home Agent ATMP profile, with the default setting of Gateway-Home-Agent for the Agent-Type parameter:

```
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
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

The Foreign Agent has an ATMP profile such as the following:

```
[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
```

Configuring a gateway profile for connection to the home network

In the following set of commands, which configure the interface to the home network, Call-Type is set to FT1 (nailed) and a group of nailed channels (group number 7) is assigned to the link. ATMP-HA-RIP is enabled on the interface.

```
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
```

Configuring a mobile-client connection to the Gateway Home Agent

Mobile-client connections on the Foreign Agent will require a tunnel configuration such as the following in a local Connection profile:

```
[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
```

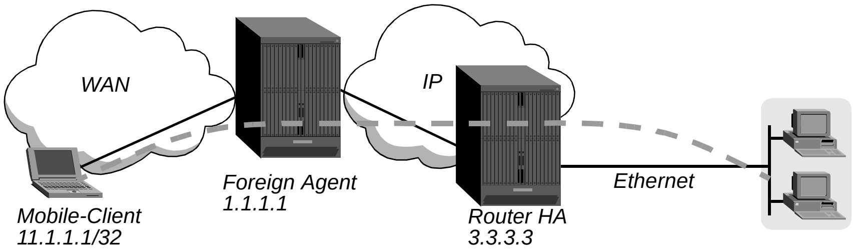
or comparable settings in a RADIUS profile:

```
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"
```

Example of a Router Home Agent configuration

Figure 4-11 shows a Router Home Agent with an Ethernet connection to the home network. The ATMP Foreign Agent and Home Agent connect across a multichannel PPP link.

Figure 4-11. Router Home Agent on the home network



For information about configuring a connection to the Foreign Agent, see “Configuring the agent-to-agent connection” on page 4-7.

Setting the Home Agent’s system address

The following commands set the Router Home Agent’s system IP address:

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

admin> set system-ip-addr = 3.3.3.3

admin> write
IP-GLOBAL written
```

Configuring the IP-Interface profile for the connection to the home network

If you enable RIP on the interface that leads to the home network, other hosts and networks can route to the mobile client. Enabling RIP is particularly useful if the home network is one or more hops away. If RIP is turned off, intervening routers require static routes that specify the Home Agent as the route to mobile clients. You can also turn on proxy ARP to allow local hosts to ARP for mobile clients. For example:

```
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
```

Configuring the Home Agent's ATMP profile

The following commands configure the Home Agent's ATMP profile:

```
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
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

The Foreign Agent has an ATMP profile such as the following:

```
[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
```

Configuring a mobile-client connection to the Router Home Agent

Mobile-client connections on the Foreign Agent require a tunnel configuration such as the following in a local Connection profile:

```
[in CONNECTION/mclient:tunnel-options]
profile-type = mobile-client
primary-tunnel-server = 3.3.3.3
password = tunnel-password
```

Or this type of connection requires comparable tunnel settings in a RADIUS profile:

```
mclient Password = "local-password"
   Service-Type = Framed-User,
   Tunnel-Type = ATMP,
   Tunnel-Server-Endpoint = "3.3.3.3",
   Tunnel-Password = "tunnel-password"
```

Configuring a Home-and-Foreign Agent

In some configurations, a TAOS unit acts as a Home Agent for some mobile clients and as a Foreign Agent for others. The two configurations operate side-by-side without any conflict, provided that all requirements are met for each type of configuration.

Configuring the ATMP profile

The ATMP profile contains the following parameters (shown with sample values) related to the Home-and-Foreign-Agent configuration:

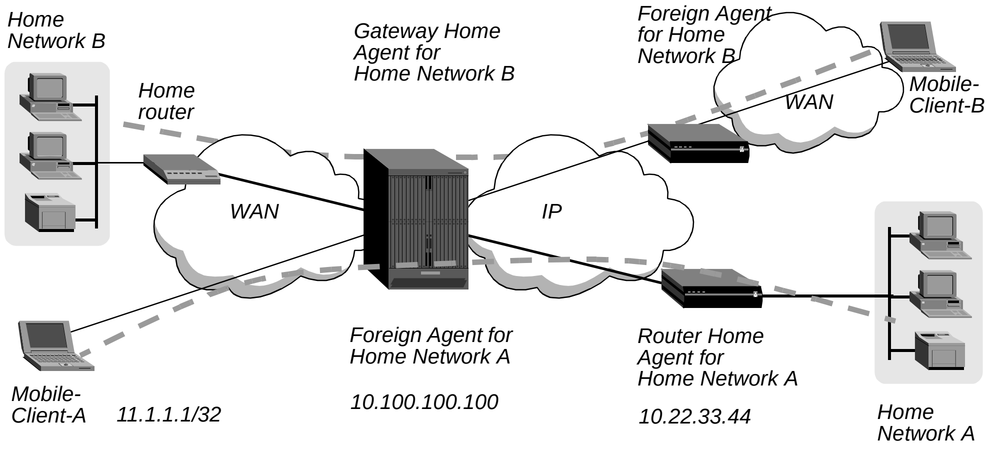
```
[in ATMP]
agent-mode = home-and-foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = tunnel-password
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

The Agent-Mode parameter must specify Home-and-Foreign-Agent. For details about all of the other settings, see “Configuring Home Agents” on page 4-16 or “Configuring a Foreign Agent” on page 4-8.

Example of a Home-and-Foreign Agent configuration

Figure 4-12 shows a TAOS unit operating as Home Agent for Home Network B and as Foreign Agent for mobile clients tunneling into Home Network A.

Figure 4-12. TAOS unit acting as both Home Agent and Foreign Agent


Home Network B
Home router
Gateway Home Agent for Home Network B
Foreign Agent for Home Network B
WAN
Mobile-Client-B
WAN
IP
Mobile-Client-A
11.1.1.1/32
Foreign Agent for Home Network A
10.100.100.100
Router Home Agent for Home Network A
10.22.33.44
Home Network A

For information about configuring connections between Home Agents and Foreign Agents, see "Configuring the agent-to-agent connection" on page 4-7.

Setting the system address

The following commands set the Home-and-Foreign Agent's system IP address:

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

admin> set system-ip-addr = 10.100.100.100

admin> write
IP-GLOBAL written
```

Configuring the ATMP profile for Home-and-Foreign Agent

The following set of commands configures the ATMP profile:

```
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
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

The Foreign Agent for Home Network B has an ATMP profile such as the following:

```
[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
```

The Home Agent for Home Network A has an ATMP profile such as the following:

```
[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
```

Configuring a mobile-client profile

The following set of commands configures a Connection profile for Mobile-Client-A in Figure 4-12. For this profile, the TAOS unit is operating as Foreign Agent to enable the mobile client to tunnel to Home Network 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
```

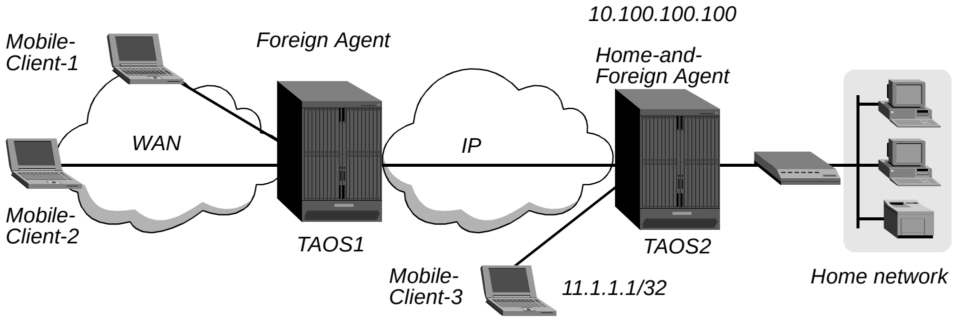
Following is a comparable RADIUS profile:

```
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"
```

Another example of a Home-and-Foreign Agent configuration

Figure 4-13 shows another configuration that makes use of the Home-and-Foreign-Agent setup. In this example, all three mobile clients want to tunnel to the home network, using TAOS2 as their Home Agent. The two ATMP units are geographically distant.

Figure 4-13. Enabling a mobile client to bypass the Foreign Agent connection



Mobile-Client-1 and Mobile-Client-2 make local calls to dial in to the Foreign Agent (TAOS1) and then tunnel to the Home Agent. However, Mobile-Client-3 is geographically closer to TAOS2, and would prefer to dial directly in to TAOS2. In this case, TAOS2 is configured to provide both Home Agent and Foreign Agent functionality to Mobile-Client-3. There is no need to encapsulate data to and from Mobile-Client-3 in GRE. The data comes in on one of TAOS2's interfaces and it is sent to another interface without encapsulation processing, but with all of the network isolation benefits that ATMP provides.

Setting the system IP address

The following commands set the Home-and-Foreign Agent's system IP address:

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

admin> set system-ip-addr = 10.100.100.100

admin> write
IP-GLOBAL written
```

Configuring the ATMP profile for Home-and-Foreign Agent

The following commands configure the ATMP profile in 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
```

Note: When you change the Agent-Mode parameter from its default Tunnel-Disabled setting to any other setting, you must reset the system for the new value to take effect.

TAOS1 has an ATMP profile such as the following:

```
[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
```

Configuring a profile for Mobile-Client-3

The next set of commands configures a Connection profile for Mobile-Client-3 in Figure 4-13. For this profile, the TAOS unit is operating as both Foreign Agent and Home Agent.

```
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
```

Following is a comparable RADIUS profile:

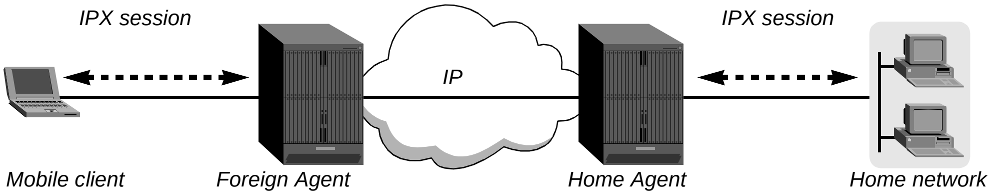
```
mobile-client-3 Password = "local-password"
   Service-Type = Framed-User,
   Framed-Protocol = MPP,
   Ascend-IP-Route = Route-IP-Yes,
   Framed-IP-Address = 11.1.1.1,
   Framed-IP-Netmask = 255.255.255.255,
   Tunnel-Type = ATMP,
   Tunnel-Server-Endpoint = "10.100.100.100:6789",
   Tunnel-Password = “tunnel-password”
```

Configuring IPX over ATMP

IPX ATMP enables ATMP mobile clients to tunnel into an IPX home network. The mobile clients can be dial-up IPX clients or dial-up terminal adapters, but not IPX routers.

IPX packets are encapsulated (GRE) through the tunnel, so the connection between the Foreign Agent and Home Agent does not require IPX routing. However, IPX routing is required for the connection between the mobile client and the Foreign Agent, and for the connection between the Home Agent and the home network, as shown in Figure 4-14.

Figure 4-14. IPX routing connections for IPX ATMP



For details about configuring IPX, see Chapter 7, "IPX Routing."

For information about configuring connections between Home Agents and Foreign Agents, see "Configuring the agent-to-agent connection" on page 4-7.

Configuring the agents for IPX routing

For details about configuring TAOS units to route IPX, see Chapter 7, "IPX Routing." The following commands configure a minimal IPX configuration to enable a TAOS unit to route IPX packets:

```
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
```

In addition to routing IPX, the Foreign Agent should typically define a unique IPX network for use in assigning addresses to NetWare dial-in clients. For example:

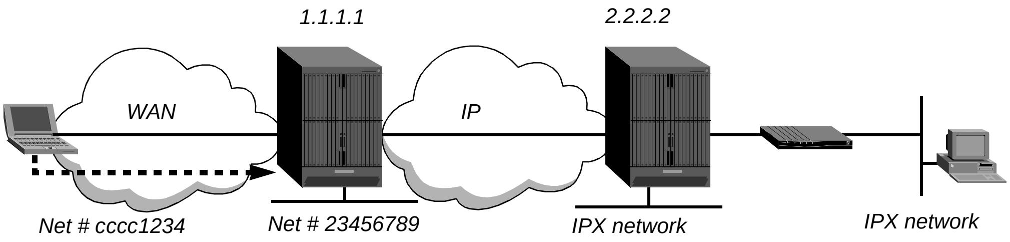
```
admin> read ipx-global
IPX-GLOBAL read

admin> set ipx-dialin = cccc1234

admin> write
IPX-GLOBAL written
```

Example of IPX ATMP to a Gateway Home Agent

After configuring the IP connection between the two agents (as described in "Configuring the agents for IPX routing" on page 4-31) and enabling IPX routing in the Foreign Agent, you must configure the IPX connections between the mobile client and Foreign Agent, and between the Home Agent and home network.

In this example, illustrated in Figure 4-15, the mobile client is running Windows 98 with IPX enabled. The mobile client is assigned an address on the virtual IPX network defined in the Foreign Agent’s IPX-Global profile (CCCC1234).

Figure 4-15. IPX ATMP with a Gateway Home Agent



The Gateway Home Agent communicates with a Pipeline unit configured for IPX routing (the home router). After the configurations described in the following subsections have been set up, the mobile client can dial in to the Foreign Agent and once connected, click on the NetworkNeighborhood icon to display the destination NetWare server and its contents.

Configuring a mobile-client IPX connection

The following set of commands configures a Connection profile for the mobile client in Figure 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
```

Following is a comparable RADIUS profile:

```
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"
```

Example of a gateway profile IPX connection

The link between the Gateway Home Agent and the home network can be Frame Relay or nailed, but it cannot be a switched connection. (Data received through a tunnel does not cause the Gateway Home Agent to bring up the link.)

The Gateway Home Agent must be configured for IPX. (See “Configuring the agents for IPX routing” on page 4-31.)

The following commands configure a Connection profile for the connection to the home router. Note that IPX RIP and Service Advertising Protocol (SAP) are disabled in the profile, to prevent RIP and SAP information from being propagated from the Home Agent to the home network.

```
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
```

IPX home router requirements

The Pipeline unit acting as home router requires an IPX-routing Connection profile for the connection to the Gateway Home Agent and a static IPX route to the mobile client. When the Home Agent is a Gateway, the home router requires a static IPX route to the mobile client. The destination network number of that route is the IPX network number used by the mobile client. The static route’s destination node number must be the Ethernet MAC address of the Home Agent’s shelf-controller Ethernet port. The MAC-Address setting is visible in the Ether-Info profile on the Home Agent. For example, the following profile shows the MAC address 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
```

In the sample static route that follows, the destination network number is CCCC1234 (the virtual network assigned to the client by the Foreign Agent), and the destination node number is the MAC address of the Home Agent's shelf-controller Ethernet port. The Connection # parameter specifies the number of the Pipeline unit's IPX-routing Connection profile for the connection to the Gateway Home Agent.

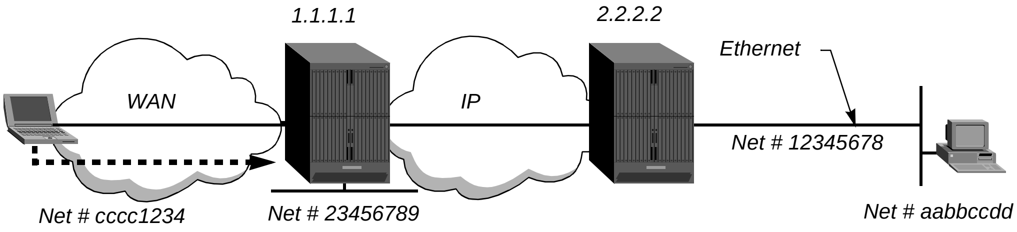
```
Ethernet
  IPX Route
   Mobile-Client-1
     Server Name=
     Active=Yes
     Network=cccc1234
     Node=0c07b6b9fd6
     Socket=
     Server Type=0
     Hop Count=2
     Tick Count=12
     Connection #=1
```

Example of IPX ATMP to a Router Home Agent

After configuring the IP connection between the two agents (as described in "Configuring the agent-to-agent connection" on page 4-7), you must configure the IPX connections between the mobile client and Foreign Agent, and between the Home Agent and home network.

In Figure 4-16, the mobile client is running Windows 98 with IPX enabled. The mobile client is assigned an address on the virtual IPX network defined in the Foreign Agent's IPX-Global profile (CCCC1234).

Figure 4-16. IPX ATMP with a Router Home Agent



After the configurations described in the following subsections have been set up, the mobile client can dial in to the Foreign Agent and once connected, click on the NetworkNeighborhood icon to display the destination NetWare server and its contents.

Configuring a mobile-client IPX connection

The following set of commands configures a Connection profile for the mobile client in Figure 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
```

Following is a comparable RADIUS profile:

```
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”
```

Example of an IPX Router Home Agent configuration

In this example, the Router Home Agent resides on the home network, so a Connection profile is not needed. (In other setups, the Router Home Agent could communicate with another IPX router across a nailed connection.) On the Router Home Agent, the following commands configure a local Ethernet interface as the IPX home network:

```
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
```

L2TP, L2F, PPTP, and IP-in-IP Tunneling

5

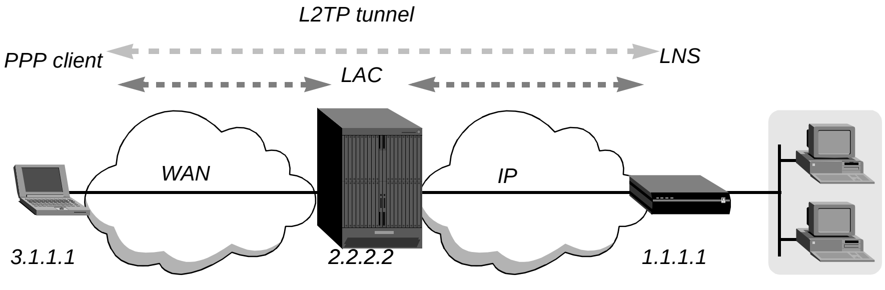
Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) provides tunneling at OSI Layer 2 (at the HDLC layer of a PPP connection). An APX 8000 or MAX TNT unit can currently operate only as an L2TP access concentrator (LAC), which means that the unit receives incoming PPP calls and initiates a connection to an L2TP network server (LNS).

Components of an L2TP tunnel

Figure 5-1 shows the elements of an L2TP tunnel. A PPP client (referred to as the *mobile client*) dials in across an asynchronous or synchronous link, using any protocol that can be carried within PPP. The TAOS unit answers the call and passes it to the LNS. LAC-to-LNS communication requires IP connectivity.

Figure 5-1. L2TP tunneling



The mobile client can be any PPP client. For example, it could be a Pipeline unit dialing a digital call, or a PC running Windows NT dialing a modem call.

The link between the LAC and the LNS can be a switched or nailed connection, or it can be an Ethernet link. The connection to the LNS is an IP link, which consists of a control link and zero or more data links. Both the control and data links are encapsulated in UDP.

The control link carries information that is used both to query whether the LNS will accept the current call and to establish a tunnel. L2TP implements a Hello mechanism by which the LAC and LNS verify that the other is still alive. They do this by sending each other a control message every minute or so. If the Hello message does not arrive for several minutes, the tunnel and all the tunneled connections are brought down.

Data links carry the client data, which consists of PPP frames. There is one data link per tunneled client connection.

Overview of tunneling parameters

The following parameters (shown with default values) can be used to configure L2TP, L2F, PPTP, and IP-in-IP tunneling:

```
[in SYSTEM]
name = ""

[in CONNECTION/"":tunnel-options]
profile-type = disabled
tunneling-protocol = atmp-protocol
primary-tunnel-server = ""
secondary-tunnel-server = ""
password = ""
client-auth-id = ""
server-auth-id = ""
assignment-id = ""


[in L2-TUNNEL-GLOBAL]
l2tp-system-name = ""
l2f-system-name = ""
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0


[in TUNNEL-SERVER/""]

server-endpoint* = ""
enabled = yes
shared-secret = ""
client-auth-id = ""
server-auth-id = ""
```

Parameter	Specifies
System > Name	Name sent to the tunnel server for authenticating the tunnel if Client-Auth-ID is not specified, and L2TP-System-Name or L2F-System-Name is not specified. See “How the system name is selected (Hostname AVP)” on page 5-11. If the domain name is configured in the IP-Global profile, the specified system name is concatenated with the domain name.
Connection > *Any-Connection* > Tunnel-Options > Profile-Type	Type of tunneling profile. Set to `mobile-client` for PPP clients using L2TP, L2F tunneling, or IP-in-IP tunneling.

Parameter	**Specifies**
Connection > *Any-Connection* > Tunnel-Options > Tunneling-Protocol	Protocol used to establish the tunnel. Specify one of the following values: • `disabled`—Tunneling is disabled. • `pptp-protocol`—Point-to-Point Tunneling Protocol (PPTP) • `l2f-protocol`—Layer 2 Forwarding (L2F) • `l2tp-protocol`—Layer 2 Tunneling Protocol (L2TP) • `atmp-protocol`—Ascend Tunnel Management Protocol (ATMP) • `ipinip-protocol`—IP-in-IP encapsulation (RFC 2003)
Connection > *Any-Connection* > Tunnel-Options >Primary-Tunnel-Server	DNS hostname or dotted-decimal IP address of the Tunnel Server end point (the intermediate destination that will decapsulate the IP packets). If it specifies a hostname, the TAOS unit executes a DNS lookup for the host’s address. If the name is invalid, the mobile client call is cleared with the reason for failure set to DIS_TS_ERR_HOSTNAME. If the primary server is unavailable, the system attempts to establish a tunnel to the secondary server.
Connection > *Any-Connection* > Tunnel-Options > Secondary-Tunnel-Server	IP address or hostname of a secondary tunnel end point. If a DNS lookup returns several IP addresses, the system attempts to establish a tunnel to each address in turn. If the primary server is unavailable, the system attempts to establish a tunnel to the secondary server. This parameter is valid for L2F and L2TP tunnels.
Connection > *Any-Connection* > Tunnel-Options > Password	Password used for authenticating the tunnel.
Connection > *Any-Connection* > Tunnel-Options > Client-Auth-ID	Name sent to the tunnel server for authenticating the tunnel. The name can contain up to 31 characters. Note that L2F does not support Client-Auth-ID or Server-Auth-ID from a Tunnel-Server profile. For more details, see “How the system name is selected (Hostname AVP)” on page 5-11.
Connection > *Any-Connection* > Tunnel-Options > Server-Auth-ID	Name sent from the tunnel server to the system initiating the tunnel during the tunnel authentication phase. The name can contain up to 31 characters. Note that this field is currently ignored if it is specified in a Connection profile. Note that L2F does not support Client-Auth-ID or Server-Auth-ID from a Tunnel-Server profile.
Connection > *Any-Connection* > Tunnel-Options > Assignment-ID	Identification (name) assigned to tunnels to allow grouping sessions, a text string of up to 31 characters. The value has local significance only. It is not transmitted to the remote tunnel end point.

Parameter	**Specifies**
L2-Tunnel-Global > L2TP-System-Name or L2F-System-Name	Name (up to 31 characters) sent to the tunnel server (LNS) when initiating an L2TP or L2F tunnel and is send when Client-Auth-ID is not specified. See "How the system name is selected (Hostname AVP)" on page 5-11.
L2-Tunnel-Global > L2TP-Mode	Enable/disable L2TP operations. Specify LAC to enable L2TP operations in the TAOS unit.
L2-Tunnel-Global > L2TP-Auth-Enabled	Enable/disable L2TP tunnel authentication. With the Yes setting, the TAOS unit uses the Shared-Secret value to authenticate the LNS before bringing up an L2TP control channel.
L2-Tunnel-Global > L2TP-Rx-Window	Advertised L2TP receive window size for data channels. The default, 0 (zero), specifies that the TAOS unit ask for no flow control for inbound L2TP payloads. Enter a value between 0 and 63. A nonzero value enables behavior that predates RFC 2661. Not all L2TP implementations support a nonzero value.
Tunnel-Server > *Any profile* > Server-Endpoint	DNS hostname or dotted-decimal IP address of the LNS end point. If this setting is a hostname, the TAOS unit executes a DNS lookup for the host's address.
L2TP-Config > Enabled	Enable/disable tunnels to the specified Server-Endpoint.
L2TP-Config > Shared-Secret	Shared secret for authenticating L2TP tunnels. For details, see "Tunnel authentication" on page A-33.
L2TP-Config > Control-Connect-Establish-Timer	Maximum number of seconds during which the TAOS unit can establish an L2TP tunnel with another unit. Enter an integer from 0 to 600. The default is 60.
L2TP-Config > First-Retry-Timer	Initial interval, in milliseconds, that the TAOS unit waits before making a second attempt to establish an L2TP tunnel with another unit. Enter an integer from `100` to `5000`. The default is `1000`.
L2TP-Config > Hello-Timer	Interval, in seconds, between Hello messages that the TAOS unit sends to another unit. Specify an integer from 0 to 600. The default is 60. The 0 setting specifies that the TAOS unit sends no Hello messages.
L2TP-Config > LAC-Incoming-Call-Timer	Number of seconds that the TAOS unit waits for call setup to complete. Specify an integer from 1 to 600. The default is 60.
L2TP-Config > Retry-Count	Maximum number of times that the TAOS unit attempts to establish a tunnel. Specify a decimal number from 1 to 10 (the default).

Overview of RADIUS attribute-value pairs

RADIUS supports this tunneling by using the following attribute-value pairs. These attribute-value pairs support tag fields, as described in RFC 2868. Each tag value (from 1 to 31) defines an independent tunnel attempt description. The Tunnel-Client-Auth-ID and Tunnel-Server-Auth-ID attributes can be specified in Access-Response packets and are generated in Accounting-Request packets. For additional information about RADIUS tunnel attributes, see "Overview of attribute sets and tags" on page 5-35.

Example of L2TP settings in RADIUS profiles

The following commands configure L2TP operations with an LNS named 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 = 4

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
```

Configuring L2TP mobile-client profiles

If a PPP client's profile is configured to initiate an L2TP tunnel, the TAOS unit attempts to open a tunnel after initial authentication of the connection. It can open a tunnel after preauthenticating the call (using CLID or DNIS authentication) or after authenticating the caller's name and password.

If the LAC opens a tunnel after preauthenticating the call, the LNS performs all PPP negotiations and the termination of the PPP connection. Even if the LAC has password authenticated a call, the LNS can (and probably should, for security reasons) authenticate again. The LAC and LNS can use different PPP authentication protocols without restriction.

Note: Because of tunneling protocol requirements, the LNS can authenticate a tunneled call only by using a PPP authentication protocol. The LNS cannot use terminal-server authentication for tunneled calls. For the system to use CLID or DNIS to preauthenticate a call, the telco switch must send the information as part of the call, and the TAOS unit must be configured to extract and use the information.

For details about preauthentication and password authentication, see Appendix A, "Authentication Methods."

Proxy LCP and authentication for L2TP tunnels

If a LAC authenticates a PPP client's dial-in call by means of a name and password, it negotiates Link Control Protocol (LCP) with the client and then opens the PPP Auth state. In earlier software versions, the information obtained from authentication and LCP negotiation on the LAC was not forwarded, so the LNS had to restart negotiation with the client. In the current software version, the LAC forwards relevant LCP information (*proxy LCP*) and the caller's name and password (*proxy authentication*). This feature provides quicker connection of the client, because the LNS does not need to restart negotiation.

With proxy LCP, the LAC sends the following information to the LNS:

- The first LCP Config Request packet received from the client
- The last LCP Config Request packet received from the client
- The last LCP Config Request packet the LAC sent to the client

With proxy authentication, the LAC initiates PPP authentication of the dial-in call and then sends the caller's name and password to the LNS in the appropriate L2TP attribute-value pairs. The LNS can then complete PPP authentication.

Proxy LCP and authentication occur for digital calls that are authenticated through any PPP authentication protocol (such as PAP, CHAP, or MS-CHAP) but not for analog PPP connections authenticated by a terminal-server login. For security reasons, the terminal server erases the caller's name and password immediately after authenticating the user.

Examples of opening a tunnel after preauthenticating the call

To enable the TAOS unit to preauthenticate a call, it must be configured to extract and use CLID or DNIS information. For details, see Appendix A, "Authentication Methods."

Examples using CLID authentication

The following commands configure a profile that opens an L2TP tunnel to an LNS (1.1.1.1) after verifying the caller-ID:

```
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-server = 1.1.1.1

admin> write
CONNECTION/l2test written
```

Following is a comparable RADIUS profile:

```
5551000 Password = “Ascend-CLID”, Service-Type = Call-Check
   Tunnel-Type = L2TP,
   Tunnel-Medium-Type = IP,
   Tunnel-Server-Endpoint = “1.1.1.1”
```

Examples using DNIS

The following commands configure a profile that opens an L2TP tunnel to an LNS named L2TP-1 if the dialed number is 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-server = l2tp-1.example.com

admin> write
CONNECTION/tunnelcx
```

Following is a comparable RADIUS profile:

```
8001234567 Password = “Ascend-DNIS”, Service-Type = Call-Check
   Tunnel-Server-Endpoint = “l2tp-1.example.com”,
   Tunnel-Type = L2TP,
   Tunnel-Medium-Type = IP
```

Examples of opening a tunnel after password authentication

In these examples, the TAOS unit negotiates the PPP call, including password authentication, and then opens the L2TP tunnel. For details about PPP authentication, see “Authenticating framed protocol sessions” on page A-6.

The following commands create a Connection profile that includes a PPP password. The TAOS unit authenticates the caller before bringing up a tunnel to an LNS at 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-server = 1.1.1.1

admin> set tunnel tunneling-protocol = l2tp

admin> write
CONNECTION/l2test written
```

Following is a comparable RADIUS profile:

```
l2test Password = “localpw”
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Tunnel-Server-Endpoint = “1.1.1.1”,
   Tunnel-Type = L2TP,
   Tunnel-Medium-Type = IP
```

Controlling tunnel authentication

By setting the Tunnel-Client-Auth-ID and Tunnel-Server-Auth-ID parameters, you can enable more flexible and secure establishment of L2TP and Layer 2 Forwarding (L2F) tunnels. (For information about L2F, see “Layer 2 Forwarding (L2F)” on page 5-26. In previous software releases, because of constraints caused by L2TP and RADIUS protocol requirements, tunnel authentication required that every network access server (NAS) in the network used the same system name, even when the network spanned multiple administrative domains.

With the current software version, by specifying a system name on a per-connection or per-server basis, each NAS can send a unique system name for tunnel authentication purposes. If

RADIUS accounting is enabled, the TAOS unit reports the names used for tunnel authentication in the Stop record.

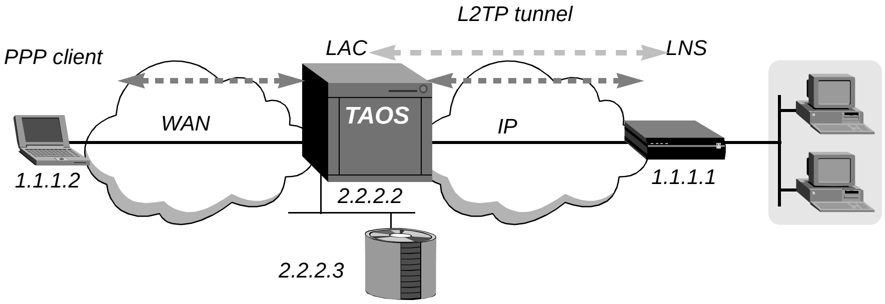
Note: Tunnel authentication occurs before a tunnel is established between two end points. It is negotiated between the TAOS unit and a tunnel server and is independent of user authentication. If tunnel authentication fails, all pending calls associated with the tunnel are dropped.

For L2TP tunnels, because the LAC can specify its name on a per-connection basis, you can configure profiles to create parallel tunnels to the same destination. For example, some sites use parallel tunnels to separate data streams that are directed to the same LNS but destined for different networks.

Examples of tunnel authentication

In the example shown in Figure 5-2, a PPP client dials into a TAOS unit to tunnel into its home network across the Internet.

Figure 5-2. Example of L2TP tunnel authentication



For the purposes of this example, the TAOS unit authenticates the initial PPP dial-in by its Dial Number Information Service (DNIS) number. (DNIS authentication is not required for tunnel authentication.) Because the TAOS unit operates only as LAC, the following example shows only the LAC configuration.

System configuration

For RADIUS to authenticate callers, you must configure the External-Auth profile. For example, the following commands configure the TAOS unit to use a RADIUS server for both authentication and accounting purposes:

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

admin> set auth-type = radius

admin> set acct-type = radius

admin> set rad-auth-client auth-server-1 = 2.2.2.3

admin> set rad-auth-client auth-port = 1645

admin> set rad-auth-client auth-key = key

admin> set rad-auth-client auth-timeout = 5

admin> set rad-acct-client acct-server-1 = 2.2.2.3

admin> set rad-acct-client acct-port = 1646
admin> set rad-acct-client acct-key = key
```

```
admin> set rad-acct-client acct-timeout = 5
```

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

The next set of commands configures the system to collect DNIS information:

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

```
admin> set clid-auth-mode = dnis-first
```

```
admin> set ppp-answer receive-auth-mode = any-ppp-auth
```

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

Connection-based tunnel authentication

The following commands configure a local Connection profile for the PPP client and specify a Client-Auth-ID name:

```
admin> new connection dnis-user
CONNECTION/dnis-user read
```

```
admin> set calledNumber = 001
```

```
admin> set tunnel-options profile-type = mobile-client
```

```
admin> set tunnel-options tunneling-protocol = l2tp-protocol
```

```
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
```

```
admin> set tunnel-options password = conn-pass
```

```
admin> set tunnel-options client-auth-id = conn-LAC
```

```
admin> write -f
CONNECTION/dnis-user written
```

Note that you need not assign an IP address because it is assigned by the LNS. Following is a comparable RADIUS profile:

```
001 User-Password = "Ascend-DNIS", Service-Type = Call-Check
   Tunnel-Type = L2TP,
   Tunnel-Server-Endpoint = 1.1.1.1,
   Tunnel-Password = conn-pass,
   Tunnel-Client-Auth-ID = conn-LAC
```

With the sample profiles, the LAC uses DNIS to authenticate the PPP client's dial-in call. It then initiates a tunnel to the LNS if a tunnel does not already exist to that end-point address. When the TAOS unit requests the tunnel, it passes the LNS the string `conn-LAC` as its local system name, and uses `conn-pass` as the password to authenticate the tunnel. The LNS uses the same strings to authenticate the LAC before establishing the tunnel.

Server-based tunnel authentication

The following commands configure a local Connection profile for the PPP client and do not specify a password or Client-Auth-ID name:

```
admin> new connection dnis-user
CONNECTION/dnis-user read
```

```
admin> set calledNumber = 001

admin> set tunnel-options profile-type = mobile-client

admin> set tunnel-options tunneling-protocol = l2tp-protocol

admin> set tunnel-options primary-tunnel-server = lns.example.com

admin> write -f
CONNECTION/dnis-user written
```

Following is a comparable RADIUS profile:

```
001 User-Password = "Ascend-DNIS", Service-Type = Call-Check
   Tunnel-Type = L2TP,
   Tunnel-Server-Endpoint = lns.example.com
```

With the sample profiles, the LAC uses DNIS to authenticate the PPP client's dial-in call. It then initiates a tunnel to the LNS if a tunnel does not already exist to that end-point address. If tunnel authentication is enabled and no tunnel password is specified in the Connection profile, the unit searches for a Tunnel-Server profile before requesting the tunnel. If it finds a Tunnel-Server profile for the LNS, the unit sends the Client-Auth-ID to the LNS and the end points use the tunnel password (the shared secret) to authenticate the tunnel. Following is a sample Tunnel-Server profile that specifies a password and local system name for use in tunnel authentication:

```
admin> new tunnel-server lns.example.com
TUNNEL-SERVER/lns.example.com read

admin> set shared-secret = ts-pass

admin> set client-auth-id = ts-LAC

admin> write
TUNNEL-SERVER/lns.example.com written
```

Following is a comparable RADIUS profile:

```
lns.example.com Password = "", Service-Type = Dialout
   Tunnel-Password = ts-pass
   Tunnel-Client-Auth-ID = ts-LAC
```

Note: If no Tunnel-Server profile exists, the LAC proceeds as described in "How the system name is selected (Hostname AVP)" on page 5-11.

Examples of creating parallel L2TP tunnels to the same end point

After the LAC has authenticated a PPP client's dial-in call, it looks for an existing tunnel that matches both the tunnel server end point and the Client-Auth-ID specified in the client's profile. If the LAC finds an established tunnel that matches these values, it uses the tunnel. If the LAC does not find a matching tunnel, it initiates a tunnel request. You can use this process to create parallel L2TP tunnels by specifying different Client-Auth-ID values in profiles.

How the system finds a matching tunnel

If the client's profile specifies a hostname as the tunnel-server end point, the system must match both the hostname and the server's actual IP address to allow the client to use an established tunnel.

If Client-Auth-ID is specified in the caller's profile, the system attempts to match the caller to an existing tunnel by using the following values:

- Tunnel server's IP address (and hostname, if specified)
- Client-Auth-ID
- Assignment-ID (if specified)

If Client-Auth-ID is *not* specified in the caller's profile, the system attempts to match the caller to an existing tunnel by using only the tunnel server's IP address (and hostname, if specified).

If the system finds a match on the basis of the values, it uses the tunnel. If the TAOS unit does not find a matching tunnel entry, it initiates a new tunnel request.

How the system name is selected (Hostname AVP)

If tunnel authentication is enabled and the TAOS unit is requesting a new tunnel, it looks for a system name to send to the LNS as follows:

1. If available, uses the Client-Auth-ID specified in the caller's Connection profile. If Client-Auth-ID is not specified in the Connection profile, the system goes on to the next alternative.
2. If available, the unit uses the Client-Auth-ID specified in the Tunnel-Server profile for the LNS. If Client-Auth-ID is not specified in a Tunnel-Server profile, the system goes on to the next alternative.
3. If available, the unit uses the L2TP-System-Name specified in the L2-Tunnel-Global profile. If L2TP-System-Name is not specified in that profile, the system goes on to the next alternative.
4. If available, the unit uses the Name specified in the unit's System profile. If Name is not specified in that profile, the system goes on to the next alternative.
5. The unit sends the string `noname`.

Examples of how Client-Auth-ID settings create parallel tunnels

In this example, the LNS system's DNS hostname is `a.example.com` (a fully qualified domain name), which resolves to two IP addresses, 1.1.1.1 and 1.1.1.2. The hostname `b.example.net` also resolves to the 1.1.1.1 address. Table 5-1 shows existing tunnels to the LNS, which were authenticated by using different Client-Auth-ID strings.

Table 5-1. Existing tunnels to the same LNS

Address	Tunnel-Server-Endpoint	Client-Auth-ID	Tunnel-Assign-ID	Tunnel-ID
1.1.1.1	`a.example.com`	a1	one	102
1.1.1.1	`a.example.com`	a1		111
1.1.1.1	`a.example.com`	a2		103

Table 5-2 shows how the system matches the values in the clients' profiles as it receives incoming calls, and the resulting action the system takes in terms of using an existing tunnel or creating a new one.

Table 5-2. Tunnels created for incoming callers based on profile settings

Values used to match tunnel:				**Resulting action**	**Tunnel-ID**
Address	**Tunnel-Server**	**Client-Auth-ID**	**Tunnel-Assignment-ID**		
1.1.1.1	a.example.com	a1	one	Reuse tunnel	102
1.1.1.1	a.example.com	a2		Reuse tunnel	103
1.1.1.1	a.example.com	a1		Reuse tunnel	111
1.1.1.1	b.example.net	b		Establish new tunnel	104
1.1.1.1	a.example.com	b		Establish new tunnel	105
1.1.1.1	a.example.com			Reuse tunnel	102 [a]
1.1.1.1	a.example.com		nn	Reuse Tunnel	102 [b]
1.1.1.1	b.example.net	a2		Establish new tunnel	106
1.1.1.2	a.example.com	a1		Establish new tunnel	107
1.1.1.1	a.example.com	a2	two	Establish new tunnel	108

[a] Tunnel-Server-Endpoint match.

[b] Tunnel-Server-Endpoint match.

Note: The caller that does not supply a Client-Auth-ID string matches the tunnel-server end point, so the existing tunnel to that end point (Tunnel-ID 102) is reused.

Examples of configuration errors causing multiple tunnels

Configuration errors can lead to unintentional parallel tunnels to the same tunnel end point. For this reason, you must either use the Client-Auth-ID setting for all user profiles to a particular LNS or decide *not* to use that setting for callers tunneling to that LNS.

For example, suppose your RADIUS users file contains the following two user profiles and tunnel server profile:

```
user1 Password = userpass
   Tunnel-Type = L2TP,
   Tunnel-Server-Endpoint = lns.example.com,
   Tunnel-Client-Auth-ID = A-LAC,
   ...
user2 Password = userpass
   Tunnel-Type = L2TP,
   Tunnel-Server-Endpoint = lns.example.com,
   ...
lns.example.com Password = "", Service-Type = Dialout
   Tunnel-Password = tunpass,
   Tunnel-Client-Auth-ID = AllMyLACs
```

If `user1` calls in first and establishes a tunnel, `user2` can reuse that tunnel, as shown in Table 5-3:

Table 5-3. Tunnels created when user1 dials in first (configuration error not detected)

Values used to match tunnels:			**Resulting action**	**Tunnel-ID**
Address	**Client-Auth-ID**	**Tunnel-Server**		
2.2.2.2	A-LAC	lns.example.com	Create new tunnel	88
2.2.2.2		lns.example.com	Reuse tunnel	88

However, if `user2` calls in first and establishes a tunnel, the system obtains a system name for authentication from the tunnel-server profile. When `user1` dials in, the caller is unable to reuse the tunnel, because the authentication names do not match. This situation is shown in Table 5-4.

Table 5-4. Tunnels created when user2 dials in first (configuration error shown)

Values used to match tunnels:			**Resulting action**	**Tunnel-ID**
Address	**Client-Auth-ID**	**Tunnel-Server**		
2.2.2.2	AllMyLACs	lns.example.com	Create new tunnel	40
2.2.2.2	A-LAC	lns.example.com	Create new tunnel	42

How tunnel assignment IDs affect tunnel matching

In addition to the criteria described in “How the system finds a matching tunnel” on page 5-10, this feature enables the system to perform an additional, final check for a tunnel assignment ID when selecting an existing tunnel or deciding to create a new one. After comparing the tunnel transport address and, if specified in the client’s profile, the tunnel server’s hostname (Server-Endpoint) against existing tunnels, the system begins comparing the following optional parameters, in the order shown:

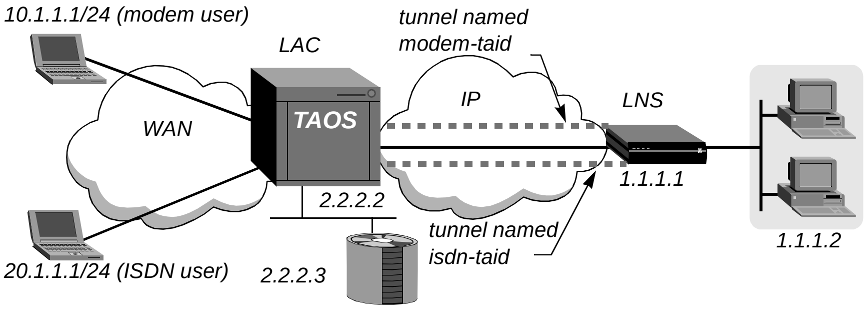
- Client-Auth-ID specified in the client’s profile and the Client-Auth-ID used for existing tunnels
- Assignment-ID specified in the client’s profile and the tunnel assignment ID of existing tunnels

The client profile matches existing tunnels only if both the Client-Auth-ID and the tunnel assignment ID match. A null value in any one of these fields in an existing tunnel matches only a null value in the corresponding parameter in the client profile. If the TAOS unit does not find a matching tunnel entry, it initiates a new tunnel request.

Example of configuring a tunnel assignment ID

In this example, the TAOS unit is configured to perform tunnel authentication for L2TP tunnels. The two PPP clients shown in Figure 5-3 are configured to use different tunnels to the LNS on the basis of their tunnel assignment IDs. (The same clients could be configured to use the same multiplexed tunnel if their tunnel assignment IDs were set to the same string.)

Figure 5-3. L2TP tunnel setup that uses tunnel assignment IDs



The following set of commands creates local Connection profiles for the two mobile clients:

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

admin> set ppp-options recv-password = test

admin> set tunnel-options profile-type = mobile-client

admin> set tunnel-options tunneling-protocol = l2tp-protocol

admin> set tunnel-options primary-tunnel-server = 1.1.1.1

admin> set tunnel-options password = shared

admin> set tunnel-options client-auth-id = taos-unit

admin> set tunnel-options assignment-id = modem-taid

admin> write
CONNECTION/modemuser written

admin> new connection isdnuser
CONNECTION/isdnuser read

admin> set ppp-options recv-password = test

admin> set tunnel-options profile-type = mobile-client

admin> set tunnel-options tunneling-protocol = l2tp-protocol

admin> set tunnel-options primary-tunnel-server = 1.1.1.1

admin> set tunnel-options password = shared

admin> set tunnel-options client-auth-id = taos-unit

admin> set tunnel-options assignment-id = isdn-taid

admin> write
CONNECTION/isdnuser written
```

Following are comparable RADIUS profiles:

```
modemuser Password = "test"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Test-Idle-Limit = 0,
    Tunnel-Type = L2TP :1,
    Tunnel-Server-Endpoint = 1.1.1.1 :1,
    Tunnel-Client-Auth-ID = taos-unit: 1,
    Tunnel-Password = shared,
    Tunnel-Assignment-ID = modem-taid:1
```

```
isdnuser  Password = "test"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Test-Idle-Limit = 0,
    Tunnel-Type = L2TP :1,
    Tunnel-Server-Endpoint = 1.1.1.1 :1,
    Tunnel-Client-Auth-ID = taos-unit: 1,
    Tunnel-Password = shared,
    Tunnel-Assignment-ID = isdn-taid:1
```

RADIUS accounting support

RADIUS accounting Stop records display the Tunnel-Assignment-ID used for the user-session. For example:

```
Tue May 2 15:58:08 2000
        User-Name = "modemuser"
        NAS-Identifier = 2.2.2.2
        NAS-Port = 11313
        NAS-Port-Type = Async
        Acct-Status-Type = Stop
        Acct-Delay-Time = 0
        Acct-Session-Id = "317658341"
        Acct-Authentic = Local
        Acct-Session-Time = 112
        Acct-Input-Octets = 2155
        Acct-Output-Octets = 513
        Acct-Input-Packets = 23
        Acct-Output-Packets = 14
        Ascend-Disconnect-Cause = 185
        Ascend-Connect-Progress = 60
        Ascend-Xmit-Rate = 28800
        Ascend-Data-Rate = 33600
        Ascend-PreSession-Time = 19
        Ascend-Pre-Input-Octets = 0
        Ascend-Pre-Output-Octets = 0
        Ascend-Pre-Input-Packets = 0
        Ascend-Pre-Output-Packets = 0
        Ascend-Modem-PortNo = 1
        Ascend-Modem-SlotNo = 7
        Ascend-Modem-ShelfNo = 1
        Caller-Id = "1119855510"
        Client-Port-DNIS = "3826"
        Tunnel-Type = L2TP
        Tunnel-Server-Endpoint = "1.1.1.1"
        Tunnel-Client-Auth-ID = "taos-unit"
        Tunnel-Server-Auth-ID = "max6k-lns"
        Tunnel-Assignment-ID = "modem-taid"
```

Configuring a secondary tunnel server for L2TP and L2F tunnels

You can configure local Connection profiles with a secondary tunnel end point for L2TP or L2F tunnel sessions. For details about RADIUS support for multiple end points, see “Summary of tunnel attribute sets” on page 5-35.

Following are the relevant parameters, shown with sample settings:

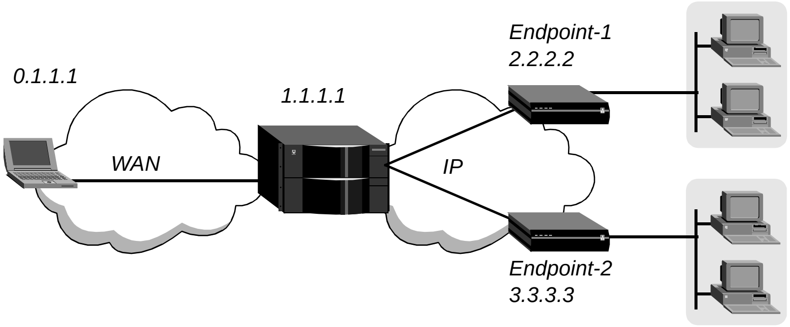
```
[in IP-GLOBAL]
system-ip-addr = 1.1.1.1

[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
```

The TAOS unit opens a tunnel session with this server only if the primary server is unavailable. Once it has established a tunnel to the secondary tunnel server, the unit maintains that tunnel until the connection terminates, even if the primary server becomes available.

Example of configuring an L2TP tunnel to two server end points

Figure 5-4 shows a TAOS unit that can connect to one of two possible LNS end points to create an L2TP tunnel for the dial-in client. In this example, the LNS end points are on remote networks, so the system requires a Connection or RADIUS profile to establish a connection to one of the end-point systems.

Figure 5-4. Primary and secondary L2TP tunnel end points



The following commands configure the TAOS unit’s system IP address:

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

admin> set system-ip-addr = 1.1.1.1

admin> write
IP-GLOBAL written
```

The following commands configure Connection profiles to the two LNS systems:

```
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 recv-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 recv-password = lac-pw

admin> set ip-options remote = 3.3.3.3

admin> write
CONNECTION/endpoint-2 written
```

The following commands create a Connection profile for the dial-in client:

```
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
```

Configuring IP security (IPSec) authentication

TAOS units support the IPSec Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols for secure transmission of IP data packets. Each protocol supports two modes of use: transport mode and tunnel mode. For complete information about the IPSec protocols, see RFC 2401, *Security Architecture for the Internet Protocol* (November 1998), RFC 2402, *IP Authentication Header* (November 1998), and RFC 2406, *IP Encapsulating Security Payload (ESP)* (November 1998).

IPSec security protocols

IPSec AH uses a shared secret (a *key*) to run portions of a data packet through digest algorithms to create a digital fingerprint. The receiving system performs the same process and compares the fingerprints. If the fingerprints match, the receiving system is assured that the packet was sent by the right source and was not altered in transit.

IPSec ESP performs full encryption of the data portion of every packet. The receiving system decrypts the packets before routing them. The encryption/decryption provides the added assurance that packet contents have not been viewed while the packet was in transit.

IPSec encapsulation modes

The TAOS unit supports IPSec transport mode and tunnel mode.

Transport mode operates between two hosts. Transport mode provides security services for higher-layer protocols, which can include selected portions of the IP header and other selected options.

Tunnel mode is required for connections between a host that does not perform IPSec processing and a security gateway. In tunnel mode, IP packets are encapsulated in an outer IP header that specifies the IPSec processing destination (IP-in-IP encapsulation).

Applying IPSec to a tunnel server or TCP connection

IPSec profiles specify an IPSec end point as well as the IPSec encapsulation method to use on the data stream transmitted to and from that end point. Both end points must have matching configurations. (The settings in the *send* configuration of one system must match those in the *receive* configuration of the other system, and vice versa.)

In an IPSec profile, the following parameters (shown with default values) enable the profile and specify the encapsulation mode and far-end IPSec end-point address:

```
[in IPSEC/""]
name* = ""
active = no
encap-mode = transport
tunnel-address = 0.0.0.0
```

Parameter	**Specifies**
Name	Name of the IPSec profile (up to 23 characters).
Active	Enable/disable the profile for use.
Encap-Mode	Encapsulation mode in which IPSec operates. For background information, see "IPSec encapsulation modes" on page 5-18. The default value is `transport` (transport mode). If the parameter is set to `tunnel`, IP-in-IP encapsulation is used to tunnel the data stream. Tunnel mode is required if the IPSec end-point addresses differ from the TCP end-point addresses for TCP-Clear sessions. If the parameter is set to `optimized`, the system uses transport mode if possible (transport mode is more efficient) and uses tunnel mode only when it is required for a particular connection.
Tunnel-Address	IP address of the far-end IPSec end point. For an L2TP connection, this is the IP address of the L2TP network server (LNS) at the far end of the tunnel. For a TCP-Clear connection, it is the address of a security gateway or dial-in host.

For example, the following commands specify that IPSec processing operates in transport mode on the data stream transmitted to and from 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
```

Note: The commands in the preceding example do not create a usable IPSec profile. IPSec AH or IPSec ESP (or both) must be configured for the IPSec profile to have an effect. For details, see “Configuring an IPSec profile for IPSec AH” on page 5-20 and “Configuring an IPSec profile for IPSec ESP” on page 5-22

Following is a comparable RADIUS profile:

```
lns.example.com Password, Service-Type = Dial-Out
   Tunnel-Password = tunpass,
   Tunnel-Client-Auth-ID = AllMyLACs,
   Asecend-IPSec-Profile = “securegw”
```

Applying an IPSec profile to an LNS

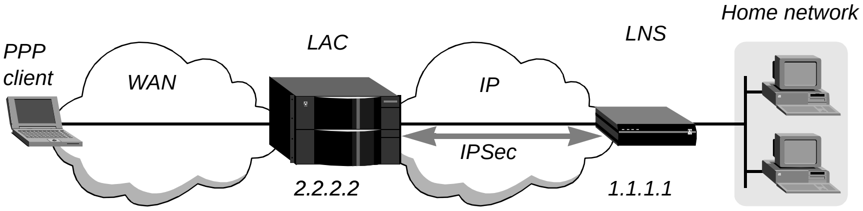
The following parameters (shown with default values) associate an IPSec profile with a particular LNS:

```
[in TUNNEL-SERVER/""]
server-endpoint = ""
ipsec-profile = ""
```

Parameter	Specifies
Server-Endpoint	Name or IP address of the tunnel end point. This parameter must specify the same host as the Tunnel-Address parameter in the IPSec profile to be applied.
IPSec-Profile	Name of the IPSec profile (up to 23 characters) that defines the transforms and end points for IPSec operations on traffic crossing L2TP tunnels to the specified end point. If the Tunnel-Server profile does not specify an IPSec profile name, a normal, nonsecure UDP socket is assigned to the L2TP session. If an IPSec profile name is specified, a new UDP socket is opened and assigned the specified profile settings.

Figure 5-5 shows a TAOS unit operating as an L2TP access concentrator (LAC) with a MAX unit operating as the LNS.

Figure 5-5. Secure IPsec L2TP tunneling configuration



The following commands apply an IPSec profile named `securegw` to the specified LNS:

```
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
```

Following is a comparable RADIUS profile:

```
1.1.1.1 Password””, Service-Type = Dial-Out
    Ascend-IPSec-Profile = “securegw”
```

Configuring an IPSec profile for IPSec AH

For IPSec AH to operate, both ends of the L2TP tunnel must specify a security parameter index (SPI) number, the type of transform to use, and a shared secret (a key). These settings must match in the LAC and LNS configurations. In addition, you can choose to enable *replay protection*, which is used to counter denial-of-service attacks.

Overview of the IPSec AH settings

Administrators at both ends of the tunnel must specify matching IPSec AH configurations. Following are the relevant TAOS unit parameters (shown with their default settings):

```
[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
```

Parameter	**Specifies**
Active	Enable/disable IPSec AH processing for packets sent or received through the tunnel.
SPI	Security parameters index—a 32-bit numeric value from 1 to 2147483647. The SPI in the Send-AH subprofile must match the LNS SPI in its receiving AH configuration, and vice versa. If the LNS is a TAOS unit (such as a MAX unit), the administrator of that unit can use the SecureConnect Manager™ (SCM) application to create and download IPSec configurations in Firewall profiles. The SPI values in SCM are in hexadecimal, while the TAOS unit SPI values are in decimal. You can enter the SPI value here in hexadecimal by preceding the value with `0x`. However, the number is still displayed in decimal in the TAOS unit’s interface.

Parameter	Specifies
AH-Type	Type of authentication transform to use. Following are valid values: • None (the default)—No authentication • MD5—MD5 mode, described in RFC 1828 • SHA1—SHA1 mode, described in RFC 1852 on the secure hash algorithm (SHA) • MD5-HMAC—Version-2 MD5, currently in draft • SHA1-HMAC—Version-2 SHA1, currently in draft
Key	Authentication key for hashing—a 64-byte text string that exactly matches the key specified in the LNS IPSec AH configuration.
Replay-Protection	Enable/disable sequence number processing. The receiving system uses a sequence number to detect arrival of duplicate packets within a constrained window. If this parameter is enabled in the Send-AH subprofile, the TAOS unit generates a sequence number for packets it sends through the tunnel. In the current software version, the TAOS unit does not verify the sequence of packets it receives from the LNS, even if Replay-Protection is enabled in the Recv-AH subprofile.

Example of an IPSec AH configuration

In the following example, an administrator creates an IPSec profile applying IPSec AH to all data sent and received through an L2TP tunnel to an LNS at the IP address 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
```

In the next commands, the TAOS unit's send configuration must match corresponding parameters in the LNS system's IPSec receive configuration, and vice versa:

```
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
```

The next commands apply the IPSec profile to the 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
```

Configuring an IPSec profile for IPSec ESP

The IPSec ESP protocol provides data encryption as well as replay protection and authentication. If you are configuring ESP in addition to IPSec AH, you can specify encryption alone and rely on AH to provide authentication and replay protection service. If you are specifying IPSec ESP without a corresponding AH configuration, you must include integrity and authentication settings to prevent attacks that could otherwise compromise the security provided by encryption alone.

Overview of IPSec ESP settings

Administrators at both IPSec end points must specify matching IPSec ESP configurations. Following are the relevant parameters, shown with their default settings:

```
[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
```

Parameter	Specifies
Active	Enable/disable IPSec ESP processing for packets sent or received through the tunnel.

Parameter	**Specifies**
SPI	Security parameters index: a 32-bit numeric value from 1 to 2147483647. The SPI in the Send-ESP subprofile must match the LNS SPI in its receiving ESP configuration, and vice versa. If the LNS is a TAOS unit (such as a MAX unit), the administrator of that unit can use the SecureConnect Manager (SCM) to create and download IPSec configurations in Firewall profiles. The SPI values in SCM are in hexadecimal, while the TAOS unit SPI values are in decimal. You can enter the SPI value here in hexadecimal by preceding the value with `0x`. However, the number is still displayed in decimal in the TAOS unit's interface.
Version	ESP version (version 1 or version 2).
ESP-Type	Type of ESP transform to use to encrypt the data portion of IP packets. Following are valid values: • None (the default)—No encryption • DES-CBC—DES-CBC mode, described in RFC 1829, on the US Data Encryption Standard cipher block chaining algorithm • 3DES-CBC—3DES-CBC mode, described in RFC 1851 on the Triple DES-CDC algorithm • 40DES-CBC—DES-CBC mode restricted to 40 bits
IV-Len	Number of bits in the Initialization Vector. For ESP-v1, you can specify 32 (a 32-bit vector) or 64 (a 64-bit vector). For ESP-v2, IV-Len is set to 64 automatically.
Key	Authentication key for ESP: A 16-byte text string that exactly matches the key specified in the LNS IPSec ESP configuration.
Key2	Second 16-byte authentication key, to be used for the second pass of 3DES-CBC mode encryption.
Key3	Third 16-byte authentication key, to be used for the third pass of 3DES-CBC mode encryption.
Auth-Type	Type of authentication transform to use when ESP-v2 is in use. Following are valid values: • None (the default)—No authentication • MD5—MD5 mode, described in RFC 1828 • SHA1—SHA1 mode, described in RFC 1852 • MD5-HMAC—Version-2 MD5, currently in draft • SHA1-HMAC—Version-2 SHA1, currently in draft
Auth-Key	Authentication key to use when ESP-v2 is in use: A 64-byte text string exactly matches the key specified in the LNS IPSec ESP-v2 configuration. This setting does not apply if Version is set to 1.

Parameter	Specifies
SPI	Security parameters index: a 32-bit numeric value from 1 to 2147483647. The SPI in the Send-ESP subprofile must match the LNS SPI in its receiving ESP configuration, and vice versa. If the LNS is a TAOS unit (such as a MAX unit), the administrator of that unit can use the SecureConnect Manager (SCM) to create and download IPSec configurations in Firewall profiles. The SPI values in SCM are in hexadecimal, while the TAOS unit SPI values are in decimal. You can enter the SPI value here in hexadecimal by preceding the value with `0x`. However, the number is still displayed in decimal in the TAOS unit's interface.
Version	ESP version (version 1 or version 2).
ESP-Type	Type of ESP transform to use to encrypt the data portion of IP packets. Following are valid values: • None (the default)—No encryption • DES-CBC—DES-CBC mode, described in RFC 1829, on the US Data Encryption Standard cipher block chaining algorithm • 3DES-CBC—3DES-CBC mode, described in RFC 1851 on the Triple DES-CDC algorithm • 40DES-CBC—DES-CBC mode restricted to 40 bits
IV-Len	Number of bits in the Initialization Vector. For ESP-v1, you can specify 32 (a 32-bit vector) or 64 (a 64-bit vector). For ESP-v2, IV-Len is set to 64 automatically.
Key	Authentication key for ESP: A 16-byte text string that exactly matches the key specified in the LNS IPSec ESP configuration.
Key2	Second 16-byte authentication key, to be used for the second pass of 3DES-CBC mode encryption.
Key3	Third 16-byte authentication key, to be used for the third pass of 3DES-CBC mode encryption.
Auth-Type	Type of authentication transform to use when ESP-v2 is in use. Following are valid values: • None (the default)—No authentication • MD5—MD5 mode, described in RFC 1828 • SHA1—SHA1 mode, described in RFC 1852 • MD5-HMAC—Version-2 MD5, currently in draft • SHA1-HMAC—Version-2 SHA1, currently in draft
Auth-Key	Authentication key to use when ESP-v2 is in use: A 64-byte text string exactly matches the key specified in the LNS IPSec ESP-v2 configuration. This setting does not apply if Version is set to 1.

Parameter	Specifies
Replay-Protection	Enable/disable sequence number processing. The receiving system uses a sequence number to detect the arrival of duplicate packets within a constrained window. If this parameter is enabled in the Send-AH subprofile, the TAOS unit generates a sequence number for packets it sends through the tunnel. In the current software version, the TAOS unit does not verify the sequence of packets it receives from the LNS, even if Replay-Protection is enabled in the Recv-AH subprofile.

Example of an IPSec ESP configuration for L2TP

In the following example, an administrator creates an IPSec profile applying IPSec ESP and partial sequence integrity (replay protection) to packets tunneled to and from an LNS at the IP address 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
```

In the next commands, the TAOS unit’s send configuration must match corresponding parameters in the LNS system’s IPSec receive configuration, and vice versa:

```
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
```

The next commands apply the IPSec profile to the 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
```

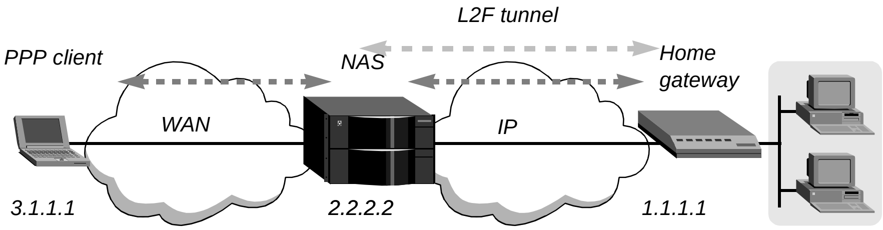
Layer 2 Forwarding (L2F)

Note: This implementation of Layer 2 Forwarding (L2F) was designed to interoperate with IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

In the current software version, a TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running IOS 11.3.

Figure 5-6 shows the elements of an L2F tunnel. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within PPP. The TAOS unit answers the call and passes it to the home gateway (a Cisco router running IOS 11.3). Communication between the NAS and the home gateway requires IP connectivity.

Figure 5-6. L2F tunneling



The connection to the home gateway is an IP link, which consists of a control link and one or more data links. Both the control and data links use UDP port 1701 and are encapsulated in UDP.

The control link carries information used to query whether the home gateway can accept the current call and to establish a tunnel. L2F implements a periodic Hello mechanism by which the NAS and home gateway verify that the other is still operational. If the Hello message does not arrive within a specified period, the tunnels are brought down.

Each tunneled client connection has one data link, which carries PPP frames.

Authenticating L2F tunnels

The TAOS unit supports both shared-secret and distinct-secret L2F tunnel authentication. The default method is to use a shared secret between the tunnel end points. (Authenticating L2F tunnels with a shared secret is similar to authenticating L2TP tunnels with a shared secret. For details, see “Layer 2 Tunneling Protocol (L2TP)” on page 5-1.

Distinct secrets enable you to specify different passwords to authenticate the NAS to the home gateway and the home gateway to the NAS.

You can also configure the TAOS unit to authenticate tunnels by first attempting to use a shared secret, and if that fails, to then use distinct secrets.

The following sequence of events describes how the TAOS unit uses distinct tunnel secrets to authenticate L2F tunnels:

1 A client connects and is partly authenticated. The TAOS unit looks up the associated Connection profile (or RADIUS profile) by client name and partially authenticates the client on the basis of the username and password settings.

2 If an L2F tunnel is specified by either the Tunnel-Type attribute in a RADIUS profile or the Tunnel-Protocol parameter in a local Connection profile, the TAOS unit either adds this client connection to an existing tunnel or creates a new tunnel to the specified server end point.

3 If a password is present by either the Tunnel-Password attribute in RADIUS or the Password parameter in a local Connection profile, the TAOS unit uses this password to authenticate the NAS to the home gateway.

4 The TAOS unit authenticates the home gateway by matching the name provided by the home gateway to the value specified by the Tunnel-Server-Endpoint attribute in RADIUS or the Server-Endpoint parameter in a local Connection profile.

5 The TAOS unit establishes the tunnel between itself and the home gateway.

If you are using RADIUS to authenticate L2F tunnels with distinct passwords, make sure of the following:

- The client’s RADIUS user profile must contain a Tunnel-Password attribute with the password that the TAOS unit uses to authenticate the tunnel to the home gateway.
- The home gateway must have a RADIUS user profile. Because this is not a user profile for interactive access, Lucent Technologies recommends that the Service-Type attribute be set to Outbound.

The following examples show a client’s RADIUS profile and a home gateway’s RADIUS profile that use distinct secrets for tunnel authentication:

```
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 = ""
```

Alternatively, the home gateway password can be configured locally in a Tunnel-Server profile.

Configuring basic L2F operations

To enable the TAOS unit to operate as an L2F end point, you must set it to run in NAS mode and configure it to recognize the L2F home gateway (a Cisco router running IOS 11.3).

If the home gateway is on a remote IP network, the TAOS unit also requires an IP-routed Connection profile or RADIUS profile that defines a connection to the home gateway. For details about configuring IP WAN interfaces, see Chapter 1, “WAN Connections.”.

Overview of global L2F parameters

For additional information about parameters that are used in L2TP configuration, see "Overview of RADIUS attribute-value pairs" on page 5-4. Following are the global L2F parameters (shown with default values) for configuring L2F operations:

```
[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 = ""
```

Parameter	Specifies
UDP-Queue-Length	Maximum number of UDP packets that can reside in the input queue for the L2F NAS. The default queue length for UDP requests is 256. Valid values for the queue length are 0–512.
L2F-Mode	Enable/disable L2F operations. Specify NAS to enable L2F operations in the TAOS unit. The default is Disabled.
L2F-System-Name	System name of the NAS unit. Used to identify the NAS to the L2F home gateway during tunnel creation.
L2F-Retry-Count	Number of times the TAOS unit will resend L2F control packets. Values can be from 1 to 16. The default is 4.
L2F-Retry-Interval	Retry interval in seconds. Values can be from 0 to 32 seconds. The default value of 0 specifies that an adaptive retry interval (based on the retry number plus 1) is to be used.
L2F-Tunnel-Secret	Authentication method used by the TAOS unit to authenticate the L2F tunnels. When the parameter is set to `shared-tunnel-secret` (the default), tunnel authentication relies on a secret shared by the NAS and the home gateway. With the `distinct-tunnel-secrets` setting, tunnel authentication uses distinct secrets for authenticating the NAS to the home gateway, and the home gateway to the NAS. With the `either-shared-or-distinct-tunnel-secret` setting, the TAOS unit first tries to authenticate with the shared secret. If that fails, the unit then uses distinct secrets to try to authenticate the tunnel. For more information, see "Authenticating L2F tunnels" on page 5-26.

Example of a basic L2F configuration

The following commands configure basic L2F operations with a home gateway named 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
```

Configuring L2F client profiles

When a PPP client dials into the TAOS unit to initiate a tunnel to the L2F home gateway, the TAOS unit must first authenticate the client by PPP authentication. Even though the TAOS unit has provided password authentication for a call, the home gateway can (and probably should, for security reasons) authenticate again. The NAS and home gateway can use different PPP authentication protocols without restriction.

Sample L2F settings in a Connection profile

Following are the L2F tunnel parameters (shown with sample values) in a Connection profile:

```
[in CONNECTION/tunnelcx:tunnel-options]
profile-type = mobile-client
tunneling-protocol = l2f-protocol
primary-tunnel-server = l2f-1
password = "nas-pw"
```

Examples of opening a tunnel after password authentication

In this example, the TAOS unit negotiates the PPP call, including password authentication, and then opens the L2F tunnel. For details about PPP authentication, see Chapter 1, “WAN Connections.”.

The following commands create a Connection profile that includes a PPP password. The TAOS unit authenticates the caller before bringing up a tunnel to a home gateway at 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-server = 1.1.1.1

admin> set tunnel-options tunneling-protocol = l2f-protocol

admin> write
CONNECTION/l2test written
```

Following is a comparable RADIUS profile:

```
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"
```

Point-to-Point Tunneling Protocol (PPTP)

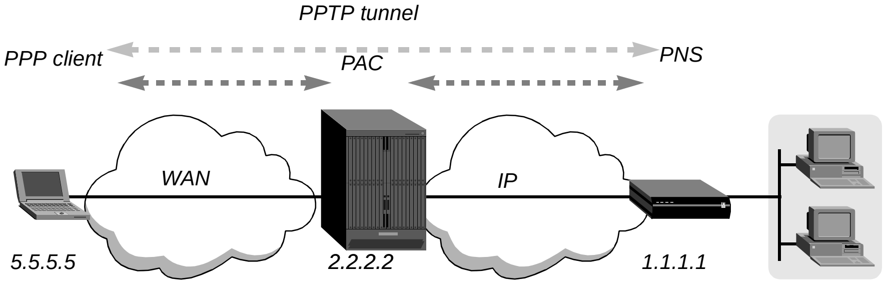
Point-to-Point Tunneling Protocol (PPTP) provides tunneling at OSI Layer 2 (at the HDLC layer of a PPP connection). It enables a PPP client to connect to a remote Windows NT server through the TAOS unit as if the connection were directly terminated at the server.

A TAOS unit operates as a PPTP access concentrator (PAC) only, which means that the unit receives incoming PPP calls and initiates a connection to the Windows NT server configured as a PPTP network server (PNS).

Components of a PPTP tunnel

Figure 5-7 shows the elements of a PPTP tunnel. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within a PPP connection. The TAOS unit answers the call and passes it to the PNS. PAC-to-PNS communication requires an IP connection.

Figure 5-7. PPTP tunneling



The mobile client can be any PPP client. For example, it could be a Pipeline dialing a digital call, or a PC running Windows NT dialing a modem call.

The link between the PAC and the PNS can be a switched or nailed connection, or it can be an Ethernet link. The PPP client’s connection to the PNS is an IP link, which consists of a control link and zero or more data links. The control link runs over TCP, and the data links run over GRE-v2.

The control link carries information that is used both to query whether the PNS will accept the current call and to establish a tunnel. PPTP implements a Hello mechanism by which the PAC and PNS each verify that the other is still alive. They do this by sending each other a control message every minute or so. If the Hello message does not arrive for several minutes, the tunnel and all the tunneled connections are brought down.

Data links carry the client data, which consists of PPP frames. There is one data link per tunneled client connection.

Configuring PPTP operations

Following are the global PPTP parameters (shown with default values):

```
[in L2-TUNNEL-GLOBAL]
pptp-enabled = no
server-profile-required = no
```

Parameter	Specifies
PPTP-Enabled	Enable/disable PPTP operations.
Server-Profile-Required	Enable/disable a requirement for a configured Tunnel-Server profile for a connection to the PNS. With a setting of Yes, PPTP must find a Tunnel-Server profile that matches the PNS specification in a Connection profile before it can create a tunnel to the server. With a setting of No (the default), PPTP first looks for a matching Tunnel-Server profile, and if it finds one, uses the settings in that profile to create (or refuse) the tunnel. However, if it does not find a matching Tunnel-Server profile, it attempts to create a tunnel anyway.

For additional information about tunneling parameters that are used to configure PPTP tunnels, see “Overview of RADIUS attribute-value pairs” on page 5-4. The following commands configure the TAOS unit to connect to a PNS named 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
```

Configuring PPTP mobile-client profiles

If a PPP client’s profile is configured to initiate a PPTP tunnel, the TAOS unit attempts to open a tunnel upon initial authentication of the connection. It can open a tunnel after preauthenticating the call (using CLID or DNIS authentication) or after authenticating the caller’s name and password.

If the PAC opens a tunnel after preauthenticating the call, the PNS performs all PPP negotiations and terminates the PPP connection. Even if the PAC has password authenticated a call, the PNS can (and probably should, for security reasons) authenticate again. The PAC and PNS can use different PPP authentication protocols without restriction.

Note: Because of tunneling protocol requirements, the PNS can only use a PPP authentication protocol to authenticate a tunneled call. The PNS cannot use other authentication methods (such as CLID, DNIS, or terminal-server authentication) for tunneled calls.

For the system to use CLID or DNIS to preauthenticate a call, the telco switch must send the information as part of the call, and the TAOS unit must be configured to extract and use the information.

For details about preauthentication and password authentication, see Appendix A, "Authentication Methods."

PPTP settings in Connection profiles

Following are the PPTP tunnel parameters (shown with sample values) in a Connection profile:

```
[in CONNECTION/tunnelcx:tunnel-options]
profile-type = mobile-client
tunneling-protocol = pptp-protocol
primary-tunnel-server = pptp-1
```

PPTP settings in RADIUS profiles

RADIUS uses the Tunnel-Type (64), Tunnel-Medium-Type (65), and Tunnel-Server-Endpoint (66) attribute-value pairs to specify PPTP tunnels. For additional information about these attributes, see "Overview of attribute sets and tags" on page 5-35.

Examples of opening a tunnel after preauthenticating the call

To enable the TAOS unit to preauthenticate a call, it must be configured to extract and use CLID or DNIS information. For details, see Appendix A, "Authentication Methods."

Examples using CLID authentication

The following commands configure a profile that opens a PPTP tunnel to a PNS (1.1.1.1) after verifying the caller-ID:

```
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-server = 1.1.1.1

admin> set tunnel tunneling-protocol = pptp

admin> write
CONNECTION/pptp-test written
```

Following is a comparable RADIUS profile:

```
5551000 Password = "Ascend-CLID", Service-Type = Outbound-User
   Tunnel-Type = PPTP,
   Tunnel-Medium-Type = IP,
   Tunnel-Server-Endpoint = "1.1.1.1"
```

Examples using DNIS

The following commands configure a profile that opens a tunnel to a PNS named PPTP-1 if the dialed number is 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-server = pptp-1.example.com

admin> write
CONNECTION/tunnelcx
```

Following is a comparable RADIUS profile:

```
8001234567 Password = “Ascend-DNIS”, Service-Type = Outbound-User
   Tunnel-Server-Endpoint = “pptp-1.example.com”,
   Tunnel-Type = PPTP,
   Tunnel-Medium-Type = IP
```

Examples of opening a tunnel after password authentication

In these examples, the TAOS unit negotiates the PPP call, including password authentication, and then opens the PPTP tunnel. For details about PPP authentication, see “Authenticating framed protocol sessions” on page A-6.

The following commands create a Connection profile that includes a PPP password. The TAOS unit authenticates the caller before bringing up a PPTP tunnel to a PNS at 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-server = 1.1.1.1

admin> set tunnel tunneling-protocol = pptp

admin> write
CONNECTION/pptp-test written
```

Following is a comparable RADIUS profile:

```
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
```

IP-in-IP encapsulation

IP-in-IP is a way to alter an IP packet's normal routing by encapsulating it within another IP header. The encapsulating header specifies the address of a router that would not ordinarily be selected as a next-hop router on the basis of the packet's real destination address. The intermediate node decapsulates the packet, which is then routed to the destination as usual. For details on how this is done, see RFC 2003, *IP Encapsulation Within IP*.

This method of rerouting packets by using encapsulation is referred to as *tunneling* the packet, and the *end points* of the tunnel are the system that encapsulates the packets (the Foreign Agent) and the system that decapsulates the packets (the Tunnel Server).

If the Foreign Agent receives an incoming packet that is larger than the IP-in-IP maximum transmission unit (MTU) size, the packet is fragmented before encapsulation. Each fragment is then encapsulated in its own IP header. The IP-in-IP MTU size is currently fixed at 1480 bytes (1500 - 20).

In the current software version, a TAOS unit encapsulates an incoming IP packet in another IP packet, forming an IP-in-IP packet. The unit does not decapsulate an IP-in-IP packet. In other words, a TAOS unit operates only as a Foreign Agent and not as a Tunnel Server. The source address in the outer IP header of the IP-in-IP packet is set to the Foreign Agent IP address and the destination IP address is set to the IP address of the Tunnel Server. The encapsulated packet is then routed to the Tunnel Server in the usual way.

Settings in a Connection profile

Following are the Connection profile parameters (shown with sample settings) that are relevant to IP-in-IP encapsulation:

```
[in CONNECTION/p50:tunnel-options]
profile-type = mobile-client
tunneling-protocol = ipinip-protocol
primary-tunnel-server = "10.2.3.4"
```

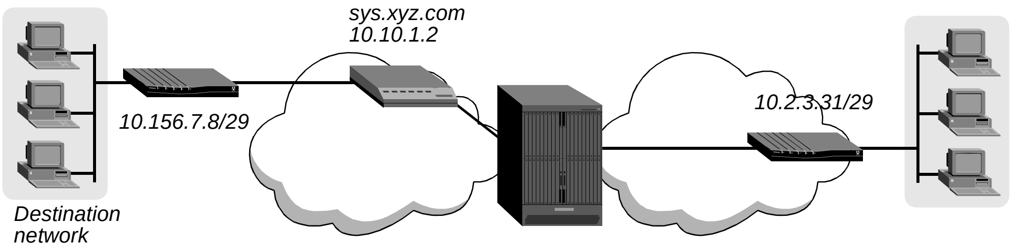
Settings in a RADIUS profile

The RADIUS attributes Tunnel-Type (64) and Tunnel-Server-Endpoint (67) can be used to indicate IP-in-IP encapsulation. For additional information about tunnel attributes, see “Overview of attribute sets and tags” on page 5-35.

Examples of an IP-in-IP connection

The Pipeline unit shown at the right of Figure 5-8 dials in to the TAOS unit to log in to the destination network. After the connection has been established, the TAOS unit encapsulates the IP packets in this data stream and forwards them to the CPE router at 10.10.1.2. That router decapsulates the packets and forwards them to their real destination.

Figure 5-8. IP-in-IP tunneling



Following are the commands entered to configure a local profile, and the system's responses:

```
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
```

Following is a comparable RADIUS profile:

```
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"
```

Summary of tunnel attribute sets

The *RADIUS Attributes for Tunnel Protocol Support Internet-Draft* defines a set of RADIUS attributes designed to support transparent tunneling to dial-in networks, where a tunnel is created automatically without any explicit action by the user. To support this type of tunneling, the user's profile includes a primary attribute set, which specifies all of the values required to set up the tunnel, and additional attribute sets that can be used to establish a tunnel if the primary server is unavailable.

Note: Use of tunneling attribute tags and preferences requires the NavisRadius™ product or another RADIUS server that supports them.

Overview of attribute sets and tags

A *tag* is a number from 1 to 31 that you can add to one or more of the RADIUS attributes listed in "Tunnel attributes used with tags" on page 5-37. Attributes that share the same tag number form an attribute set. Attribute sets in the same user profile are processed in numeric order (the set with tag 1 is processed before the set with tag 2, and so forth), unless the sets are reordered by means of the Tunnel-Preference attribute.

A tag value of 0 (zero) is considered untagged. Untagged attribute sets are processed before tagged attribute sets, unless a Tunnel-Preference setting specifies otherwise.

A tag is separated from an attribute-value pair by a colon. Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3:

```
joebloggs User-Password = "murphy"
    Tunnel-Type = L2TP : 1,
    Tunnel-Server-Endpoint = "1.1.1.1" : 1,
    Tunnel-Password = "loloaqic" : 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
```

This profile specifies that the NAS (the TAOS unit) must attempt first to establish an L2TP tunnel to the LNS at 1.1.1.1. If that attempt fails, the system attempts to bring up an L2F tunnel to a server at 2.2.2.2. If that attempt also fails, the system tries an L2TP tunnel to 3.3.3.3.

In the current software version, a user profile can specify up to 32 tunnel attribute sets. However, because the system waits a certain interval before each attempt to initiate a tunnel and retries a certain number of times, the client’s PPP connection typically times out before 32 tunnel attempts are made.

Supported tunnel protocols

RADIUS attribute tags can be used for all supported tunnel protocols. The number of attribute sets used is limited for some protocols, as shown in Table 5-5.

Table 5-5. Tunnel protocols and tagged attribute sets

Tunnel protocol	Attribute sets used
L2TP	All specified attribute sets are used.
L2F	All specified attribute sets are used.
PPTP	Only the attribute set with the highest priority is used. Priority is defined by the Tunnel-Preference (83) value or by tag order.
ATMP	Only the two sets with the highest priority are used. (From the second attribute set, only the Tunnel-Server-Endpoint (67) value is used. Other values can be omitted.) Priority is defined by the Tunnel-Preference (83) value or by tag order.
IP-in-IP	Only the primary attribute set applies.

All the attribute sets in a profile must specify similar tunnel protocols, either all Layer 3 tunnels (such as ATMP) or Layer 2 tunnels (such as L2TP or L2F). You can mix L2TP and L2F only. The following examples show two valid cases:

```
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 = HApassword :1,
   Tunnel-Private-Group-ID = MyHomeNet :1
```

Tunnel attributes used with tags

Following are the tunnel attribute-value pairs that are relevant to transparent tunneling:

RADIUS Attribute	**Value**
Tunnel-Type (64)	Tunneling protocol(s) to be used. Currently, only L2TP (3) and L2F (2) operate with full tunnel attribute and tag support.
Tunnel-Medium-Type (65)	Medium for establishing the tunnel. Currently, IP (1) is the only supported value.
Tunnel-Client-Endpoint (66)	DNS hostname or dotted-decimal IP address of the LNS end point (a string value). If it specifies a hostname, the TAOS unit executes a DNS lookup for the host’s address.
Tunnel-Server-Endpoint (67)	IP address or hostname of the tunnel end point. If a DNS lookup returns several IP addresses, the system attempts to establish a tunnel to each address in turn.
Tunnel-Password (69)	Shared secret for authenticating the tunnel. For details, see “Tunnel authentication” on page A-33.
Tunnel-Private-Group-ID (81)	Identifies a group of users to an L2TP network server (LNS), TAOS units configured as LACs, and non-Lucent L2TP network servers that support this feature. This feature is also supported in the Ascend Tunnel Management Protocol (ATMP).
Tunnel-Assignment-ID (82)	Identification (name) assigned to tunnels to allow grouping sessions, a text string of up to 31 characters. The value has local significance only. It is not transmitted to the remote tunnel end point.

RADIUS Attribute	**Value**
Tunnel-Preference (83)	Numeric preference value for an attribute set. If more than one set of tunneling attributes is returned by the RADIUS server to the TAOS unit, the Tunnel-Preference attribute can be included in a set to indicate its relative preference, with the lowest preference value designating the most preferred set. If Tunnel-Preference is not included in any of the attribute sets, the sets are processed in the order of their respective tag numbers. If some but not all attribute sets include a Tunnel-Preference, those that do not are designated as the least preferred sets. Attribute sets with identical preferences are processed in random order.
Tunnel-Client-Auth-ID (90)	Name used by the tunnel initiator (the NAS) to authenticate the tunnel server. For details, see “Layer 2 Forwarding (L2F)” on page 5-26, “How the system finds a matching tunnel” on page 5-10, and “How the system name is selected (Hostname AVP)” on page 5-11.
Tunnel-Server-Auth-ID (91)	Name sent from the tunnel end point (the gateway or LNS) to the system initiating the tunnel during the tunnel authentication phase. The name can contain up to 31 characters. This attribute does not apply unless the protocol used to establish the tunnel is L2TP or L2F. The attribute can be specified in Access-Response packets and is generated in Accounting-Request packets.
Ascend-Tunnel-VRouter-Name (31)	Name of a virtual router (VRouter) to use for establishing the L2TP or L2F tunnel. The specified VRouter must exist on the LAC. For details, see “Configuring VRouters for L2TP, L2F, and ATMP connections” on page 6-13.

Tunnel attributes in Access-Accept and Accounting-Request messages

The following tables list the RADIUS and Ascend vendor-specific tunnel attributes and whether the attribute can be present in an Access-Accept message from the RADIUS server or an Accounting-Request message to the RADIUS server. These attributes support tagging. Table 5-6 lists the attributes described in RFC 2868 and RFC 2867. Tags are not generated for accounting records (see RFC2868 and RFC 2867 for additional information).

Table 5-6. RADIUS tunnel attributes that can be present in RADIUS messages

RADIUS attribute	ID	Type	Auth-Accept	Acct-Reply
Tunnel-Type	64	integer	Multiple instances allowed using tags.	One instance allowed.
Tunnel-Medium-Type	65	integer	Multiple instances allowed using tags. Can be omitted.	Not allowed.

Table 5-6. RADIUS tunnel attributes that can be present in RADIUS messages (continued)

RADIUS attribute	ID	Type	Auth-Accept	Acct-Reply
Tunnel-Client-Endpoint	66	string	Multiple instances allowed using tags. Can be omitted.	One instance allowed. Can be omitted.
Tunnel-Server-Endpoint	67	string	Multiple instances allowed using tags. Can be omitted.	One instance allowed. Can be omitted.
Acct-Tunnel-Connection	68	string	Not allowed.	One instance allowed.
Tunnel-Password	69	string	Multiple instances allowed using tags. Can be omitted.	Not allowed.
Tunnel-Private-Group-ID	81	string	Multiple instances allowed using tags. Can be omitted.	One instance of allowed. Can be omitted.
Tunnel-Assignment-ID	82	string	Multiple instances allowed using tags. Can be omitted.	One instance allowed. Can be omitted.
Tunnel-Preference	83	string	Multiple instances allowed using tags. Can be omitted.	Not allowed.
Tunnel-Client-Auth-ID	90	string	Multiple instances allowed using tags. Can be omitted	One instance allowed. Can be omitted
Tunnel-Server-Auth-ID	91	string	Multiple instances allowed using tags. Can be omitted	One instance allowed. Can be omitted

Table 5-7 lists the vendor-specific tunnel attribute that can be present in an Access-Accept message from the RADIUS server or an Accounting-Request message to the RADIUS server.

Table 5-7. Vendor-specific tunnel attribute

VSA **Vendor ID 529**	**ID**	**Type**	**Tag**	**Auth-Accept**
Ascend-Tunnel-VRouter-Name	31	string	Multiple instances allowed using tags. Can be omitted.	One instance allowed. Can be omitted

Consider the following:

- Some attributes are omitted from the Accounting-Request message if the default value applies or no value is specified in the Access-Request.
- An Accounting-Request message contains at most a single instance of any given attribute.
- An Access-Accept message can have multiple instances of a given attribute (belonging to different sets). Each instance must have a different tag value. If more than one instance of the same attribute with the same tag value is present, only one of is used and the rest are ignored.

Note: Ascend VSA (vendor ID 529) is used exclusively for ATMP tunnels.

Deprecated tunnel attributes

Table 5-8 and Table 5-9 list the deprecated tunnel attributes for RADIUS and Ascend vendor-specific attributes. These attributes do not support tagging and might be discontinued in a future software version.

Table 5-8. Deprecated RADIUS tunneling attributes

Attribute name	ID	Type	Auth-Accept	Acct-Reply
Tunneling-Protocol	127	integer	One instance allowed.	One instance allowed.
Ascend-Primary-Home-Agent	129	string	One instance allowed.	Not allowed.
Ascend-Secondary-Home-Agent	130	string	One instance is allowed. Can be omitted.	Not allowed.
Ascend-Home-Agent-IP-Addr	183	ipaddr	One instance is allowed. Can be omitted	One instance allowed.
Ascend-Home-Agent-Password	184	string	One instance allowed.	One instance allowed.
Ascend-Home-Network-Name	185	string	One instance allowed.	One instance is allowed. Can be omitted.
Ascend-Home-Agent-UDP-Port	186	integer	One instance is allowed. Can be omitted.	One instance allowed.

Table 5-9. Deprecated 16-bit vendor-specific tunnel attribute

16-bit Ascend VSA (Vendor ID 4846)	ID	Type	Auth-Accept	Acct-Reply
Ascend-Tunnel-Auth-Type	260	integer	Not allowed.	One instance allowed.

L2TP hidden attributes

By supporting hidden attributes in the current software version, the TAOS implementation of L2TP enables a unit to parse and decrypt hidden attributes as well as the random vector attribute-value pair. Note that the assigned tunnel ID attribute-value pair cannot be hidden in the Start-Control-Connection-Request (SCCRQ) message.

Example of reordering sets using Tunnel-Preference

Following is a sample profile that specifies three attribute sets, tagged 1, 2, and 3, with a Tunnel-Preference value that changes the order in which the NAS attempts tunnel establishment for this user:

```
joebloggs Password = "murphy"
    Tunnel-Type = L2TP : 1,
    Tunnel-Server-Endpoint = "1.1.1.1" : 1,
    Tunnel-Password = "loloaqic" : 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
```

With these preference values, the NAS identifies the attribute set tagged 2 as the primary attribute set, and first attempts to establish an L2F tunnel to a server at 2.2.2.2. It tries an L2TP tunnel to the LNS at 1.1.1.1 only if the initial tunnel attempt fails. If the second attempt also fails, the system attempts to establish an L2TP tunnel to 3.3.3.3.

Using DNS to select multiple servers

By taking advantage of the DNS list feature, you can set a TAOS unit operating as a LAC to attempt to connect to a series of server end points if the first attempt fails.

To use this feature, you must configure the TAOS unit for DNS list and the DNS servers at your site must support a list feature that enables them to return multiple addresses for a hostname in response to a DNS query. For details about configuring DNS list, see “Configuring DNS lookups and a DNS list” on page 2-53.

The following example shows how to enable DNS list with a maximum of 3 hosts in the list:

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

admin> set dns-list-attempt = yes

admin> set dns-list-size = 3

admin> write
IP-GLOBAL written
```

For the TAOS unit to use DNS list when attempting to bring up a tunnel, the client’s Connection or RADIUS profile must specify a DNS-resolvable hostname as the tunnel end point. For example, the following command shows a hostname specified as the primary tunnel-server in a Connection profile:

```
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
```

Following is a RADIUS profile with a comparable setting:

```
5551000 Password = "Ascend-CLID", Service-Type = Call-Checks
   Tunnel-Type = L2TP,
   Tunnel-Medium-Type = IP,
   Tunnel-Server-Endpoint = "tunnel-endpoint-1"
```

When the client dials in, the system sends a DNS query to resolve the tunnel-server hostname. If it receives a list of IP addresses in return, the TAOS unit first tries to connect to the first IP address in the list. If that attempt fails, the unit continues to attempt to connect to the IP addresses in the list until a tunnel is successfully established, the DNS list has no more IP addresses, or the connection times out.

L2TP, PPTP, and L2F disconnect and progress codes

The current software release supports progress codes for the following tunneling protocols:

- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)

This release also supports disconnect codes for L2TP.

You can use disconnect and progress codes to troubleshoot the configuration of your unit's tunneling systems. These progress and disconnect codes are logged by the Syslog, RADIUS accounting, and call logging servers.

The following progress codes are reported by tunneled calls using L2TP, PPTP, or L2F:

Progress code	Description
240	Tunnel is being started. Set when the unit has determined that a call must be tunneled. Errors occurring during this period usually indicate that a tunnel server entry is invalid.
241	System is resolving the address of a remote tunnel server end point by DNS. Errors occurring during this period usually indicate a problem with DNS or an invalid tunnel server entry.
242	System is contacting a remote tunnel server. Set after the unit has resolved the address of the remote tunnel end point and has started trying to contact it. Errors occurring during this phase usually indicate that the remote server is unreachable because it is not operating, because no route to it exists, or because of tunnel authentication errors, depending on the tunneling protocol used. Call authentication errors do not usually affect this phase.
243	Call is being transferred to a remote tunnel server. Set after the unit contacts the remote tunnel end point. At this point, the two tunnel end points are actively working on establishing the tunnel, authenticating each other if needed, and negotiating the tunnel session (tunnel authentication is independent of user authentication). Errors occurring during this phase usually indicate resource or configuration problems on the remote server, such as incorrect or invalid tunnel passwords or configuration conflicts.
244	Tunnel is established. Call has been tunneled to the remote tunnel end point and it is ready to transfer data. This code is sometimes superseded by code 60 (Session up).

The following disconnect codes are supported by tunneled calls using L2TP:

Disconnect code	Description
730	Unknown reason.

731 Tunnel protocol is disabled by a configuration setting or software license.

732 Operation is disallowed by configuration.

733 Invalid tunnel end point entry values.

734 Out of resources.

735 Tunnel end point is being shut down. All calls and tunnels using the same tunnel end point are affected.

736 Administrative tunnel disconnect. All calls using the same tunnel are affected. Other tunnels to the same tunnel end point are not affected.

750 Server is not responding because it timed out.

751 Server is not responding to periodic hello commands.

752 Tunnel authentication failed.

753 Missing tunnel password. A tunnel password is required but cannot be found.

754 Tunnel protocol error. A protocol mismatch probably occurred between the tunnel end points.

770 Call was cleared due to carrier loss.

771 Call failed because no carrier was detected.

772 Call failed due to a busy signal.

773 Call failed due to a lack of dial tone.

774 Call failed due to an invalid destination number.

775 Call failed because of invalid framing or because no framing was detected.

776 Incoming call was rejected by the remote tunnel end point for unspecified reasons.

777 Outgoing call was rejected by the remote tunnel end point (LAC) for unspecified reasons.

778 Call was not established within the allotted time.

For example, if you issue the `l2tpstop` command on the terminal screen to disconnect an L2TP tunnel, the following codes are reported on the LAC:

```
admin> l2tpstop 2

Syslog :

    Nov 10 17:04:21 tnt 1/5: [1/5/1/0] STOP: ’test’; cause 736.;
    progress 244.; host 0.0.0.0 [MBID 1; 54507->4739] [test]

    Nov 10 17:04:21 tnt 1/5: [1/5/1/0] LAN session info: Conn=(PPP
    31200/33600 244/736) Auth=(16 0/0 18/1) Sess=(24 133/5 220/7)
    Tunn=(L2TP s=1.1.1.2 cid=tnt sid=max a=l2tp-tunnel) [MBID 1; 54507-
    >4739] [test]

RADIUS accounting:

    Ascend-Disconnect-Cause = 736 (DIS_L2TUNNEL_ADMIN_DISCONNECT)
    Ascend-Connect-Progress = 244 (PR_TUNNEL_UP)
```

Note: The preceding Syslog output is shown on multiple lines because of space limitations.

Virtual Routers (VRouters)

6

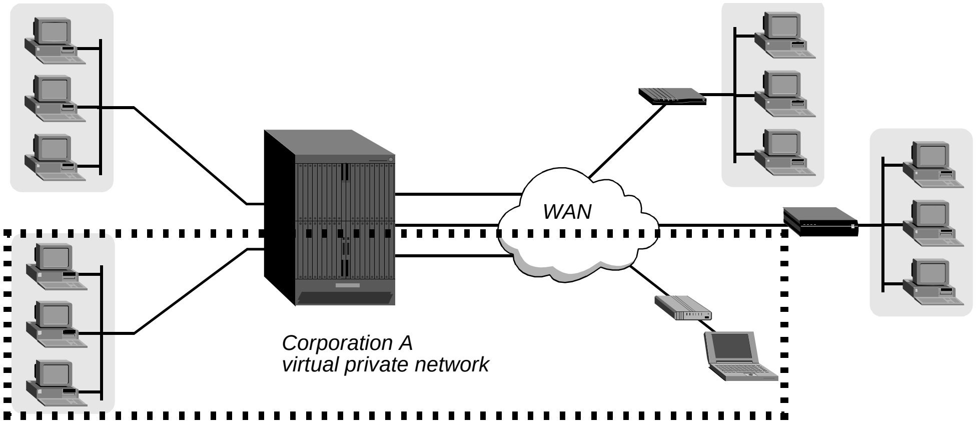
Configuring VRouters

A virtual router (also called a *VRouter*) is a grouping of interfaces in the TAOS unit. Each VRouter has its own associated routing table, ARP table, route cache, and address pools, and maintains its own routing and packet statistics.

If you do not configure any VRouters, the TAOS router operates exactly as it has in earlier versions of the software. When one or more VRouters are specified, the main router operates as the global VRouter. All interfaces that are not explicitly grouped with a defined VRouter are grouped with the global VRouter.

Figure 6-1 shows a TAOS unit with one VRouter operating for Corporation A. Interfaces related to Corporation A are grouped and handled by one VRouter, creating a virtual private network (VPN) for Corporation A. Corporation A's WAN interfaces can dial in to a local TAOS unit, which can be on a public network, to reach Corporation A's private LANs.

Figure 6-1. Virtual IP routing



How VRouters affect the routing table

When VRouters are not defined, the TAOS router maintains a single IP routing table that enables the router to reach any of its many interfaces. In that context, each interface known to the system requires a unique address.

With VRouters, addresses must be unique within the VRouter's routing domain, but not necessarily within the TAOS unit. Because each VRouter maintains its own routing table, and because it knows about only those interfaces that explicitly specify the same VRouter, there is no requirement that the private networks maintain unique address spaces.

How VRouters affect network commands

The following commands support virtual routing. If no VRouter name is specified on the command line, the global VRouter is assumed. If a VRouter name is specified, the command performs its usual function but applies only to the specified VRouter:

Command	**Usage with optional VRouter arguments**
Netstat	netstat [*VRoutername*] -options [*params*]
IProute	iproute add [-r *vRouterName*] *destination/size* *gateway* [*pref*] [*metric*]
	iproute delete [-r *vRouterName*] *destination/size* [*gateway*]
Traceroute	traceroute [-n] [-v] [-m *max_ttl*] [-p *port*] [-q *nque-ries*] [-w *waittime*] [-r *vRouter*] [-s *src_addr*] *host-name* [*datasize*]
IPcache	ipcache [-r *vRouterName*] [debug] [cache]
Ifmgr	ifmgr -r [*vRouterName*] *-option* -d (d)isplay interface table entries. -d *ifNum* (d)etails of given i/f table entry. -t (t)oggle debug display. ifmgr [up|down] [*ifNum*|*ifName*]
ARPtable	arptable [*vRouter*] [[-a *hostname MAC_address*] | [-d *hostname*] | [-f]] [*vRouter*]: VRouter to which this ARP command is applicable [-a *hostname MAC_address*]: Adds hostname entry to the ARP table with MAC_address [-d *hostname*]: Deletes hostname from ARP table [-f]: Clears an entire ARP cache
IP-Pools	ip-pools [*vRouterName*]
Ping	ping [-q | -v] [-i *sec* | -I *msec*] [-s *packet-size*] [-r *vRouter*] [-x *source_address*] *host-name*
Telnet	telnet [-a | -b | -t] [-v *VRouterName*] [-l[e] | -r[e]] *host-name* [*port-number*]

Current VRouter limitations

Currently, SNMP management does not display information about the TAOS unit on a per-VRouter basis. Errors and events are not logged on a per-VRouter basis. The Syslog host defined in the system’s Log profile must be accessible to the main VRouter.

Currently, the ATMP Home Agent in router mode presents incoming packets only to the main VRouter. In addition, servers defined in the following profiles must be accessible to the main VRouter:

- Debug
- Trap
- External-Auth
- IP-Global (for SNTP and multicast)
- Call-Logging
- SNMP
- SS7-Gateway
- Stacking
- Transaction-Server
- VoIP

Creating a VRouter

When at least one VRouter profile is configured, the System-IP-Address parameter and the Global-VRouter parameter in the IP-Global profile apply to the global VRouter. All interfaces that are not explicitly assigned to another VRouter are grouped with the global VRouter.

For each VRouter in the system, an instance of RIP is created to process routes. The new instance of RIP sends and receives update packets only on the interfaces associated with its particular VRouter and manipulates only that VRouter’s routing table. A default instance of RIP is always created for the global VRouter.

When you create a VRouter, the new instance of RIP sends and receives packets only on the interfaces associated with that VRouter and manipulates only that VRouter’s routing table. All RIP-related parameters in a VRouter profile use default settings that are recommended for most sites.

Settings in a VRouter profile

A VRouter profile contains the following parameters (shown here with default values):

```
[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+
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 0 +
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""+
pool-summary = no
rip-policy = Poison-Rvrs
```

```
summarize-rip-routes = no
rip-trigger = yes
```

Parameter	Specifies
Name	Unique name for the VRouter, up to 15 characters. Interfaces belonging to the VRouter are grouped by specifying this name in the IP-Interface or Connection profile.
VRouter-IP-Address	System IP address for the VRouter.
Pool-Base-Address Assign-Count Pool-Name Pool-Summary	IP address pools for the VRouter. The parameters operate identically to the parameters of the same names in the IP-Global profile, except that they are exclusive to one VRouter. If address pools are not specified in a VRouter profile, VRouters can share the address pools defined in the IP-Global profile.
RIP-Policy	Policy for sending update packets that include routes received on the same interface. (For details, see “RIP policy for propagating updates back to the originating subnet” on page 2-42.)
Summarize-RIP-Routes	If the VRouter is running RIP-v1, the Summarize-RIP-Routes parameter specifies whether to summarize subnet information when in advertisements. If the VRouter summarizes RIP routes, it advertises a route to all the subnets in a network of the same class. For example, the route to 200.5.8.13/28 (a class C address) would be advertised as a route to 200.5.8.0. When the VRouter does not summarize information, it advertises each route in its routing table as is.
RIP-Trigger	Enable/disable RIP triggering. With a setting of Yes (the default), RIP updates include only changed routes. (For details, see “RIP triggering” on page 2-42.)

Example of defining a VRouter

The following commands create a VRouter for Corporation A:

```
admin> new vrouter corpa
VROUTER/corpa read

admin> list
[in VROUTER/corpa (new)]
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+
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 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
```

Displaying the VRouter's routing and interface tables

The new VRouter defined for Corporation A in "Example of defining a VRouter" maintains the following minimal routing and interface tables at this point:

```
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
```

Displaying the VRouter's statistics

The VRouter also maintains its own IP, TCP, UDP, and ICMP statistics. For example:

```
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 resonse packets sent
       0 leave packets sent
mcast:
       0 packets received
       0 packets forwarded
       0 packets in error
       0 packets dropped
       0 packets transmitted
```

Note: There is no support for IP multicast on a per-VRouter basis, so the IGMP and MCast statistics relate only to the global VRouter.

Defining address pools for a VRouter

The following commands define an address pool for the Corporation A VRouter defined in "Example of defining a VRouter" on page 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
```

Following is a comparable RADIUS pool definition:

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User
   Ascend-IP-Pool-Definition = "1 130.100.100.128 127 corpa"
```

The Corporation A VRouter is now maintaining the following pool of addresses:

```
admin> ip-pools corpa

Pool#                Base         Count      InUse
   1           130.100.100.128      127          0

 Number of remaining allocated addresses:    0
```

Note: The Ascend-IP-Pool-Definition attribute supports a VRouter name as the last syntax element in a pool definition. The value of Ascend-IP-Pool-Definition uses the following syntax:

```
"pool-num base-addr assign-count [vrouter-name]"
```

For background information about address pools, see “Configuring and using address pools” on page 2-62. The process of defining address pools for a VRouter is the same as described in that section.

Assigning interfaces to a VRouter

To assign VRouter membership to an interface, you specify a VRouter name in the interface profile. In addition to PPP and other framed connections, TCP-Clear connections are also managed on a per-VRouter basis. If a Connection profile or RADIUS profile is associated with a VRouter and configured for TCP-Clear, the system locates the specified host only in the VRouter’s routing table.

Settings in local profiles

To assign VRouter membership to an interface in local profiles, set the VRouter parameter. For example:

```
[in IP-INTERFACE/{ { shelf-1 slot-5 5 } 0 } ]
vrouter = corpa
```

```
[in CONNECTION/corpa-client]
vrouter = corpa
```

Parameter	Specifies
VRouter	Name of a defined VRouter. Specifying the VRouter name groups the interface with the VRouter. The default null value specifies the global VRouter.

Settings in RADIUS profiles

RADIUS uses the following attribute-value pair to support the use of a VRouter:

RADIUS Attribute	Value
Ascend-VRouter-Name (102)	Name of a defined VRouter. Specifying the VRouter name groups the interface with the VRouter. The default null value specifies the global VRouter.

Examples of assigning VRouter membership to interfaces

The following commands group three WAN interfaces with the `corpa` VRouter:

```
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
```

Following are comparable settings in RADIUS profiles:

```
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"
```

Displaying assigned interfaces in the VRouter's tables

After interfaces have been assigned, as described in "Examples of assigning VRouter membership to interfaces" on page 6-8, new interfaces show up in the VRouter's routing and interface tables when the interfaces become active. For example:

```
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
```

Defining VRouter static routes

You specify a static route associated with a VRouter for one of the following reasons:

- To define a route on a per-VRouter basis
- To specify an inter-VRouter route

Settings in an IP-Route profile

Following are the VRouter-related parameters (shown here with default values) in IP-Route profiles:

```
[in IP-ROUTE/""]
vrouter = ""
inter-vrouter = ""
```

Parameter	**Specifies**
VRouter	Name of the VRouter that will own this route. The route will be part of that VRouter’s routing table. If no name is specified (the default), the global VRouter is assumed.
Inter-VRouter	Name of a VRouter to use as the route’s next hop. Packets destined for the route’s destination address are sent to the specified VRouter, which consults its own routing table to further route the packets. The Gateway-Address parameter must be set to the zero address for this parameter to apply.

Settings in RADIUS profiles

The value of the Framed-Route (22) attribute can specify a VRouter name in the following syntax:

"*dest-addr* [*/prefix*] *gateway-addr metric* [*private*] [*profile*] [*preference*] [*vrouter-name*]"

Note: The fields within the value of the Framed-Route attribute are positional. With the exception of the optional prefix-length specification, if any of the optional fields are specified, the optional fields to the left of that setting must also be specified.

Examples of defining a route on a per-VRouter basis

Following is an example of defining a static route to Corporation B. This route is within the Corporation A VRouter domain (the VRouter named `corpa` will own this route).

```
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
```

Following is a comparable RADIUS profile:

```
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"
```

Displaying the static route in the VRouter’s table

The following sample output shows the new static route that was added to the Corporation A VRouter’s routing table in “Examples of defining a route on a per-VRouter basis” :

```
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
```

Specifying an inter-VRouter route

In the following example, the static route specifies the Corporation A VRouter as the route's next hop. All packets to the specified destination network are sent to the specified VRouter for a routing decision.

```
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
```

Following is a comparable RADIUS route profile:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User
   Framed-Route = "11.0.0.0/28 0.0.0.0 corpa"
```

Displaying the inter-VRouter route in the global table

In the following example, the route has been added to the global VRouter's routing table, not to that of the Corporation A VRouter:

```
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
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
```

Configuring VRouter domain name servers

VRouter DNS configuration includes settings for primary and secondary DNS servers, domain names, and client DNS servers. The settings direct connections that belong to the VRouter to a particular DNS service. To completely segment the VRouter's DNS information from any other hosts, you can configure and manage DNS information separately for each VRouter. The addresses configured for client DNS servers are presented to dial-in users during IP Control Protocol (IPCP) negotiation.

If DNS information is not found in the VRouter profile, the system uses the DNS information in the IP-Global profile. The DNS list and the local DNS table maintained in RAM are systemwide DNS configurations that are not supported separately for each VRouter.

Overview of VRouter DNS settings

Following are the VRouter-specific DNS parameters (shown with their default settings):

```
[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
```

Parameter	**Specifies**
Domain-Name	Primary domain name (up to 63 characters) to use for DNS lookups for this VRouter. The TAOS unit appends this domain name to hostnames when performing lookups.
Sec-Domain-Name	Secondary domain name to use for DNS lookups for this VRouter if the hostname is not found in the primary domain.
DNS-Primary-Server	Address of the primary local DNS server to use for lookups for this VRouter.
DNS-Secondary-Server	Address of the secondary local DNS server to use for lookups for this VRouter. Used only if the primary server is not found.
Client-DNS-Primary-Server	Address of a client DNS server for dial-in clients of this VRouter.
Client-DNS-Secondary-Server	Address of a secondary DNS server for dial-in clients of this VRouter.
Allow-As-Client-DNS-Info	Enable/disable use of main (local) DNS information if the client DNS servers are not found. To isolate local network information for this VRouter, set to `false`.

Example of a typical VRouter DNS configuration

The following commands specify a primary and secondary domain name for DNS lookups for a VRouter named `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
```

If a lookup fails in the first domain, the router tries again with the secondary domain name. To enable the TAOS unit to use DNS to look up addresses, specify DNS server addresses, as shown in the following example:

```
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
```

If the primary server is unavailable, the TAOS unit attempts a lookup on the secondary server. The following commands configure a client DNS server for this VRouter:

```
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
```

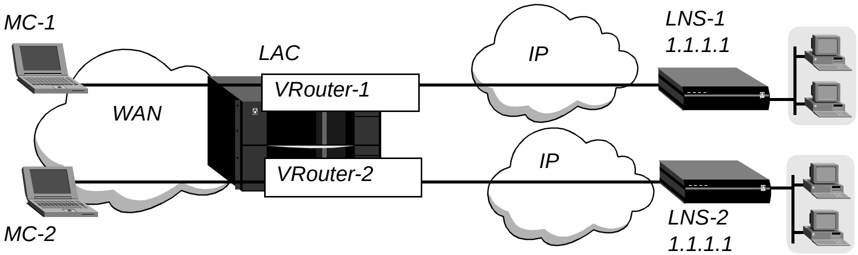
The secondary server is accessed only if the primary one is inaccessible. If both of these client DNS servers are not accessible, the TAOS unit does not allow the client to access local DNS servers. For information about administrative commands for VRouter DNS, see the *APX 8000/MAX TNT Administration Guide*.

Configuring VRouters for L2TP, L2F, and ATMP connections

In previous releases, tunnels used only the main VRouter. In the current software version, you can build L2TP, L2F, and ATMP tunnels on specific VRouters. L2TP, L2F, and ATMP packets (control channel and encapsulated data) are sent using the configured VRouter for that tunnel. For information about L2TP and L2F tunnels, see Chapter 5, “L2TP, L2F, PPTP, and IP-in-IP Tunneling.” For information about ATMP, see Chapter 4, “Ascend Tunnel Management Protocol (ATMP).”

Because each VRouter maintains its own routing table and knows about only those interfaces that explicitly specify the same VRouter, this feature allows the system to separate traffic for different LNS systems. For example, Figure 6-2 shows two dial-in clients, MC-1 and MC-2. Each client tunnels to a different LNS, but both LNS systems have the IP address 1.1.1.1. Because the tunnels are built on separate VRouters, the traffic is kept separate and directed to the appropriate server endpoint.

Figure 6-2. L2TP tunnels built on separate VRouters



Note that TAOS unit must dedicate one IP interface to each VRouter. Following are the parameters, shown with sample values, for dedicating an Ethernet or a WAN IP interface to a VRouter:

```
[in IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 }]
vrouter = VRouter-1
```

```
[in CONNECTION/LNS-2]
vrouter = VRouter-2
```

Connection profile setting

Following is the parameter (shown with its default value) for specifying a VRouter name:

```
[in CONNECTION/MC-1:tunnel-options]
vrouter = ""
```

Parameter	Specifies
VRouter	Name of a virtual router to use for establishing the L2TP tunnel. The specified VRouter must exist on the LAC. With the default null value, the global VRouter is used.

For example, the following commands configure a mobile-client profile for an L2TP session that belongs to a VRouter named 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
```

With this sample profile, the TAOS unit authenticates the caller before building a tunnel to the LNS at 1.1.1.1 on the specified VRouter.

RADIUS profile setting

RADIUS uses the following attribute-value pair to specify a VRouter name:

RADIUS attribute	**Value**
Ascend-Tunnel-VRouter-Name (31)	Name of a virtual router to use for establishing the L2TP or L2F tunnel. The specified VRouter must exist on the LAC. With the default null value, the global VRouter is used. This attribute supports tagging.

For example, the following mobile-client profile specifies an L2TP session that belongs to a VRouter named 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"
```

Following is a sample RADIUS profile for an ATMP connection:

```
commgroup Password="123"

User-Service=Framed-User,
Framed-IP-Address=199.199.199.200,
Framed-IP-Netmask=255.255.255.0,
Framed-Protocol=PPP,
Ascend-Route-IP=1,
Tunnel-Type = ATMP
Tunnel-Server-Endpoint=10.5.7.2,
Tunnel-Password = "atmp",
Ascend-Home-Agent-UDP-Port=5150,
Ascend-Home-Network-Name="HOMNET",
Ascend-Tunnel-VRouter-Name = "companyvr"
```

Creating VRouters in IPX networks

A VRouter is a grouping of the LAN or WAN interfaces in a TAOS unit. Each VRouter has its own associated IPX ARP table, IPX routing table, IPX service table, IPX session table, IPX address pools, IPX ping statistics, IPX traffic statistics, and IPX dial-in route tables.

Creating an IPX VRouter

You create a VRouter profile for an IPX network just as you would for an IP network. For detailed instructions on how to create a VRouter profile, see *"Creating a VRouter"* on page 6-3.

For an IPX netwOrk, you configure the VRouter profile by setting the following parameters. Parameters in the VRouter profile that are not in the following list do not apply to IPX networks.

Parameter	Specifies
Name	Unique name for the VRouter, up to 23 characters. To group interfaces belonging to this VRouter, you specify this value in the IPX-Interface profile. See “Assigning the IPX interface to a VRouter” on page 6-17.
Ipx-Routing-Enabled	Enable/disable IPX routing on the specified VRouter. Set this parameter to `yes` to enable IPX routing on the VRouter. By default, this parameter is set to `no`.
Ipx-Dialin-Pool	Dial-in pool of IPX network addresses to be shared by the IPX WAN interfaces. Specify the addresses in dotted-hexadecimal notation, similar to that of an IPX network number. If no dial-in pool is specified, the TAOS unit uses the global VRouter pool specified in the IPX-GLOBAL profile.

Example of defining an IPX VRouter

The following commands create a VRouter profile `ipxcorp1`:

```
admin> new vrouter ipxcorp1
VROUTER/ipxcorp1 read

admin> set ipx-routing-enabled = yes
admin> set ipx-dialin-pool = 00:00:00:00

admin> write

VROUTER/ipxcorp1 written
```

Defining a global IPX VRouter

You configure a global VRouter for a TAOS unit by setting the `global-vrouter` parameter in the IPX-GLOBAL profile.

Parameter	Specifies
Global-Vrouter	Unique name for a global VRouter, up to 23 characters. By default, this parameter is set to `main`.

The following commands define a global VRouter for a TAOS unit in an IPX network:

```
admin> read IPX-GLOBAL
IPX-GLOBAL read

admin> list

[in IPX-GLOBAL]

interface-address = { { any-shelf any-slot 0 } 0 }
ipx-routing-enabled = no
ipx-dialin-pool = 00:00:00:00
global-vrouter = main

admin> set global-vrouter = mainv
admin> write
IPX-GLOBAL written
```

Assigning the IPX interface to a VRouter

You assign an IPX interface to a VRouter by setting the VRouter parameter in the IPX-Interface profile.

Parameter	Description
Vrouter	Assigns the IPX interface to a VRouter. If no VRouter is specified, the interface belongs to the global VRouter.

The following set of commands assigns an IPX interface to the VRouter `ipxcorp1:`

```
admin> read ipx-interface {{1 15 1}}
IPX-INTERFACE/{ { shelf-1 slot-15 1 } 0 } read
admin> list
[in IPX-INTERFACE/{ { shelf-1 slot-15 1 } 0 }]
admin> set vrouter = ipxcorp1
admin> write
IPX-INTERFACE/{ { shelf-1 slot-15 1 } 0 } written
```

Static routes for VRouters

In an IPX network, a TAOS unit uses the VRouter setting specified in the IPX-Route profile to dial out to reach the destination network. You do not have to modify the settings in the IPX-Route profile.

Displaying VRouter network information

The Netware command shows IPX network and server information for a specified VRouter. If no VRouter is specified, the unit displays statistics for the global VRouter. You use the Netware commands as follows:

```
netware [vroutername] [-option]
```

Syntax element	Description
Vroutername	VRouter for which you want to display IPX network and server information.
-n	Displays NetWare IPX networks.
-p	Displays NetWare IPX pings.
-s	Displays NetWare IPX servers.
-t	Displays NetWare IPX statistics.

Current limitations on VRouters in IPX networks

- SNMP management does not display information about a TAOS unit on a per-VRouter basis. Errors and events are not logged on a VRouter basis. The existing VRouter implementation in TAOS does not have a MIB.

- The TAOS implementation of VRouters for IPX networks does not include support for ATMP or L2TP tunnel handling on a VRouter basis.
- The Service Advertising Protocol (SAP) home server proxy is not handled on a VRouter basis.
- IPX stacking on a VRouter basis is not supported.

Deleting a VRouter

Deleting a VRouter profile deletes the virtual router. For example:

```
admin> delete vrouter corpa
```

Lucent Technologies recommends that you reset the system after deleting a VRouter with active connections. If a system reset is not possible, the recommended course of action before deleting the VRouter is to manually tear down its active connections, and then modify the local Connection, IP-Interface, and IP-Route profiles that point to the VRouter to point instead to the global VRouter or another existing VRouter

IPX Routing

7

IPX routing on the WAN

A TAOS unit configured for IPX routing enables NetWare clients and distributed Novell networks to use NetWare services across the WAN. Lucent Technologies has optimized IPX routing for the WAN. The optimization required some modifications of standard IPX behavior and the addition of IPX extensions to enable the TAOS unit to operate as clients expect for NetWare LANs. This section discusses issues related to scaling LAN protocols to the WAN.

How TAOS units use IPX SAP

A TAOS unit follows standard IPX Service Advertising Protocol (SAP) behavior for routers when connecting across the WAN to IPX devices that do not run TAOS software. However, when it connects to another TAOS unit configured for IPX routing, both ends of the connection exchange their entire SAP tables.

When a NetWare client sends a SAP request to locate a service, the TAOS unit consults its SAP table and replies with its own hardware address and the internal network address of the requested server. This is analogous to proxy ARP in an IP environment. The client can then transmit packets whose destination address is the internal address of the server. When the TAOS unit receives those packets, it consults its RIP table. If it finds an entry for their destination address, it brings up the connection (unless it is already up) and forwards the packets.

How TAOS units use IPX RIP

A TAOS unit follows standard IPX RIP behavior for routers when connecting to IPX devices that do not run TAOS software. However, when it connects to another TAOS unit configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, each TAOS unit maintains the imported RIP entries as static until the unit is reset or power cycled.

How IPX RIP works

IPX RIP is similar to the routing information protocol in the TCP/IP protocol suite, but it is a different protocol. IPX routers broadcast RIP updates both periodically and each time a WAN connection is established. The TAOS unit receives IPX RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

IPX RIP default route

A TAOS unit recognizes network number –2 (0xFFFFFFFE) as the IPX RIP default route. When it receives a packet for an unknown destination, it forwards the packet to the IPX router advertising the default route. For example, if the TAOS unit receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the TAOS unit forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet. If more than one IPX router is advertising the default route, the unit makes a routing decision based on hop and tick count.

Support for IPXWAN negotiation

The TAOS unit supports the IPXWAN protocol, which is essential for communicating with the Multi-Protocol Router and with Novell software (such as NetWare Connect2) that supports dial-in connections. For full specifications of the IPXWAN protocol, see RFC 1634 and *NetWare Link Services Protocol Specification—IPX WAN Version 2*.

When two TAOS units bring up an IPX connection, they negotiate all options during the IPXCP phase. IPXWAN negotiation never takes place between two TAOS units, because neither unit initiates the negotiation process by sending out an IPXWAN Timer_Request packet.

Connections with IPX devices that do not run TAOS software, but use Novell software operating over PPP, do not negotiate options during the IPXCP phase, so all options are negotiated during the IPXWAN phase of link establishment. The far-end device sends an IPXWAN Timer_Request packet, which triggers IPXWAN negotiation in the TAOS unit. The devices compare internal network numbers and assign the slave role to the unit with the lower number. The other unit becomes the master of this link for the duration of the IPXWAN negotiation. The slave unit returns an IPXWAN Timer_Response packet, and the master unit initiates an exchange of information about the final router configuration. The TAOS unit supports the following routing options:

- TAOS IPX Routing—unnumbered RIP or SAP without aging.
- Novell Routing (Unnumbered RIP/SAP with aging)
- None. The peer is a dial-in client. No RIP or SAP are used except on request, and you can assign Net and Node Numbers.)

Header compression is rejected as a routing option. After IPXWAN negotiation is completed, transmission of IPX packets begins, using the negotiated routing option.

Extensions to standard IPX

NetWare uses dynamic routing and service location, so clients expect to be able to locate a server dynamically, regardless of where it is physically located. Because this scheme was designed to work in a LAN environment, not for WAN operations, TAOS provides extensions to standard IPX. The added features enhance WAN functionality, as shown in Table 7-1.

Table 7-1. TAOS IPX extensions

TAOS IPX extensions	Purpose
Virtual network for dial-in clients	To enable it to route IPX to nonrouters (NetWare clients), the TAOS unit supports a virtual IPX network defined in its IPX-Global profile. The unit can therefore assign a unique network address to the client. The client's connection must specify that it is a dial-in peer.
Accepting or rejecting RIP and SAP updates	The TAOS unit can transmit RIP and SAP updates, receive them, or both, or you can disable RIP or SAP updates for any IPX routing connection.
Bringing up connections in response to a SAP query	The Dial-Query feature is designed for sites that support many clients and connections to only a few remote IPX networks. The TAOS unit brings up all connections that enable Dial-Query when it receives a SAP query for a file server (service type 0x04) and its SAP table has no entry for that service type.
Static routes to servers	Even though the TAOS unit learns its routes via RIP, it clears the entire RIP table when reset or powered down. Some sites configure a static IPX route to enable the TAOS unit to open a connection to that location and download the RIP table when the unit is powered up.
SAP filters	IPX SAP filters enable you to prevent the SAP table from becoming too large, by explicitly including or excluding servers, services, or service types on any interface.

Recommendations for NetWare client software

NetWare clients on a WAN do not need special configuration in most cases. However, if the local network supports NetWare servers, you should configure NetWare clients with a preferred server on the local network, not at a remote site. If the local network does not support NetWare servers, configure local clients with a preferred server that is on the network with the lowest connection costs. For more information, see the NetWare documentation.

Because of possible performance issues, executing programs remotely is not recommended. For best results, put LOGIN.EXE on each client's local drive.

Both Macintosh and UNIX clients can use IPX to communicate with servers. However, both types of clients also support native protocols: AppleTalk (Macintosh) or TCP/IP (UNIX). If

Macintosh clients must access NetWare servers across the WAN by using AppleTalk software (rather than MacIPX), the TAOS unit must support AppleTalk routing. Otherwise, AppleTalk packets will not make it across the connection. If UNIX clients access NetWare servers by means of TCP/IP (rather than UNIXWare), the TAOS unit must also be configured as an IP router. Otherwise, TCP/IP packets will not make it across the connection.

Note: Packet Burst lets servers send a data stream across the WAN before a client sends an acknowledgment. The feature is included automatically in server and client software for NetWare 3.12 or later. If local servers are running NetWare 3.11, they should have PBURST.NLM loaded. For more information, see your NetWare documentation.

Configuring the IPX-Global profile

Before you can configure IPX on a LAN interface, you must enable IPX routing globally. You also have the option of defining a virtual IPX network to be used for assigning IPX addresses to NetWare clients that do not present an address. Following are the relevant parameters (shown with sample settings):

```
[in IPX-GLOBAL]
ipx-routing-enabled = yes
ipx-dialin-pool = 12:34:56:78
```

Parameter	Specifies
IPX-Routing-Enabled	Enable/disable IPX routing for the interface. When you write the profile, the TAOS unit comes up in IPX routing mode. At that time, it creates an IPX-Interface profile for each installed Ethernet port.
IPX-Dialin-Pool	An IPX network number to be used for assigning an IPX address to certain dial-in clients. The number must be unique in the entire IPX routing domain. For details, see “Defining a virtual IPX network for dial-in clients."

Defining a virtual IPX network for dial-in clients

When a NetWare client dials in, the TAOS unit negotiates a routing session with the client by assigning the client an address on the virtual IPX network. The client must accept the network number, but if it has its own node number, the TAOS unit uses that number to form the full network:node address. If the client does not have a node number, the TAOS unit assigns it a unique node address on the virtual network.

The IPX network number you assign must be unique within the entire IPX routing domain of the TAOS unit. The TAOS unit advertises the route to this virtual IPX network.

Example of an IPX-Global configuration

Following is an example of how to enable IPX routing mode and define a network for address assignment to dial-in clients that are not routers:

```
admin> read ipx-global
IPX-GLOBAL read
```

```
admin> set ipx-routing-enabled = yes

admin> set ipx-dialin = cccc1234

admin> write
IPX-GLOBAL written
```

When you write the profile, the TAOS unit enters IPX routing mode and creates IPX-Interface profiles for each Ethernet interface. Be sure that the network number you assign to the IPX-Dialin parameter is unique in the TAOS unit routing domain.

Configuring LAN IPX interfaces

After you enable IPX routing in the IPX-Global profile, the system creates an IPX-Interface profile for each Ethernet interface in the system. IPX-Interface profiles do not exist until you enable IPX routing globally.

Note: Even if the TAOS unit does not support IPX routing on the shelf-controller Ethernet interface, IPX-Routing-Enabled must be set to Yes, and a valid IPX frame type must be specified, in the IPX-Interface profile for the shelf-controller Ethernet ports.

Overview of LAN IPX settings

The IPX-Interface profiles contain the following parameters (shown with their default settings):

```
[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 = ""
```

Parameter	Specifies
IPX-Routing-Enabled	Enable/disable IPX routing on the interface, provided that the IPX-Frame parameter is also set.
IPX-Frame	Specifies the IPX frame type the TAOS unit will route and spoof. With a setting of None (the default), IPX routing is disabled on the interface. Valid values are 802.2 (for NetWare 3.12 or later), 802.3 (for NetWare 3.11 or earlier), SNAP, and Enet-II.
IPX-Net-Number	The IPX network number in use on the segment. The default zero address enables the system to acquire the number from other IPX routers on the network.
IPX-Type-20	Enables/disable propagation of Type-20 packets on the LAN interface. For details, see “Propagating IPX Type-20 packets on a LAN interface” on page 7-6.
IPX-SAP-Filter-Name	Name of an IPX-SAP Filter profile, to be applied to the LAN interface. For details, see “Example of applying a SAP filter to a LAN interface” on page 7-17.

Enabling IPX routing and spoofing on the interface

To enable TAOS units to route IPX on an Ethernet interface, you must set both the IPX-Routing-Enabled parameter and the IPX-Frame parameter. The IPX-Frame parameter specifies which IPX frame type the TAOS unit will route and spoof.

Note: A TAOS unit routes and spoofs only one IPX frame type. If some NetWare software transmits IPX in a frame type other than the type you specify, the unit drops those packets. If you are not familiar with the concept of packet frames, see the Novell documentation.

To determine which frame type to use on a LAN interface, go to a NetWare server's console on that segment and type LOAD INSTALL to display the AUTOEXEC.NCF file. Following is a sample AUTOEXEC.NCF line that specifies 802.3 frames:

```
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

Assigning an IPX network number

If there are other NetWare routers (servers) on the LAN interface, the IPX number assigned to the TAOS unit for that interface must be consistent with the number in use by the other routers. The best way to ensure such consistency is to leave the default null address as the setting for the IPX-Net-Number parameter. The null address causes the TAOS unit to learn its network number from another router on the interface, or from the RIP packets received from the local IPX server.

If you enter an IPX network number other than zero, the TAOS unit becomes a seed router, and other routers can learn their IPX network number from the unit. For details about seed routers, see the Novell documentation.

Propagating IPX Type-20 packets on a LAN interface

Some applications, such as NetBIOS over IPX, use IPX Type-20 packets to broadcast names over a network. By default, the broadcasts are not propagated over routed links (although Novell recommends that they be) and are not forwarded over links that have less than 1 Mbps throughput. If you are using an application (such as NetBIOS over IPX) that requires these packets in order to operate, you can enable the router to propagate IPX Type-20 packets over a LAN interface by setting the IPX-Type-20 parameter to Yes.

Example of an IPX-Interface configuration

Following is an example of input that enables the TAOS unit to route 802.3 IPX frames to and from the LAN interface and to propagate IPX Type-20 packets:

```
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
```

Note that this example does not specify an IPX-Net-Number value, which means the TAOS unit is a nonseed router that will learn its address from another IPX router on the network or from the RIP packets received from the local IPX server.

Configuring WAN IPX interfaces

IPX routing connections typically use PPP authentication (described in “Authenticating framed protocol sessions” on page A-6), because the TAOS unit does not have a built-in authentication mechanism, such as matching IPX addresses to a profile. In addition, the IPX-Answer profile must enable IPX routing, which is the default setting.

Overview of IPX connection settings

You can configure IPX connections in local Connection profiles or in RADIUS user profiles.

Settings in Connection profiles

IPX routing connections can specify settings for one or more of the following IPX options (shown with their default values):

```
[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
```

Parameter	**Specifies**
IPX-Routing-Enabled	Enable/disable IPX routing on the interface.
Peer-Mode	Type of far-end device (dial-in NetWare client or IPX router). Valid values are Router-Peer and Dialin-Peer. With the Dialin-Peer setting, the TAOS unit assigns an IPX network number on the virtual IPX network, as described in “Defining a virtual IPX network for dial-in clients” on page 7-4.
RIP	If Peer-Mode is set to Router, enable/disable IPX RIP updates on the interface. Does not apply if Peer-Mode is set to Dialin-Peer.
SAP	If Peer-Mode is set to Router, enable/disable IPX SAP updates on the interface. Does not apply if Peer-Mode is set to Dialin-Peer.
Dial-Query	Enable/disable initiation of a connection upon receipt of a SAP query for service type 0x04 (File Server) when that service type is not present in the SAP table.
Net-Number	Four-byte hexadecimal IPX network number for the link to the client. Required only if the far-end device must negotiate the number before connecting.

Parameter	Specifies
Net-Alias	Second IPX network number, to be used only when connecting to routers that use numbered interfaces and do not run TAOS software.
SAP-Filter	Name of an IPX-SAP Filter profile, to be applied to the LAN interface. For details, see “Example of applying a SAP filter to a WAN interface” on page 7-18.
IPX-SAP-HS-Proxy	Enable/disable IPX Home Server Proxy.
IPX-SAP-HS-Proxy-Net	IPX network numbers for up to six Home Servers, for use when Home Server Proxy is enabled.
IPX-Header-Compression	Enable/disable IPX header compression, provided that the encapsulation method supports it.

Settings in RADIUS profiles

RADIUS user profiles use the following attribute-value pairs to configure IPX routing:

Attribute	Specifies
Ascend-Route-IPX (229)	Enable/disable IPX routing on the interface. Valid values are Route-IPX-No (0) and Route-IPX-Yes (1). Route-IPX-No is the default.
Ascend-IPX-Peer-Mode (216)	Type of far-end device (dial-in NetWare client or IPX router). Valid values are IPX-Peer-Router (0) and IPX-Peer-Dialin (1). If IPX Peer-Dialin is specified, the TAOS units assigns an IPX network number on the virtual IPX network, as described in “Defining a virtual IPX network for dial-in clients” on page 7-4.
Framed-IPX-Network (23)	Four-byte hexadecimal IPX network number of the IPX router at the remote end of the connection. This address is used in Access-Accept packets.
Ascend-IPX-Alias (224)	Second IPX network number, to be used only when connecting to routers that use numbered interfaces and do not run TAOS software.

Specifying whether the remote device is a router or dial-in client

The Peer-Mode parameter and the Ascend-IPX-Peer-Mode RADIUS attribute specify whether the remote site is a dial-in NetWare client or another IPX router. To set a default Peer-Mode value for RADIUS profiles, see “Answer-Defaults IPX Peer-Mode setting” on page 7-9.

When Peer-Mode specifies Dialin-Peer, the TAOS unit negotiates an IPX routing session with the dial-in NetWare client by assigning the client a node address on the virtual IPX network defined in the IPX-Global profile. The client must accept the network number that is assigned. If the client has its own node number, the TAOS unit uses that number to form the full network address. If it does not have a node number, the unit assigns it a unique node address on the virtual network.

Note: When connecting to a dial-in Netware client, the TAOS unit does not send RIP and SAP advertisements across the connection, and it ignores RIP and SAP advertisements received from the far end. However, it does respond to RIP and SAP queries received from dial-in clients.

Answer-Defaults IPX Peer-Mode setting

TAOS units support the following parameter (shown with its default value) for setting a default IPX peer mode for RADIUS profiles:

```
[in ANSWER-DEFAULTS:ipx-answer]
peer-mode = router-peer
```

When Use-Answer-For-All-Defaults is set to Yes (the default), the system uses the IPX-Answer Peer-Mode setting when creating a baseline profile for RADIUS-authenticated calls.

Controlling RIP and SAP updates to and from a remote router

When the remote end of the connection is a router, you can specify how to handle RIP and SAP packets across this WAN connection. Both the RIP and the SAP parameters are set to Both by default, which means that the TAOS unit both sends updates across the WAN connection (informing other routers on the remote network of its routes or services) and receives updates from the remote router (including those routes or services in its RIP or SAP table).

If you set the RIP parameter to Send, the TAOS unit sends its routes to the remote router, but does not receive any updates on this interface. If you set the parameter to Recv, the unit receives updates from the remote router but does not propagate the local IPX routes to the remote site. If you set RIP to Off, no routes are propagated in either direction.

The same settings apply to the SAP parameter. If SAP is set to both send and receive broadcasts on the WAN interface, the TAOS unit broadcasts its entire SAP table to the remote network and listens for SAP table updates from that network. Eventually, both networks have a full table of all services on the WAN. To control which services are advertised and where, you can either disable the exchange of SAP broadcasts across a WAN connection or specify that the TAOS unit will only send or only receive SAP broadcasts on that connection.

Using Dial-Query

Setting the Dial-Query parameter configures the TAOS unit to bring up a connection when it receives a SAP query for service type 0x04 (File Server) and that service type is not present in the TAOS unit’s SAP table. If the unit has no SAP table entry for service type 0x04, it brings up every connection that has Dial-Query set. For example, if 20 Connection profiles have Dial-Query set, the TAOS unit brings up all 20 connections in response to the query.

If the TAOS unit has a static IPX route for even one remote server, it brings up that connection instead of choosing the more costly solution of bringing up every connection that has Dial-Query set.

When to use Net-Number and Net-Alias

Net-Number specifies the IPX network number of the remote-end router. This parameter, which is rarely needed, accommodates those remote-end routers that require the TAOS unit to know the router's network number before connecting.

The Net-Alias parameter specifies a second IPX network number, to be used only when connecting to routers that use numbered interfaces and do not run TAOS software.

Home-server proxy

For mobile NetWare clients, you can specify the network number of from one to six NetWare servers that should receive SAP queries across the connection. If you do not, when the client is at a distant location and sends a Get Nearest Server Request query, the responses come from servers closer to that location, rather than from the expected home server or servers. With the home-server proxy feature, mobile clients can bring up a connection to the server or servers they usually use.

To enable home-server proxy, set the IPX-SAP-HS-Proxy parameter to Yes, and specify from one to six IPX network numbers for the IPX-SAP-HS-Proxy-Net parameter. The TAOS unit then directs the client's SAP queries only to the specified networks.

Following is an example of how to enable the home-server proxy feature in an IPX-routing Connection profile:

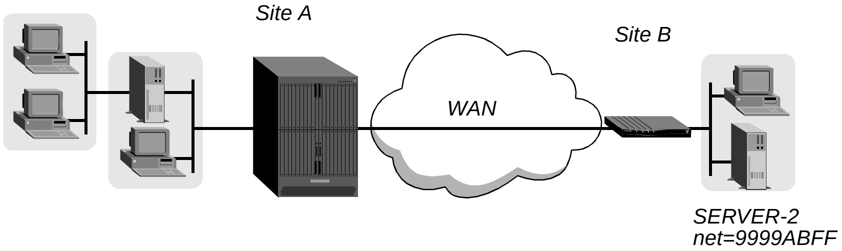
```
admin> read conn ipxclient
CONNECTION/ipxclient read

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
```

Setting IPX-SAP-HS-Proxy to Yes enables the feature. You must then specify at least one (and up to six) IPX network addresses to which SAP broadcasts will be directed.

Examples of a connection to a Novell LAN

Figure 7-1 shows a TAOS unit providing a connection between an IPX network, which supports NetWare servers and clients, and a remote site that supports a TAOS unit as well as NetWare servers and clients.

Figure 7-1. IPX connection with NetWare servers on both sides



In this example, the NetWare server at Site B is configured with the following specifications:

```
Name = SERVER-2
internal net 013DE888
Load 3c509 name = net-card frame = ETHERNET_8023
Bind ipx net-card net = 9999ABFF
```

Following is an example of specifying a connection to the TAOS unit at Site 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
```

Following is a comparable RADIUS profile:

```
sitebgw Password = "sitebpw"
   Service-Type = Framed-User,
   Framed-Protocol = MPP,
   Ascend-Route-IPX = Route-IPX-Yes,
   Ascend-IPX-Peer-Mode = IPX-Peer-Router
```

When RIP is turned off on a connection, you might want to create a static route to the server at the remote site. The route ensures that the TAOS unit can bring up this connection, even immediately following a system reset. The following example shows how to configure a route to Server-2 at Site 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
```

Following is a comparable RADIUS profile:

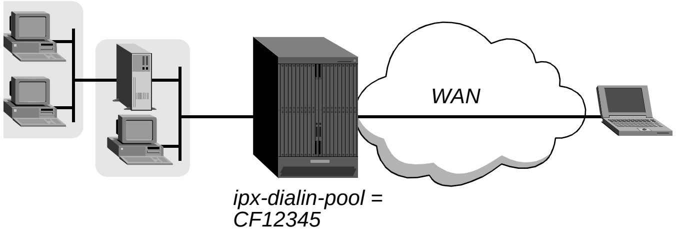
```
ipxroute-sa-1 Password = "ascend", Service-Type = Outbound-User
   Ascend-IPX-Route="sitebgw 013DE888 000000000001 0451 0004 SERVER-2"
```

Note: The destination network number is the server’s internal network number. For more information about IPX routes, see “Configuring static IPX routes” on page 7-12.

Examples of a connection to a dial-in client

Figure 7-2 shows a NetWare client dialing in to the TAOS unit to reach a corporate IPX network. The caller is running NetWare client software with PPP software for dialing in.

Figure 7-2. Dial-in NetWare client



Dial-in NetWare clients do not have an IPX network address. To establish an IPX routing connection to the local network, the clients must dial in with PPP software, and the Connection profile must have Peer-Mode set to Dialin-Peer. In addition, the TAOS unit must have a virtual IPX network defined for assignment to these clients. For information about defining a virtual IPX network, see "Configuring the IPX-Global profile" on page 7-4.

Following is an example of input that configures an IPX routing connection for the client shown in Figure 7-2:

```
admin> new conn client-1
CONNECTION/client-1 read

admin> set ppp recv-password = client-pw

admin> set ipx ipx-routing = yes

admin> set ipx peer = dialin

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

Following is a comparable RADIUS profile:

```
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
```

Configuring static IPX routes

When the TAOS unit resets or power cycles, it clears RIP and SAP tables from memory. Static routes create entries in new RIP and SAP tables as the unit initializes. The static routes enable the TAOS unit to reach a NetWare server and download more complete tables from there.

In the case where a TAOS unit is connecting to another TAOS unit, you might choose not to configure any static routes. However, that means that after a power-cycle or reset, you must dial the initial IPX routing connection manually. After that connection is established, the TAOS unit downloads the RIP table from the other TAOS unit and maintains the routes as static until its next power-cycle or reset.

The disadvantage of static routes is that they require manual updating whenever the specified server is removed or has a change in its address. One advantage is that they ensure that the TAOS unit can bring up the connection in response to clients' SAP requests. Another advantage is that they help to prevent time-outs when a client takes a long time to locate a server on the WAN.

Note: You do not need to create IPX routes to servers that are on the local Ethernet network.

Overview of IPX route settings

You can configure IPX routes in local IPX-Route profiles or in RADIUS pseudo-user profiles.

Settings in local IPX-Route profiles

Static IPX routes are configured with the following parameters (shown with their default settings):

```
[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
```

Parameter	**Specifies**
Name	Name of the IPX-Route profile, typically the name of the remote NetWare server.
Server-Type	NetWare service type. The service type is a number included in SAP advertisements. For example, NetWare file servers are SAP service type 0x04.
Dest-Network	Internal network number of a remote NetWare server. NetWare file servers are assigned an internal IPX network number by the network administrator and usually use the default of 000000000001 as a node number on that network. The combined network and node address is the destination network address for file read/write requests. (If you are not familiar with internal network numbers, see your NetWare documentation for details.)
Server-Node	Server's node address on the internal network. Servers typically use the default node address of 000000000001 on the internal network.
Server-Socket	Well-known socket number in the server. For details, see "Socket numbers in static routes" on page 7-15.
Hops	Hops to the server's internal network. Usually, the default hop count of 2 is appropriate, but you might need to increase the value for very distant servers.

Parameter	Specifies
Ticks	Ticks are IBM PC clock ticks (1/18 second). Best routes are calculated on the basis of tick count, not hop count. Usually, the default tick count of 12 is appropriate, but you might need to increase the value for very distant servers.
Profile-Name	Name of the Connection or RADIUS dial-out profile used to reach the server. The default value is null. When the TAOS unit receives a query for the specified server or a packet addressed to that server, it finds the referenced profile and dials the connection.
Active-Route	Enable/disable the route. A disabled route is not used.

Settings in RADIUS ipxroute profiles

An `ipxroute` profile is a pseudo-user profile in which the first line has the following format:

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

The *name* argument is the TAOS unit system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the TAOS unit stops retrieving the profiles when it encounters the gap.

Note: To specify routes that can be dialed out by more than one system, eliminate the *name* argument. The first word of the pseudo-user profile is then `route-N.`

Each pseudo-user profile specifies one or more routes with the Ascend-IPX-Route attribute. The value of the Ascend-IPX-Route attribute uses the following syntax:

```
"profile net [node] [socket] [server-type] [hops] [ticks] [server-
name]"
```

Syntax element	Specifies
profile	Name of the dial-out user profile that uses the route. When the TAOS unit receives a query for the specified server or a packet addressed to that server, it finds the referenced profile and dials the connection.
net	Internal network number of a remote NetWare server. NetWare file servers are assigned an internal IPX network number by the network administrator and usually use the default of 000000000001 as a node number on that network. The combined network and node address is the destination network address for file read/write requests. (If you are not familiar with internal network numbers, see your NetWare documentation for details.)
node	Server’s node address on the internal network. Servers typically use the default node address of 000000000001 on the internal network.
socket	Well-known socket number in the server. For details, see “Socket numbers in static routes” on page 7-15.
server-type	NetWare service type. The service type is a number included in SAP advertisements. For example, NetWare file servers are SAP service type 0x04.

Syntax element	Specifies
hops	Hops to the server's internal network. Usually, the default hop count of 2 is appropriate, but you might need to increase the value for very distant servers.
ticks	Ticks are IBM PC clock ticks (1/18 second). Best routes are calculated on the basis of tick count, not hop count. Usually, the default tick count of 12 is appropriate, but you might need to increase the value for very distant servers.
server-name	Name of the remote NetWare server.

Socket numbers in static routes

The socket number you specify must be a well-known socket number. For example, Novell file servers typically use socket 0x451.

Services that use dynamic socket numbers might use a different socket each time they load, and they will not work with IPX Route profiles. To bring up a connection to a remote service that uses a dynamic socket number, specify a master server with a well-known socket number on the remote network.

Examples of a static IPX route

The following example shows how to create a new IPX-Route profile for a remote server named 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
```

Following is a comparable RADIUS profile:

```
ipxroute-sa-1 Password = "ascend", Service-Type = Outbound-User
   Ascend-IPX-Route="sitebgw cc1234ff 000000000001 0451 0004 Server-1"
```

Defining and applying IPX SAP filters

IPX SAP filters contain specifications that determine which remote NetWare services will be excluded from or included in the TAOS unit's SAP table or SAP response packets.

Note: SAP filters work only when IPX SAP is enabled on the interface (as it is by default). You can prevent the TAOS unit from sending or receiving any SAP udpates on a WAN interface by setting SAP to No in the IPX-Options subprofile of a Connection profile.

Overview of IPX SAP filter settings

Following are the SAP filter parameters (shown with their default values):

```
[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 = ""
```

Each of the eight input and output filters include the same parameters.

Parameter	Specifies
IPX-SAP-Filter-Name	Name of the SAP filter. You must assign a name so that the filter can be applied by name to an interface. The name you assign becomes the IPX-SAP-Filter profile’s index.
Input-IPX-SAP-Filters (1–8)	Subprofile containing up to eight input-filter specifications that make up the SAP filter. Specifications are defined individually and applied in order (1–8) to SAP packets the TAOS unit receives. Input filters determine which remote services are accessible to local NetWare users.
Output-IPX-SAP-Filters (1–8)	Subprofile containing up to eight output-filter specifications that make up the SAP filter. Specifications are defined individually and applied in order (1–8) to SAP response packets. The TAOS unit transmits SAP responses in reply to a SAP request packet. Output filters determine which local NetWare services are available to remote users.
Valid-Filter	Enable/disable the input or output filter. A setting of No (the default), causes the system to skip that filter when filtering the SAP data. Set this parameter to Yes for each defined filter you intend to use.
Type-Filter	Inclusion or exclusion of the service specified by the Server-Name or the Server-Type parameter (or both). Exclude is the default. The Include setting is typically used to include a specific service when previous filters have excluded a general type of service.
Server-Type	NetWare service type. Service types are hexadecimal numbers representing a type of NetWare service. Type FFFF represents all types. The number for File Service is 0004. For complete information about SAP service types, see your NetWare documentation.

Parameter	Specifies
Server-Name	Name of a local or remote NetWare server. You can use the wildcard characters asterisk (*) and question mark (?) for partial name matches.

Example of filtering a file server from the SAP table

The following example shows how to create a SAP filter that identifies a particular file server and filters it from the SAP table. If the directory services feature is not supported, servers or services that are not in the TAOS unit's SAP table will be inaccessible to clients on other TAOS unit's interfaces.

```
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
```

Example of filtering remote NetWare services from the SAP table

The following example shows how to create a SAP filter that excludes all NetWare services on the interface from the TAOS unit's SAP table. When this filter is applied in a Connection profile, WAN users *can* access local services, but local users cannot access any services on the remote network.

```
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
```

Example of applying a SAP filter to a LAN interface

When applied to a LAN interface, a SAP filter includes or excludes specific local services from the TAOS unit's SAP table and the unit's responses to SAP queries on the interface. If the directory services feature is not supported, servers or services that are not in the TAOS unit's SAP table will be inaccessible to clients across the WAN. A filter applied to a LAN interface takes effect immediately.

Following is an example of applying a SAP filter to a LAN interface:

```
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
```

Example of applying a SAP filter to a WAN interface

You can apply a SAP filter to a WAN interface by specifying the filter profile name as the value of the SAP-Filter parameter. When applied to a WAN interface, a SAP filter includes or excludes specific services from the TAOS unit’s SAP table and the unit’s responses to SAP queries on the interface. A filter applied to a WAN interface takes effect when the connection next becomes active.

Following is an example of applying a SAP filter to a WAN interface:

```
admin> read conn clientnet
CONNECTION/clientnet read

admin> set ipx sap-filter = nowan

admin> write
CONNECTION/client written
```

AppleTalk Routing and Remote Access

8

A TAOS unit configured for AppleTalk routing enables dial-in connections from AppleTalk Remote Access (ARA) Client software, from PPP dial-in software that supports AppleTalk, and from other AppleTalk-enabled TAOS units.

Note: AppleTalk routing must be enabled on the shelf controller to enable the system to forward AppleTalk packets from the card on which the packet is received to the shelf controller. This requirement applies to any kind of AppleTalk connection, even if the individual Connection profile for a remote device does not use routing.

Configuring the Atalk-Global profile

When an ARA or AppleTalk PPP client dials in, the TAOS unit assigns the client an AppleTalk address on a virtual AppleTalk network. You define the virtual AppleTalk network in the Atalk-Global profile by setting the following parameters (shown with sample settings):

```
[in ATALK-GLOBAL]
atalk-dialin-pool-start = 1000
atalk-dialin-pool-end = 1002
```

AppleTalk networks are assigned a network range, which is a contiguous range of integers from 1 to 65,199. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap.

Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in. For example, a network with the range 1001-1002 could support up to 2 x 253, or 506, clients. Following is an example of defining a virtual network. In this case, the network range is 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
```

Configuring LAN AppleTalk interfaces

In the Atalk-Interface profile, you enable AppleTalk routing and specify whether the TAOS unit operates as a seed or nonseed router on the interface. In the current software version, only the built-in Ethernet interface on the shelf controller can be configured as an AppleTalk interface. The Atalk-Interface profile contains the following parameters (shown with default settings):

```
[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 = [ "" "" "" "" "" "" "" "" "" "" ]
```

Parameter	**Specifies**
Atalk-Routing-Enabled	Enable/disable AppleTalk routing on the shelf-controller Ethernet interface. If this parameter is set to No, none of the other parameters applies.
Hint-Zone	Name of the zone in which the TAOS unit resides. Applies only when the TAOS unit is a nonseed router.
Atalk-Router	Routing mode. If this parameter is set to Atlk-Router-Off, none of the remaining parameters applies. With the Atlk-Router-Seed setting, the unit comes up with the specified zone and network configuration, which must be completely consistent with the corresponding specifications in other AppleTalk routers on the interface. With the Atlk-Router-Nonseed setting, the unit learns its zone and network configuration from another AppleTalk router (a seed router) on the network.
Atalk-Net-Start Atalk-Net-End	Network range for the interface. Applies only for a seed router configuration. (For details, see “Example of configuring a seed router” on page 8-2.)
Default-Zone	Default AppleTalk zone for the interface. Applies only for a seed router configuration. The default zone is the zone assigned to an AppleTalk service on this interface if the service does not select a zone in which to reside.
Zone-List	Zone list for the interface. Applies only for a seed router configuration.

Example of configuring a seed router

A seed router has its own hard-coded network and zone configuration. Other routers can learn their configuration from a seed router. To configure the TAOS unit as a seed router, you must configure a network range and zone list and specify that the unit is a seed router.

The network range is a contiguous range of integers from 1 to 65,199. Each range must be unique. No two interfaces can use the same range, and no two network ranges can overlap.

Each number in the range can be associated with up to 253 nodes, so the range determines how many clients the interface can support. For example, an interface with the range 1006-1010 could support up to 5 x 253, or 1265, clients.

The zone list is a list of 1 to 32 AppleTalk zone names. Each name consists of from 1 to 33 characters, including embedded spaces. The characters must be in the standard printing character set, and must not include an asterisk (*).

The following commands configure a seed router with the network range 1006–1010, three zones, and the default zone for the LAN interface:

```
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
```

Configuring a nonseed router

A nonseed router acquires its network and zone configuration from another router on the network. If the TAOS unit is configured in nonseed mode, a seed router must be available at start-up time, or the TAOS unit cannot come up in AppleTalk routing mode. (If the TAOS unit comes up without AppleTalk routing enabled because no seed routers were available at start-up, you must reset the system after a seed router becomes available.)

When the system resets, it sends out a ZipGetNetInfo request packet to obtain its configuration from a seed router. If you specify the name of the AppleTalk zone in which the TAOS unit resides (the recommended procedure), the system can include the specified zone name in the ZipGetNetInfo packet, and the router can return a valid network range for that zone.

The following commands configure the TAOS unit as a nonseed router:

```
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
```

Configuring WAN AppleTalk interfaces

PPP and ARA are the encapsulation protocols used for AppleTalk dial-in on the TAOS unit. AppleTalk PPP and ARA Client software are available from Apple Computer (both ARA and PPP are supported in ARA 3.0) and from other vendors such as Netmanage Pacer PPP. Both AppleTalk PPP and ARA can be used over a modem or V.120 ISDN TA connection. AppleTalk PPP can also be used over a synchronous PPP connection when the calling unit is a Pipeline or MAX unit.

Note: AppleTalk routing must be enabled in a Connection profile for incoming PPP connections, but it is not necessary for ARA client connections.

You can configure a connection for AppleTalk connectivity in the following ways:

- ARA client connection
- PPP dial-in connection (AppleTalk PPP)
- Synchronous PPP connection with a Pipeline or MAX unit (AppleTalk routing)
- DDP-IP gateway (IP over AppleTalk)

Settings in the Answer-Defaults profile

To enable ARA client connections, you must enable ARA-Answer in the Answer-Defaults profile. In addition, if you intend to allow ARA Guest access, set the Profiles-Required parameter to No (it is typically set to Yes for security purposes). Following are the relevant parameters:

```
[in ANSWER-DEFAULTS]
profiles-required = no

[in ANSWER-DEFAULTS:ara-answer]
enabled = yes
```

Following is an example of input that enables ARA-Answer and disables ARA Guest access:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ara-answer enabled = yes

admin> set profiles-required = yes

admin> write
ANSWER-DEFAULTS written
```

Setting Profiles-Required to Yes disables ARA Guest access.

Settings in a Connection profile

You configure ARA or AppleTalk PPP connections by using the following parameters (shown with sample settings):

```
[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
```

Parameter	Specifies
Encapsulation-Protocol	Encapsulation method. For ARA connections, specify ARA.
Recv-Password	Password expected from the dial-in client.
ARA-Enabled	Enable/disable ARA processing for the connection.
Maximum-Connect-Time	Maximum number of minutes an ARA session can remain connected. The default setting, 0 (zero), disables the timer. If you specify a maximum connect time, the TAOS unit initiates an ARA disconnect when that time is up. The ARA link disconnects gracefully, but remote users are not notified. Users will find out the ARA link is gone only when they try to access a device.
Atalk-Routing-Enabled	Enable/disable AppleTalk routing for the connection. If AppleTalk routing has not been enabled in the Atalk-Interface profile, or if the Answer-Defaults profile does not enable ARA-Answer, this parameter has no effect.
Atalk-Static-Zonename	Zone name the TAOS unit uses when routing packets to a remote site for a dial-out AppleTalk connection. Note that currently only dial-in AppleTalk is supported.
Atalk-Static-Netstart Atalk-Static-Netend	Network range for packets that the TAOS unit routes to a remote site for a dial-out AppleTalk connection. Note that currently only dial-in AppleTalk is supported.
Atalk-Peer-Mode	Type of dial-in client (router or dial-in peer). With the Dialin-Peer setting, the TAOS unit negotiates a routing session with the dial-in client by assigning the client a node address on the virtual AppleTalk network defined in the Atalk-Global profile. The client must accept the network number assigned.

Settings in a RADIUS profile

RADIUS uses the following attribute-value pairs to configure ARA and AppleTalk routing connections:

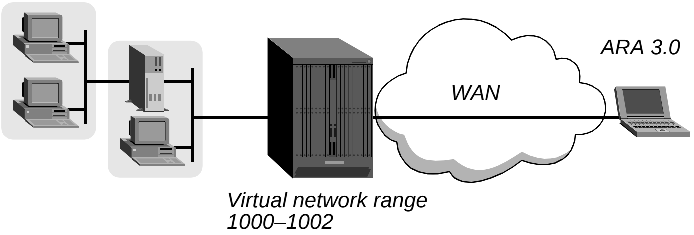
Attribute	Value
Framed-Protocol (7)	Encapsulation method. For ARA connections, specify ARA (255).
Ascend-Send-Secret (214)	Password sent to the server by the dial-in client.
Ascend-Route-Appletalk (118)	Enable/disable AppleTalk routing for the connection. Valid values are Route-Appletalk-No (0) and Route-Appletalk-Yes (1).

Attribute	Value
Ascend-Appletalk-Peer-Mode (117)	Type of dial-in client. Valid values are Appletalk-Peer-Router (0) and Appletalk-Peer-Dialin (1). With a setting of Appletalk-Peer-Dialin, the TAOS unit negotiates a routing session with the dial-in client by assigning the client a node address on the virtual AppleTalk network defined in the Atalk-Global profile. The client must accept the network number assigned.

Examples of configuring an ARA client connection

An ARA client connection uses the ARA encapsulation protocol and does not require AppleTalk routing. In Figure 8-1, the dial-in client is running ARA 3.0, with ARA encapsulation selected and with an internal modem. In this example, the client will be assigned a network address on the virtual 1000–1002 network and a maximum ARA connection time of 60 minutes.

Figure 8-1. ARA Client dial-in



The following commands configure a Connection profile for the ARA client:

```
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
```

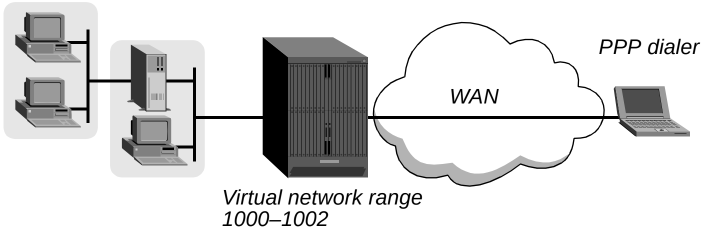
Following is a comparable RADIUS profile:

```
araclient Password = "ara-password"
    Service-Type = Framed-User,
    Framed-Protocol = ARA,
    Ascend-Send-Secret = "ara-password"
```

Examples of configuring a PPP AppleTalk dial-in

An AppleTalk PPP dial-in client connection uses the PPP encapsulation protocol. In Figure 8-2, the dial-in client is running ARA 3.0, and has selected either PPP encapsulation or is using another PPP dialer that supports AppleTalk. The client will be assigned a network address on the virtual 1000-1002 network.

Figure 8-2. AppleTalk connection using a PPP dialer



The following commands configure a Connection profile for the PPP client:

```
admin> new connection ppp-atalk
CONNECTION/ppp-atalk read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp recv-password = localpw

admin> set appletalk atalk-routing-enabled = yes

admin> set appletalk atalk-peer-mode = dialin

admin> write
CONNECTION/ppp-atalk written
```

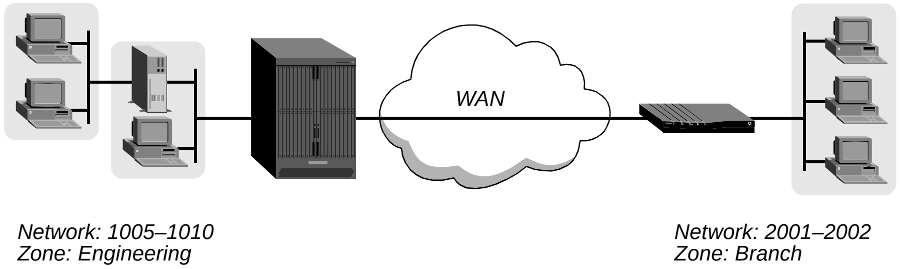
Following is a comparable RADIUS profile:

```
ppp-atalk Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Route-Appletalk = Route-Appletalk-Yes,
    Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Dialin
```

Examples of configuring a connection to an AppleTalk router

An AppleTalk routing connection uses the PPP encapsulation protocol or one of its multilink variants (MP or MP+). In Figure 8-3, the remote Pipeline unit is configured as an AppleTalk router that is on the extended AppleTalk network 2000-2001 and in the Branch zone.

Figure 8-3. AppleTalk routing connection



The following commands configure a connection to the remote router:

```
admin> read connection atalk-router
CONNECTION/atalk-router read

admin> set active = yes

admin> set encaps = ppp

admin> set ppp recv-password = rtr-password

admin> set appletalk atalk-routing enabled = yes

admin> set appletalk atalk-peer-mode = router-peer

admin> write
CONNECTION/atalk-router written
```

Following is a comparable RADIUS profile:

```
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
```

Examples of an IP-over-AppleTalk connection

To route IP and AppleTalk, the TAOS unit must be configured both as an IP router and an AppleTalk router. For details about configuring the IP router and individual IP connections, see Chapter 2, “IP Routing.” To support IP, the Connection profile for a dial-in client must specify an IP configuration, and the client must configure Macintosh TCP/IP software (such as Open Transport). Table 8-1 describes Macintosh TCP/IP configurations for a PPP connection.

Table 8-1. Macintosh TCP/IP settings for PPP connections

Macintosh software	IP settings for a PPP AppleTalk connection
Open Transport	The TCP/IP Control Panel must specify a PPP connection and the client IP address. If the Connection profile has a hard-coded IP address, type that address manually in the Control Panel. If the Connection profile specifies dynamic address assignment, set the Control Panel to obtain an address from the PPP server.
MacTCP	The MacTCP Control Panel should select the PPP icon and the client IP address. If the Connection profile has a hard-coded IP address, type that address manually in the Control Panel. If the Connection profile specifies dynamic assignment of an address, set the Control Panel to obtain an address from a server. (The Dynamic option in MacTCP is not supported.)

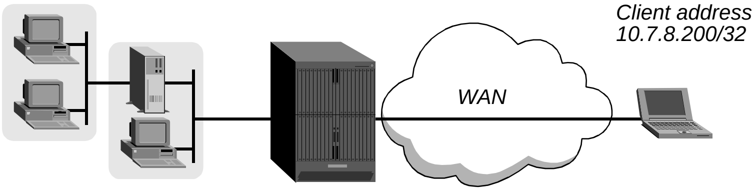
When ARA encapsulation is in use, the TAOS unit handles IP packets by encapsulating them in DDP. Table 8-2 describes Macintosh TCP/IP configurations for an ARA connection.

Table 8-2. Macintosh TCP/IP settings for ARA connections

Macintosh software	IP settings for an ARA connection
Open Transport	The TCP/IP Control Panel must specify a connection via Mac-IP and the client IP address. If the Connection profile has a hard-coded IP address, type that address manually in the Control Panel. If the Connection profile specifies dynamic assignment of an address, set the Control Panel to obtain an address from the Mac-IP server.
MacTCP	The MacTCP Control Panel should select the ARA icon and the client IP address. If the Connection profile has a hard-coded IP address, type that address manually in the Control Panel. If the Connection profile specifies dynamic assignment of an address, set the Control Panel to obtain an address from a server. (The Dynamic option in MacTCP is not supported.)

In Figure 8-4, the dial-in client is running ARA 3.0 (which includes DDP-IP tunneling capabilities) and an IP application such as Telnet to communicate with an IP host on the TAOS unit's local interface. The client has a hard-coded IP address.

Figure 8-4. ARA connection that encapsulates IP packets in DDP



The following commands configure a profile that enables the client to use ARA client 3.0 to dial in and then initiate a Telnet connection to a host on the TAOS unit's IP network:

```
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
```

Following is a comparable RADIUS profile:

```
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
```

Packet Filters

9

Filter overview

A filter consists of specifications describing packets and actions to take upon packets that match the descriptions. After you apply a filter to an interface, the TAOS unit monitors the data stream on that interface.

Depending on how you define a filter, it can apply to inbound packets, outbound packets, or both. In addition, filters are flexible enough to specify taking an action (such as forward or drop) on those packets that match the specifications, or on all packets *except* those that match the specifications.

Basic types of filters

Each Filter profile contains up to 12 input filters (applied to inbound packets) and 12 output filters (applied to outbound packets). Each of the up to 24 specifications can be one of the following basic types of filters:

- Generic filters
- IP filters
- Type-of-service filters
- IPX filters (local Filter profiles only)
- Route filters (local Filter profiles only)

Generic filters examine the byte- or bit-level contents of any packet, comparing specified bytes or bits with a value defined in the filter. On the basis of this comparison, the filter specifies a forwarding action. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information.

IP filters apply only to IP-related packets. They specify a forwarding action on the basis of higher-level fields in IP packets (for example, the source or destination address, or the protocol number). They operate on logical information, which is relatively easy to obtain.

Type-of-Service (TOS) filters set priority bits in the TOS header of IP packets. Other routers can then use the information to prioritize and select links for particular data streams.

IPX filters apply only to NetWare packets. They specify a forwarding action on the basis of higher-level fields, such as source or destination network, node, and socket numbers. Like IP filters, IPX filters operate on logical information, which is relatively easy to obtain.

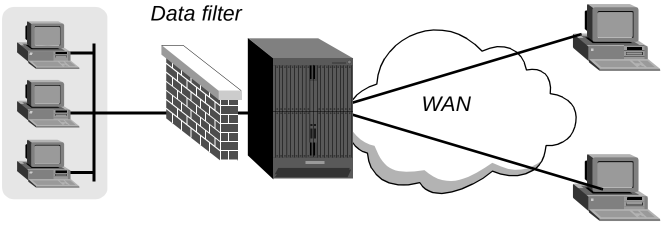
Route filters apply only to RIP update packets. They specify whether matching routes in a RIP packet will be accepted into the routing table, denied, or accepted with an increased metric. Route filters can also specify a source address, which means that they can take an action on all updates from that address.

Data and call filters

Data filters are commonly used for security, but they can apply to any purpose that requires the TAOS unit to drop or forward specific packets. The focus is typically on keeping out traffic that you do not want on a LAN. For example, you can use data filters to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. You can also use data filters to allow users to access only specific devices across the WAN.

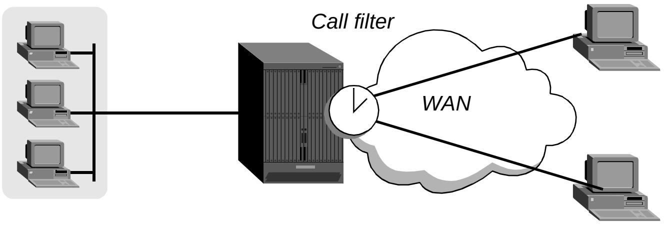
When you apply a data filter (Figure 9-1), its forwarding action (forward or drop) affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa. Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process.

Figure 9-1. Data filters drop or forward certain packets



Call filters (Figure 9-2) prevent unnecessary connections and help the TAOS unit distinguish active traffic from “noise.” By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection’s idle timer.

Figure 9-2. Call filters prevent certain packets from resetting the timer



When you apply a call filter, its forwarding action (forward or drop) does *not* affect which packets are sent across an active connection. The forwarding action of a call filter determines which packets can either initiate a connection or reset a session's timer. When a session's idle timer expires, the session is terminated. With the default Idle-Timer setting of 120 seconds, the TAOS unit terminates a connection that has been inactive for two minutes.

How filters work

A Filter profile can include up to 12 input-filter and 12 output-filter specifications (filters). Each filter has its own forwarding action—forward or drop. The filters are applied in sequence. At the first successful comparison between a filter and the packet being examined, the filtering process stops and the forwarding action in that filter is applied to the packet. For route filters, the forwarding action has no effect, but another type of action in the filter is applied to the packet when a comparison succeeds.

If no comparison succeeds, the packet does not match the filter. However, this does not mean that the packet is forwarded. When no filter is in use, the TAOS unit forwards all packets, but applying a filter to an interface reverses this default. For security purposes, the unit does not automatically forward nonmatching packets. It requires a filter that explicitly allows such packets to pass. (For a sample input filter that forwards packets that did not match a previous filter, see "Examples of an IP filter to prevent local address spoofing" on page 9-15.)

Note: For a call filter to prevent an interface from remaining active unnecessarily, you must define filters for both input and output packets. Otherwise, if only input filters are defined, output packets will keep a connection active, or vice versa.

Generic filters

In a generic filter, all of the settings in a filter specification work together to specify a location in a packet and a number to be compared to that location. The type of comparison that constitutes a match (equal or not-equal) must also be specified. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet.

If a generic filter is applied as a call filter and a comparison succeeds, the forwarding action is either to reset the idle timer or not, depending on how the filter is defined. If a generic filter is applied as a data filter, the forwarding action is either to forward the packet or drop it.

IP filters

In an IP filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet. The IP filter tests proceed in the following order:

1. Apply the Source-Address-Mask value to the Source-Address value and compare the result to the source address of the packet. If they are not equal, the comparison fails.
2. Apply the Dest-Address-Mask value to the Dest-Address value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.
3. If the Protocol parameter is zero (which matches any protocol), the comparison succeeds. If it is nonzero and not equal to the protocol field in the packet, the comparison fails.
4. If the Src-Port-Cmp parameter is not set to None, compare the Source-Port number to the source port number of the packet. If they do not match as specified by the Src-Port-Cmp parameter, the comparison fails.
5. If the Dst-Port-Cmp parameter is not set to None, compare the Dest-Port number to the destination port number of the packet. If they do not match as specified by the Dst-Port-Cmp parameter, the comparison fails.
6. If TCP-Estab is set to Yes and the protocol number is 6, the comparison succeeds.

If an IP filter is applied as a call filter and a comparison succeeds, the forwarding action is either to reset the idle timer or not, depending on how the filter is defined. If an IP filter is applied as a data filter, the forwarding action is either to forward the packet or drop it.

Type of service (TOS) filters

In an IP TOS filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the action specified in that filter is applied to the packet. The TOS filter tests proceed in the following order:

1. Apply the Source-Address-Mask value to the Source-Address value and compare the result to the source address of the packet. If they are not equal, the comparison fails.
2. Apply the Dest-Address-Mask value to the Dest-Address value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.
3. If the Protocol parameter is zero (which matches any protocol), the comparison succeeds. If it is nonzero and not equal to the protocol field in the packet, the comparison fails.
4. If the Src-Port-Cmp parameter is not set to None, compare the Source-Port number to the source port number of the packet. If they do not match as specified by the Src-Port-Cmp parameter, the comparison fails.
5. If the Dst-Port-Cmp parameter is not set to None, compare the Dest-Port number to the destination port number of the packet. If they do not match as specified by the Dst-Port-Cmp parameter, the comparison fails.

If a comparison succeeds, the system sets the precedence bits and class of service (depending on how the filter is defined) in the TOS header of the packet.

IPX filters

In an IPX filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet. The IPX filter tests proceed in the following order:

1. Compare the Src-Net-Address number to the source network number of the packet. If they are not equal, the comparison fails.
2. Compare the Dest-Net-Address number to the destination network number in the packet. If they are not equal, the comparison fails.
3. Compare the Src-Node-Address number to the source node number of the packet. If they are not equal, the comparison fails.
4. Compare the Dest-Node-Address number to the destination node number in the packet. If they are not equal, the comparison fails.
5. If the Src-Socket-Cmp parameter is not set to None, compare the Src-Socket number to the source socket number of the packet. If they do not match as specified by the Src-Socket-Cmp parameter, the comparison fails.
6. If the Dst-Socket-Cmp parameter is not set to None, compare the Dest-Socket number to the destination socket number of the packet. If they do not match as specified by the Dst-Socket-Cmp parameter, the comparison fails.

If an IPX filter is applied as a call filter and a comparison succeeds, the forwarding action is either to reset the idle timer or not, depending on how the filter is defined. If an IPX filter is applied as a data filter, the forwarding action is either to forward the packet or drop it.

Route filters

In a Route filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the RIP packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the action specified in that filter is applied to the matching route or packet. The Route filter tests proceed in the following order:

1. Apply the Source-Address-Mask value to the Source-Address value and compare the result to the source address of the packet. If they are not equal, the comparison fails.
2. Apply the Route-Mask value to the Route-Address value and compare the result to the routes in the packet. If there is no match, the comparison fails.

If a comparison succeeds, the system performs one of the following actions, depending on how the filter is defined:

- If Action is set to Add, increase the metric field of the matching routes by the Add-Metric value and then add them to the routing table.
- If Action is set to Accept, add the matching routes to the routing table.
- If Action is set to Deny, reject the matching routes (do not add them to the routing table).

Specifying a filter’s direction

A local Filter profile can define up to 12 input-filter specifications and 12 output-filter specifications. Following are the relevant parameters (shown with their default settings):

```
[in FILTER/"":input-filters:input-filters[1]]
valid-entry = no
```

```
[in FILTER/"":output-filters:output-filters[1]]
valid-entry = no
```

Parameter	Specifies
Input-Filters (1–12)	Each filter can contain up to 12 input-filter specifications, which are defined individually and applied in order (1–12) to the inbound packet stream. The order in which the input filters are defined is significant.
Output-Filters (1–12)	Each filter can contain up to 12 output-filter specifications, which are defined individually and applied in order (1–12) to the outbound packet stream. The order in which the output filters are defined is significant.
Valid-Entry	Enable/disable the filter specification. With a setting of No (the default), the system skips the specification when filtering the data stream. Set this parameter to Yes for each defined filter you intend to use.

In a RADIUS profile, each filter is specified separately by using the Ascend-Data-Filter and Ascend-Call-Filter attributes. As is always the case with filters, the order in which they are applied within the user profile is significant.

In a RADIUS filter definition, you specify the direction in which to monitor the data stream as `in` or `out`. This setting provides the same function as the Input-Filters and Output-Filters parameters in a local profile. The following example shows an input-filter definition in RADIUS:

```
test-user Password = "test-pw"
    Ascend-Data-Filter = "ip in forward tcp dstport > 1023"
```

Specifying a filter’s forwarding action

For generic, IP, or IPX filters, each input or output filter in a local Filter profile specifies a forwarding action for packets that match the filter. Following is the relevant parameter (shown with its default settings):

```
[in FILTER/"":input-filters:input-filters[1]]
forward = no
```

```
[in FILTER/"":output-filters:output-filters[1]]
forward = no
```

Parameter	Specifies
Forward	Forwarding action for the filter. When no filters are in use, the TAOS unit forwards all packets by default. When a filter is in use, the default is to discard matching packets (Forward = No).

Note: For route filters and Type of Service filters, the forwarding action has no effect. Those filters perform a different type of action on matching packets.

In a RADIUS definition, you specify the action a filter takes as `forward` or `drop`. This setting provides the same function as the Forward parameter in a local profile. The following example shows an input filter whose forwarding action is to drop matching packets:

```
test-user Password = "test-pw"
    Ascend-Data-Filter = "ip in drop tcp dstport > 1023"
```

Defining generic filters

Generic filters can match any packet, regardless of its protocol type or header fields. The filter specifications operate together to define a location in a packet and a hexadecimal value to compare to it.

Generic filter settings in a local Filter profile

In a local Filter profile, a generic filter uses the following parameters (shown with their default values):

```
[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
```

The same parameters are also available in the Output-Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	**Specifies**
Type	Type of filter. Valid values are Generic-Filter (the default), IP-Filter, IPX-Filter, Route-Filter, and TOS-Filter. Only the parameters in the corresponding subprofile will be applicable.
Offset	Byte-offset at which to start comparing packet contents to the Value setting specified in the filter. For details, see “Specifying the offset to the bytes to be examined” on page 9-9.
Len	Number of bytes to test in a packet, starting with the byte specified by the Offset parameter. For details, see “Specifying the number of bytes to test” on page 9-9.

Parameter	Specifies
More	Enable/disable application of the next filter before determining whether the packet matches the specification. If More is set to Yes, the current specification is linked to the one immediately following. The match occurs only if *both* specifications are matched. (The subsequent specification must be enabled, or the TAOS unit ignores the filter specification in which More is set to Yes. The More parameter enables you to create a filter that examines multiple noncontiguous bytes within a packet before the forwarding decision is made.
Comp-Neq	Type of comparison to perform. If Comp-Neq (Compare-Not-Equals) is set to Yes, the comparison succeeds (the filter matches) if the contents do not equal the specified value. For a filter that requires the packet contents to equal the specified value, leave Comp-Neq set to No.
Mask	Binary mask. The system applies the mask to the value specified by the Value parameter before comparing it to the bytes in a packet specified by the Offset parameter. For details, see “Masking the value before comparison” on page 9-10.
Value	Hexadecimal number to be compared to the packet data identified by the Offset, Length, and Mask calculations. After you have entered the number, the system enters a colon at the byte boundaries.

Generic filter settings in a RADIUS profile

In RADIUS, a generic filter entry is a value of the Ascend-Call-Filter or Ascend-Data-Filter attribute. To specify a generic filter value, use the following format:

```
"generic dir action offset mask value compare [more]"
```

Keyword or argument	Value
`generic`	Type of filter. Valid types specified by the Ascend-Data-Filter and Ascend-Call-Filter attributes are `generic` (the default) and `ip`.
`dir`	Specifies direction of the packets. You can specify `in` (to filter packets coming in to the TAOS unit or `out` (to filter packets going out of the TAOS unit).
`action`	Specifies the action that the TAOS unit takes with a packet that matches the filter. Specify either `forward` or `drop`.
`offset`	Byte-offset in a packet at which to start comparing packet contents to the *`value`* specified in the filter. For details, see “Specifying the offset to the bytes to be examined” on page 9-9.
`mask`	Binary mask. The system applies the *`mask`* to the specified *`value`* before comparing it to the bytes specified by *`offset`*. For details, see “Masking the value before comparison” on page 9-10.

Keyword or argument	**Value**
value	A hexadecimal number to compare to the packet contents at the specified *offset*. The length of the number must be the same as the length of the mask (up to 12 bytes).
compare	A comparison operator that determines how the TAOS unit compares packet contents to the filter value. You can specify = (equal to) or != (not equal to). The default is = (equal to).
more	If the more flag is present, the TAOS unit applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The direction and forwarding action of the next filter must be the same as the current filter, or the TAOS unit ignores this flag.

Specifying the offset to the bytes to be examined

The offset in a generic filter is a byte-offset from the start of a packet to the start of the data in the packet to be tested. For example, assume a filter with the following filter specification:

```
[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
```

Or assume a filter with comparable RADIUS filter definition:

```
Ascend-Data-Filter = "generic in drop 2 0fffffff000000f
07fe45700000009"
```

Then assume a packet with the following contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

When the filter is applied, the first two byes in the packet (2A and 31) are ignored because of the two-byte offset.

Specifying the number of bytes to test

In a RADIUS profile, the length of the mask must equal the length of the Value setting. The system tests that number of bytes in the packet, starting at the specified offset. In a local Filter profile, the Len setting specifies the number of bytes to test in a packet, starting with the byte specified by the Offset parameter. The Mask setting is assumed to have the same number of octets as the data specified by the Len parameter.

For example, assume a filter with the following filter specification:

```
[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
```

Then assume a packet with the following contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The filter tests the value of bytes three (97) through ten (99).

Masking the value before comparison

A generic filter can include a mask to apply to the value specified by the Value parameter before the TAOS unit compares it to the bytes starting at the specified offset. You can use the mask to specify exactly which bits you want to compare. The mask is assumed to have the same number of octets as the data specified by the Len parameter.

The TAOS unit translates both the mask and the value specified by the Value parameter into binary format and then applies a logical AND to the results. Each binary 0 (zero) in the mask hides the bit in the corresponding position in the value. A mask of all ones (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents. For example, assume a filter with the following specification:

```
[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
```

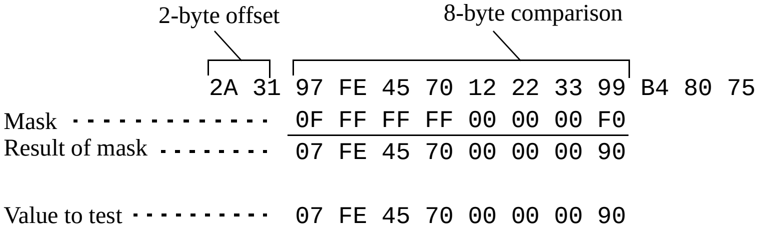
Or assume a filter with comparable RADIUS definition:

```
Ascend-Data-Filter = "generic in drop 2 0fffffff000000f
07fe45700000009"
```

Then assume a packet with the following contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The Value setting matches the packet data after application of the mask.



Assuming that the Forward parameter is set to No, the packet is dropped because it matches this filter. The byte comparison works as follows:

- The TAOS unit ignores 2A and 31 because of the 2-byte offset.
- The 9 in the third byte is also ignored, because the mask has a 0 (zero) in its place. The 7 in the third byte matches the Value parameter’s 7 for that byte.

- In the fourth byte, F and E match the fourth byte specified by the Value parameter.
- In the fifth byte, 4 and 5 match the fifth byte specified by the Value parameter.
- In the sixth byte, 7 and 0 match the sixth byte specified by the Value parameter.
- The seventh (12), eighth (22), and ninth (33) bytes are ignored because the mask has zeroes in those places.
- In the tenth byte, 9 matches the Value parameter’s 9 for that byte. The second 9 in the packet’s tenth byte is ignored because the mask has a 0 (zero) in its place.

Examples of a generic call filter

The following example shows how to define a generic call filter. The filter’s purpose is to prevent inbound packets from resetting the session timer.

In the input filter, the default values are left unchanged in the Gen-Filter subprofile, so all packets are matched. Also, the forwarding action is left at its default of No. In the output filter, the default values again match all packets, but the forwarding action is set to Yes. Therefore, the filter does not prevent outbound packets from resetting the timer or placing a call.

```
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
```

Following is a comparable RADIUS filter definition:

```
test-user Password = "test-pw"
    Ascend-Call-Filter = "generic in drop"
    Ascend-Call-Filter = "generic out forward"
```

Defining IP filters

IP filters affect only IP and related packets. They make use of high-level information in packets (for example, protocol numbers, logical addresses, and TCP or UDP ports).

IP filter settings in a local Filter profile

The IP-Filter subprofile contains the following parameters (shown with their default values):

```
[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
```

The same parameters are also available in the Output-Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	**Specifies**
Type	Type of filter. Valid values are Generic-Filter (the default), IP-Filter, IPX-Filter, Route-Filter, and TOS-Filter. Only the parameters in the corresponding subprofile will be applicable.
Protocol	Protocol number. A number of 0 (zero) matches all protocols. If you specify a nonzero number, the TAOS unit compares it to the Protocol field in each packet. For a list of assigned protocol numbers, see RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.
Source-Address-Mask	Mask to be applied to the Source-Address value before comparing that value to the source address of a packet.
Source-Address	IP address. After applying the Source-Address-Mask value, the TAOS unit compares the result to the source address in a packet. For details, see “Filtering by source or destination IP address” on page 9-14.
Dest-Address-Mask	A mask to be applied to the Dest-Address value before comparing that value to the destination address of a packet.
Dest-Address	IP address. After applying the Dest-Address-Mask value, the TAOS unit compares the result to the source address in a packet. For details, see “Filtering by source or destination IP address” on page 9-14.
Src-Port-Cmp	Type of comparison to perform when comparing source port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s source port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Source-Port value.
Source-Port	Port number to be compared with the source port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 9-14.
Dst-Port-Cmp	Type of comparison to perform when comparing destination port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s destination port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Dest-Port value.
Dest-Port	Port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 9-14.
TCP-Estab	Enable/disable application of the filter only to packets in an established TCP session. Applicable only if the protocol number has been set to 6 (TCP).

IP filter settings in a RADIUS profile

In RADIUS, an IP filter entry is a value of the Ascend-Call-Filter or Ascend-Data-Filter attribute. To specify an IP filter value, use the following format:

```
"ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ][[ proto ]
[ destport cmp value ] [ srcport cmp value ] [est]]"
```

Note: A filter definition cannot contain newline indicators. The syntax is shown here on two lines for printing purposes only.

Keyword or argument	Value
`ip`	Type of filter. Valid types specified by the Ascend-Data-Filter and Ascend-Call-Filter attributes are `generic` (the default) and `ip`.
`dir`	Specifies direction of the packets. You can specify `in` (to filter packets coming in to the TAOS unit or `out` (to filter packets going out of the TAOS unit).
`action`	Specifies the action that the TAOS unit takes with a packet that matches the filter. You can specify either `forward` or `drop`.
`dstip` *`n.n.n.n/nn`*	If the `dstip` keyword is followed by a valid IP address, the filter will match only packets with that destination address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `dstip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see "Filtering by source or destination IP address" on page 9-14.
`srcip` *`n.n.n.n/nn`*	If the `srcip` keyword is followed by a valid IP address, the filter will match only packets with that source address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `srcip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see "Filtering by source or destination IP address" on page 9-14.
`proto`	A protocol number. A value of zero matches all protocols. If you specify a nonzero number, the TAOS unit compares it to the Protocol field in packets. For a list of protocol numbers, see RFC 1700.
`dstport` *`cmp value`*	If the `dstport` keyword is followed by a comparison symbol and a number, the number is compared to the destination port of a packet. The comparison symbol can be < (less than), = (equal), > (greater than), or != (not equal). The port value can be one of the following names or numbers: 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), or talk (517). For more details, see "Filtering by port numbers" on page 9-14.

Keyword or argument	Value
`srcport` *`cmp value`*	If the `srcport` keyword is followed by a comparison symbol and a number, the number is compared to the source port of a packet. The comparison symbol can be < (less than), = (equal), > (greater than), or != (not equal to). The port value can be one of the following names or numbers: 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), or talk (517). For more details, see “Filtering by port numbers” on page 9-14.
`est`	If the `est` flag is present, it restricts application of the filter to packets in an established TCP session. The protocol number must be set to 6 (TCP), or the flag is ignored.

Filtering by source or destination IP address

When you specify a source or destination address in an IP filter, the TAOS unit applies the filter’s forwarding action to packets received from or sent to that address. If you also specify a subnet mask, the TAOS unit applies the mask to the address value before comparing the resulting value to the source or destination address in a packet.

To apply the mask, the TAOS unit translates both the mask and address values into binary format and then uses a logical AND to apply the mask to the address. The mask hides the bits whose positions match those of the binary zeroes in the mask. A mask of all zeros (the default) masks all bits. If the address value itself is also all zeros (the default), the filter matches any source or destination address. A mask of all ones (255.255.255.255) masks no bits, so the full address for a single host is compared to the address value.

You can use the address mask to mask out the host portion of an address, for example, or the host and subnet portion, so the specification matches the address to or from any host on a given network.

Filtering by port numbers

IP filters can specify a port number to be compared to the source or destination port (or both) in a packet. A port number of zero matches nothing. TCP and UDP port numbers are typically assigned to services. For a list of well-known port assignments, see RFC 1700, *Assigned Numbers*.

Note: For security purposes, you should filter all services from outside your domain that are not required. UDP-based services make you network particularly vulnerable to certain types of security attacks.

The specified type of comparison determines when a match occurs. If no comparison operator is specified in the filter, no comparison is made. You can specify that the filter matches the packet if the packet’s port number is less than, equal to, greater than, or not equal to the port number specified in the filter.

Examples of an IP filter to prevent local address spoofing

IP-address spoofing typically occurs when a remote device illegally acquires a local address and uses it to try to break through a data filter. This section presents an example of a data filter that prevents IP-address spoofing. For related information, see “Example of per-session source address checking” on page 2-22.

The sample filter first defines three input filters. The first filter drops packets whose source address is on the local IP network. The second filter drops packets whose source address is the loopback address (127.0.0.0). The third input filter accepts all remaining source addresses (by specifying a source address of 0.0.0.0) and forwards them to the local network.

In this example, the local IP network has an IP address of 192.100.50.128, with a subnet mask of 255.255.255.192. These values are just arbitrary examples.

Note: If you apply this filter to the Ethernet interface, the TAOS unit drops IP packets it receives from the local LAN, and you will not be able to Telnet to the unit.

The following set of commands creates the first input filter, setting the type to IP-Filter. The first filter specifies the source mask and address for the local network. If an incoming packet has the local address, the TAOS unit drops it instead of forwarding it to the Ethernet network, because Forward is set to No (the default).

```
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
```

The next set of commands creates the second input filter, setting the type to IP-Filter. The second filter specifies the loopback source address. If an incoming packet has the loopback address, the TAOS unit drops it instead of forwarding it to the Ethernet network, because Forward is set to 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
```

The next set of commands creates the third input filter, setting the type to IP-Filter and setting Forward to Yes. Except for Forward=Yes, the third filter uses all default values. Because Forward is set to Yes, the TAOS unit forwards all remaining packets (those with nonlocal source addresses) to the Ethernet network.

```
admin> set input 3 valid = yes

admin> set input 3 forward = yes

admin> set input 3 type = ip-filter
```

The next set of commands creates an output filter, setting the type to IP-Filter and the forwarding action to Yes. This filter specifies the source mask and address for the local network. (Packets originating on the local network should be forwarded across the 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
```

Following is a comparable RADIUS filter definition:

```
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"
```

Examples of an IP filter for more complex security issues

This section illustrates some of the issues you might need to consider when writing your own IP filters. However, the sample filter presented here does not address the fine points of network security. You might want to use this filter as a starting point and augment it to address your security requirements.

In this example, the local network supports a Web server, and the administrator needs to carry out the following tasks:

- Provide dial-in access to the server’s IP address
- Restrict dial-in traffic to all other hosts on the local network

However, many local IP hosts need to dial out to the Internet and use IP-based applications such as Telnet or FTP, so their response packets need to be directed appropriately to the originating host. In this example, the Web server’s IP address is 192.9.250.5. The filter will be applied in Connection profiles as a data filter.

The following set of commands creates the first input filter, setting the type to IP-Filter and Forward to Yes, and configures the first filter to allow packets to reach the Web server’s destination address at a destination TCP port that can be used for Telnet or 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 = eql

admin> set input 1 ip-filter dest-port = 80
```

The next set of commands creates the second input filter, with Type set to IP-Filter and Forward set to Yes. This filter allows inbound TCP packets in response to a local user's outbound Telnet request, by specifying that TCP packets whose destination port number is higher than that of the source port are forwarded. (Telnet requests go out on port 23, and responses come back on some random port above port 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
```

The next set of commands creates the third input filter, with Type set to IP-Filter and Forward set to Yes. This filter allows inbound RIP updates, by specifying that inbound UDP packets are forwarded if the destination port number is higher than that of the source port. (For example, suppose a RIP packet goes out as a UDP packet to destination port 520. The response to this request goes to a random destination port above port 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
```

The following commands create the fourth input filter, setting the type to IP-Filter and Forward to Yes. The fourth filter uses all default values, which allows unrestricted Pings and Traceroutes. Unlike TCP and UDP, ICMP does not use ports, so a port comparison is unnecessary.

```
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
```

Following are comparable RADIUS filter definitions:

```
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"
```

Defining TOS filters

To enable proxy-QoS for all packets that match a specific filter specification, you can define a TOS filter locally in a Filter profile, and then apply the filter to any number of Connection profiles or RADIUS profiles. (The Filter-ID attribute can apply a local Filter profile to

RADIUS user profiles.) You can also define TOS filters directly in a RADIUS user profile by setting the Ascend-Filter attribute. For TOS filters, the forwarding action in the filter has no effect.

TOS filter settings in a local Filter profile

Defining a local TOS filter involves setting the following parameters (shown with their default settings):

```
[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
```

Parameter	Specifies
Protocol	Protocol number. A value of zero matches all protocols. If you specify a nonzero number, the TAOS unit compares it to the Protocol field in each packet. For a list of protocol numbers, see RFC 1700.
Source-Address-Mask	Mask to be applied to the Source-Address value before comparing that value to the source address of a packet.
Source-Address	IP address. After applying the Source-Address-Mask value, the TAOS unit compares the result to the source address in a packet. For details, see “Filtering by source or destination IP address” on page 9-14.
Dest-Address-Mask	Mask to be applied to the Dest-Address value before comparing that value to the destination address of a packet.
Dest-Address	An IP address. After applying the Dest-Address-Mask value, the TAOS unit compares the result to the destination address in a packet. For details, see “Filtering by source or destination IP address” on page 9-14.
Src-Port-Cmp	Type of comparison to perform when comparing source port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s source port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Source-Port value.
Source-Port	Port number to be compared with the source port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 9-14.

Parameter	**Specifies**
Dst-Port-Cmp	Type of comparison to perform when comparing destination port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s destination port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Dest-Port value.
Dest-Port	Port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 9-14.
Precedence	Priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled and the packet matches the filter, the bits can be set to one of the following values (most significant bit first): • 000—Normal priority • 001—Priority level 1 • 010—Priority level 2 • 011—Priority level 3 • 100—Priority level 4 • 101—Priority level 5 • 110—Priority level 6 • 111—Priority level 7 (the highest priority)
Type-of-Service	Type of service of the data stream. The value of this attribute sets the four bits following the three most significant bits of the TOS byte. The four bits are used to choose a link according to the type of service. When TOS is enabled and the packet matches the filter, one of the following values can be set in the packet: • Normal—Normal service • Cost—Minimize monetary cost • Reliability—Maximize reliability • Throughput—Maximize throughput • Latency—Minimize delay

TOS filter settings in a RADIUS profile

In RADIUS, a TOS filter entry is a value of the Ascend-Filter attribute. To specify a TOS filter value, use the following format:

```
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 ]
```

Note: A filter definition cannot contain newline indicators. The syntax is shown here on multiple lines for printing purposes only.

Keyword or argument	Description
`iptos`	Specifies an IP TOS filter.
`dir`	Specifies direction of the packets. You can specify `in` (to filter packets coming in to the TAOS unit or `out` (to filter packets going out of the TAOS unit).
`dstip` *`n.n.n.n/nn`*	If the `dstip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that destination address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `dstip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see "Filtering by source or destination IP address" on page 9-14.
`srcip` *`n.n.n.n/nn`*	If the `srcip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that source address. If a subnet mask portion of the address is present, the TAOS unit compares only the masked bits. If the `srcip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see "Filtering by source or destination IP address" on page 9-14.
`proto`	A protocol number. A value of zero matches all protocols. If you specify a nonzero number, the TAOS unit compares it to the Protocol field in packets. For a list of protocol numbers, see RFC 1700.
`dstport` *`cmp value`*	If the `dstport` keyword is followed by a comparison symbol and a port, the port is compared to the destination port of a packet. The comparison symbol can be < (less than), = (equal to), > (greater than), or != (not equal to). The port value can be one of the following names or numbers: 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), or talk (517). For more details, see "Filtering by port numbers" on page 9-14.
`srcport` *`cmp value`*	If the `srcport` keyword is followed by a comparison symbol and a port, the port is compared to the source port of a packet. The comparison symbol can be < (less than), = (equal to), > (greater than), or != (not equal to). The port value can be one of the following names or numbers: 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), or talk (517). For more details, see "Filtering by port numbers" on page 9-14.

Keyword or argument	Description
`precedence` *`value`*	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. If a packet matches the filter, the bits are set to the specified value (most significant bit first). Specify one of the following values: • 000—Normal priority • 001—Priority level 1 • 010—Priority level 2 • 011—Priority level 3 • 100—Priority level 4 • 101—Priority level 5 • 110—Priority level 6 • 111—Priority level 7 (the highest priority).
`type-of-service` *`value`*	Type of Service of the data stream. If a packet matches the filter, the system sets the four bits following the three most significant bits of the TOS byte to the specified value. The four bits are used to choose a link according to the type of service. Specify one of the following values: • Normal (0)—Normal service • Disabled (1)—Disables TOS • Cost (2)—Minimize monetary cost • Reliability (4)—Maximize reliability • Throughput (8)—Maximize throughput • Latency (16)—Minimize delay

Examples of defining a TOS filter

The following set of commands defines a TOS filter for TCP packets (protocol 6) that are destined for a single host at 10.168.6.24. The packets must be sent on TCP port 23. For incoming packets that match this filter, the priority is set at level 2. This relatively low priority means that an upstream router that implements priority queuing can drop these packets when it becomes loaded. The commands also set TOS to prefer a low latency connection, which means that the upstream router will choose a fast connection if one is available, even if it has higher cost or lower bandwidth, or is less reliable than another available link.

```
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
00:00:00:0+
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+
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
```

Following is a RADIUS user profile that contains a comparable filter definition:

```
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
    precedence 010 type-of-service latency"
```

Note: Filter definitions cannot contain newline indicators. The preceding example shows the Ascend-Filter value on two lines for printing purposes only.

Defining IPX filters

IPX filter specifications are not supported in RADIUS. They affect only NetWare packets, and their main purpose is to identify specific networks, hosts, or services. In a local Filter profile, the IPX-Filter subprofile contains the following parameters (shown with their default values):

```
[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
```

The same parameters are also available in the Output-Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	Specifies
Type	Type of filter. Valid values are Generic-Filter (the default), IP-Filter, IPX-Filter, Route-Filter, and TOS-Filter. Only the parameters in the corresponding subprofile will be applicable.
Src-Net-Address	Network-Number portion of the source IPX address.
Dest-Net-Address	Network-Number portion of the destination IPX address.
Src-Node-Address	Node-Number portion of the source IPX address.
Dest-Node-Address	Node-Number portion of the destination IPX address.
Src-Socket	Source socket number.
Src-Socket-Cmp	Type of comparison to perform against the source socket number. You can specify that the filter matches the packet if the packet's source socket number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the source socket number specified in the filter.
Dest-Socket	Destination socket number.
Dst-Socket-Cmp	Type of comparison to perform against the destination socket number. You can specify that the filter matches the packet if the packet's destination socket number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the destination socket number specified in the filter.

Filtering by source or destination IPX address

The network address and node address parameters are designed to work together to specify a source or destination NetWare server. A full IPX network address uses the following format:

`network-number:node-number`

The Src-Net-Address and Dest-Net-Address parameters specify the network-number portion of the address. The network number is a unique 8-byte hexadecimal number that is common to all hosts on a particular LAN. NetWare servers have an internal network number that is the destination network address for file read/write requests. (If you are not familiar with internal network numbers, see your NetWare documentation for details.)

The Src-Node-Address and Dest-Node-Address parameters specify the node-number portion of the address. The node number is a 12-byte hexadecimal number that is unique to each node on a LAN. Each filter that specifies an IPX network number should also specify the corresponding node number. (For example, if you specify a value for Src-Net-Address in a filter, you should also specify a value for Src-Node-Address.)

Typically, a NetWare server address has the node number 1 (00:00:00:00:00:01) on the server's internal network. A node number of all 1s (FF:FF:FF:FF:FF:FF) matches all nodes on a LAN.

Filtering by socket number

NetWare servers use a particular socket number for each service. For example, NetWare file service typically uses socket 0451 (04:51). Some services use dynamic socket numbers, which can change each time they load. A socket number of all 1s (FF:FF) matches any socket on the specified server.

When you specify a NetWare socket number, you must also indicate how to compare the socket number in a packet to the specification in the filter. The Src-Socket-Cmp parameter specifies the method of comparison for the source socket number. You can specify that the filter matches the packet if the packet's source socket number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the source socket number specified in the filter.

The Dst-Socket-Cmp parameter specifies the method of comparison for the destination socket number. You can specify that the filter matches the packet if the packet's destination socket number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the destination socket number specified in the filter.

Example of an outbound IPX filter

When the following sample IPX filter is applied as a data filter to a WAN interface, it causes the TAOS unit to drop all outbound IPX packets that have a destination IPX network address of 00003823, regardless of the destination IPX node or socket number in the packets. All other packets are forwarded.

```
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 = ffffffffffff

admin> set output 2 forward = yes

admin> write
FILTER/dstipx read
```

Example of an inbound IPX filter

When the following sample IPX filter is applied as a data filter to a WAN interface, it causes the TAOS unit to drop all inbound IPX packets received from a specific source. In this example, the filter causes the TAOS unit to drop packets from source IPX network address 00000005:00abcde12345 and source socket number 4002. All other packets are forwarded.

```
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 = eql

admin> set input 2 forward = yes

admin> write
FILTER/srcipx read
```

Defining route filters

Route filter specifications are not supported in RADIUS. Route filters affect only RIP packets. For route filters, the forwarding action in the filter has no effect.

In a local Filter profile, the Route-Filter subprofile contains the following parameters (shown with their default values):

```
[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
```

The same parameters are also available in the Output-Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	Specifies
Type	Type of filter. Valid values are Generic-Filter (the default), IP-Filter, IPX-Filter, Route-Filter, and TOS-Filter. Only the parameters in the corresponding subprofile will be applicable.
Source-Address-Mask	Mask to be applied to the Source-Address value before comparing that value to the source address of a RIP update packet.
Source-Address	IP address. After applying the Source-Address-Mask value, the TAOS unit compares the result to the source address in a RIP packet. For related information, see “Filtering by source or destination IPX address” on page 9-23.
Route-Mask	Mask to be applied to the destination address of a route.
Route-Address	IP address. After applying the Route-Mask value, the TAOS unit compares the result to routes in a RIP packet. If it finds a route with a matching destination, it takes the specified action.
Add-Metric	Number from 1 to 15, to be added to the metric value for a route that matches the filter specification, if the specified value for the Action parameter is Add.

Parameter	Specifies
Action	An action to take on a route that matches the filter specification. Valid values are None (the default), Accept (accept the route by allowing it to affect the routing table), Deny (deny the route by not allowing it to affect the routing table), or Add (add the value of the Add-Metric parameter to the route metric and accept the route).

Example of a filter that excludes a route

In this example, the defined input filters accept all inbound RIP packets except those with a destination of 90.0.0.0. Following are the commands entered to define the filter, and the system's responses:

```
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
```

In this sample route filter, any route that matches filter 1 is rejected, and all other routes are accepted (because they match filter 2).

Example of a filter that configures a route's metric

In this example, an output filter identifies the route 11.0.0.0 in outbound RIP packets and assigns a high metric to that route. Following are the commands entered and the system's responses:

```
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
```

Defining dynamic remote filters

You can create RADIUS pseudo-user profiles that define data filters, and apply the filters to multiple local Connection or RADIUS profiles by referring to the pseudo-user profile name.

When the TAOS unit receives a filter ID in an Access-Accept packet from RADIUS, it searches for a matching local filter. If it does not find one, the TAOS unit requests the filter from the RADIUS server. You can specify how the system should behave if the filter referred to in a profile is not found. The system can either establish the session and log a message about the missing filter, or simply terminate the call.

Externally defined filters are cached locally for a configurable interval. The FiltCache command displays statistics about each cached RADIUS filter profile, and enables you to flush profiles from the cache. For more information about the FiltCache command, see the *APX 8000/MAX TNT Administration Guide*.

Current limitations on dynamic remote filters

In the current software version, the remote filter implementation is subject to the following limitations:

- Filters applied to dialout calls are not supported in this release.
- Call filters, route filters, and TOS filters are not supported in this release. Only data filters are currently supported.

Overview of local profile settings

Following are the local parameters (shown with default values) related to dynamic remote filters:

```
[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
```

Parameter	**Specifies**
Filter-Required	Whether access to the filter is required for the session. With the default value of `no`, the system establishes the session even if the specified filter is not found. If the parameter is set to `yes`, the system disconnects the call if the filter is not found. This parameter does not apply if the profile does not refer to a filter by name. In the Answer-Defaults profile, this parameter is used for RADIUS user profiles that apply a filter and do not specify a value for Ascend-Filter-Required (50).

Parameter	**Specifies**
Data-Filter	Name of a Filter profile associated with the connection. The name can be that of a local profile or of a pseudo-user profile in RADIUS. However, if a local Connection profile does not use authentication, it cannot specify a RADIUS filter profile.
Default-Filter-Cache-Time	Number of minutes to cache RADIUS filter profiles that do not include a value for Ascend-Cache-Time (57). The default is `1440` (24 hours). Once the cache timer expires, cached profiles are deleted from system memory. The next time a remote filter is needed, the system retrieves the profile from RADIUS and stores it in cache again. Keeping a profile in cache increases performance when establishing sessions that use the filter, at the cost of some system memory. If this parameter is set to `0` (zero), the default timer is disabled so that only RADIUS profiles that specify a cache time are cached.

Overview of RADIUS user profile settings

RADIUS user profile support for filter profiles is provided by the following vendor-specific attributes (VSAs):

RADIUS Attribute	**Specifies**
Filter-ID (11)	Name of a local or remote filter profile associated with the connection.
Ascend-Filter-Required (50)	Whether access to the filter is required for the session. With the default value of Required-No (0), the system establishes the session even if the specified filter is not found. If the attribute is set to Required-Yes (1), the system disconnects the call if the filter is not found. This attribute does not apply if the profile does not refer to a filter by name. If no value is specified for this attribute, setting for the Filter-Required parameter in the Answer-Defaults profile is used to determine system behavior when the specified filter is not found.

A filter profile is a pseudo-user profile in which the first two lines have the following format:

```
profile-name Password = "ascend" Service-Type = Outbound
```

The *profile-name* value is any name you assign to the profile. Duplicate filter names are not allowed. If a local Filter profile is already stored, the TAOS unit does not retrieve a filter profile of the same name from the RADIUS server. Filter profile definitions can include the following attribute-value pairs:

RADIUS Attribute	Specifies
Ascend-Data-Filter (242)	An abinary-format filter definition using one of the following formats: "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)	Whether the timer for cached routes in this profile is reset each time a new session that refers to the pseudo-user profile becomes active. Refresh-No (0) does not reset the timer. Refresh-Yes (1) resets the cache timer when a session referring to the profile becomes active.
Ascend-Cache-Time (57)	Number of minutes to cache the profile. Once the cache timer expires for a RADIUS profile, the profile is deleted from system memory. The next time it is needed, the system retrieves it from RADIUS and stores it in cache again. Keeping a profile in cache increases the performance of route lookups, at the cost of some system memory. The minimum possible cache time is 0 minutes, which causes the system to retrieve the profile every time it is needed. This value is usually not desirable. If no value is specified for this attribute, the setting for the Default-Filter-Cache-Time parameter in the IP-Global profile is used.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS unit must be configured in VSA compatibility mode. Following are the relevant settings:

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

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

For details about these settings, see the *APX 8000/MAX TNT Reference*.

Examples of configuring a filter profile in RADIUS

Following is a sample RADIUS filter profile:

```
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"
```

The cache timer has been set to 20 minutes, and the timer is reset each time the filter is applied to a session.

The following commands configure a default cache time for RADIUS filter profiles:

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

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

admin> write
IP-GLOBAL written
```

Following is a sample RADIUS filter profile that uses the default instead of specifying a value for 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"
```

Examples of applying remote filters

The following commands modify a Connection profile so that the session uses a remote filter and the system disconnects the call if the filter is not found:

```
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
```

The following RADIUS profile applies the same filter profile and has the same requirements. This profile also specifies how the filters must be cached for this connection.

```
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
```

The following commands configure the system to reject incoming calls when the RADIUS user profile specifies a filter that is not found and the user profile does not explicitly state what to do if the filter is not found:

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

admin> set session-info filter-required = yes

admin> write
ANSWER-DEFAULTS written
```

Following is a sample RADIUS profile that uses the default instead of specifying a value for 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"
```

Applying a filter to an interface

When you apply a filter to a WAN interface, it takes effect when the connection is brought up.

Packets can pass through both a data filter and call filter on a WAN interface. When both a data filter and call filter are applied to the same interface, the data filter is applied first.

Settings in local profiles

To apply a filter to an interface, set the following parameters (shown with their default settings):

```
[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= ""
```

Parameter	Specifies
Call-Filter	Name of a Filter profile. For details, see “Examples of applying a call filter to a WAN interface” on page 9-34. The setting in the Answer-Defaults profile is used only for RADIUS-authenticated connections that do not include a call filter.
Data-Filter	Name of a Filter profile. For details, see “Examples of applying a data filter to a WAN interface” on page 9-33. The setting in the Answer-Defaults profile is used only for RADIUS-authenticated connections that do not include a data filter.
Filter-Persistence	Enable/disable filter persistence across connection state changes.
Route-Filter	Name of a Filter profile. For details, see “Examples of applying a route filter to a WAN or LAN IP interface” on page 9-35.
TOS-Filter	Name of a Filter profile. For details, see “Examples of applying a TOS filter to a WAN interface” on page 9-34.
Filter-Name	Name of a Filter profile. For details, see “Example of applying a filter to a LAN interface” on page 9-35.

Settings in RADIUS profiles

The following RADIUS attribute-value pairs are used to apply a filter to a WAN connection:

RADIUS Attribute	**Value**
Ascend-Call-Filter (243)	Abinary-format filter definition using one of the following formats: "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]]" For details, see “Defining generic filters” on page 9-7 and “Defining IP filters” on page 9-11.
Ascend-Data-Filter (242)	Abinary-format filter definition using one of the following formats: "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]]" For details, see “Defining generic filters” on page 9-7 and “Defining IP filters” on page 9-11.
Ascend-Filter (90)	String-format filter specification using the following format: 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*] For details, see “Defining TOS filters” on page 9-17.
Filter-ID (11)	Name of a local Filter profile that defines a data filter. The next time the TAOS unit accesses the RADIUS user profile in which this attribute appears, the referenced filter is applied to the connection.

How the system uses Answer-Defaults profile settings

When the Use-Answer-For-All-Defaults parameter is set to Yes (the default), TAOS unit uses the settings in the Answer-Defaults profile to create a baseline profile for RADIUS-authenticated calls. The unit uses the baseline values for settings that are not specified in the caller’s RADIUS profile. For example, if the caller’s RADIUS profile does not apply a data filter, a call filter, or both, and the Use-Answer-for-All-Defaults parameter is set to Yes, any filters applied in the Answer-Defaults profile are applied to the authenticated connection. But if the caller’s profile does apply a data or call filter, filters applied in the Answer-Defaults profile are used.

Examples of applying a data filter to a WAN interface

When you apply a data filter, its forwarding action (forward or drop) affects the actual data stream by preventing certain packets from reaching the Ethernet network from the WAN, or vice versa. Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process. In the following examples, the TAOS unit supports the following two local Filter profiles:

```
admin> dir filter
370  09/13/1998 15:04:31  ip-spoof
372  09/13/1998 15:04:43  web-access
```

Following is an example of applying a data filter:

```
admin> read conn tlynch
CONNECTION/tlynch read

admin> set session data-filter = ip-spoof

admin> write
CONNECTION/tlynch written
```

Following is a comparable RADIUS profile:

```
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"
```

The following RADIUS profile refers to both local filters:

```
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"
```

As is always the case with filters, the order in which they are applied within the user profile is significant. If the TAOS unit supports multiple Filter profiles with similar names, it attempts to match the first Filter profile to the characters specified in the user profile.

Following is an example of defining an antispoofing filter within the user's RADIUS profile:

```
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"
```

Examples of applying a call filter to a WAN interface

Call filters prevent unnecessary connection time and help the TAOS unit distinguish active traffic from “noise.” By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection’s idle timer.

The following commands apply a filter to a WAN connection and set the idle timer to 20 seconds. If no packets get through the call filter in either direction for 20 seconds, the connection is torn down.

```
admin> read conn bob
CONNECTION/bob read

admin> set session call-filter = out-only

admin> set session idle-timer = 20

admin> write
CONNECTION/bob written
```

Following is a comparable RADIUS profile:

```
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"
```

Examples of applying a TOS filter to a WAN interface

TOS filters instruct the system to set priority bits and Type-of-Service (TOS) classes of service on behalf of customer applications. The TAOS unit does not implement priority queuing, but it does set information that can be used by upstream routers to prioritize and select links for particular data streams. TOS filters specify which bits to set in the TOS header of IP packets.

The following set of commands applies a TOS filter to a Connection profile. When the incoming data stream contains packets that match the TOS filter specification, the proxy-QoS and TOS settings specified in the filter are set in those packets.

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

admin> set ip-options tos-filter = jfans-tos-filter

admin> write
CONNECTION/jfan-pc written
```

Following is a comparable RADIUS profile in which the TOS filter is specified by the Filter-ID attribute:

```
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"
```

Following is a RADIUS profile in which the TOS filter is specified within the profile:

```
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"
```

Note: Filter definitions cannot contain newline indicators. The preceding example shows the specification on two lines for printing purposes only.

Examples of applying a route filter to a WAN or LAN IP interface

Route filters specify which routes in RIP update packets will be allowed to affect the routing table. They can also be used to increase the metric assigned to a route before adding it to the routing table.

When a route filter is applied to an IP interface, the TAOS unit monitors RIP packets on that interface and takes a specified action when a route matches the filter specifications. Depending on how the filter is defined, it can apply to inbound RIP packets, outbound RIP packets, or both. Route filters are supported only in Filter profiles defined locally in the command-line interface, not in filters defined in RADIUS.

Route filters do not stop RIP update packets from being forwarded. Rather, their action determines whether the system adds matching routes to its routing table.

Following is an example of applying a filter in a Connection profile:

```
admin> read conn bdv
CONNECTION/bdv read

admin> set ip-options route-filter = route-test

admin> write
CONNECTION/bdv written
```

Following is an example of applying a route filter to a local IP interface:

```
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
```

Example of applying a filter to a LAN interface

Ethernet interfaces are connected routes, so call filters are not applicable. However, you can apply a data filter that affects which packets are allowed to enter or leave the Ethernet network. A filter applied to an Ethernet interface takes effect immediately. If you change any settings in a Filter profile, the changes apply as soon as you save the Filter profile.

Note: Use caution when applying a filter to the Ethernet interface. You could inadvertently render the TAOS unit inaccessible from the local LAN.

The following set of commands applies a filter to a local network interface:

```
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
```

IP Fax

10

Store-and-forward IP fax

The store-and-forward IP fax feature enables the TAOSunit to interact with a third-party fax server, such as the servers provided by Open Port Technology, Inc. Fax-over-IP technology enables ISPs and corporate hubs to use the Internet to deliver faxes.

When the IP fax feature is enabled in the TAOSunit, the system acts as a remote access server (RAS), accepting fax calls on the same ports and telephone lines used for dial-in modem connections. The unit also performs modem dial-out functions to deliver faxes from the Internet to fax machines on the Public Switched Telephone Network (PSTN).

Incoming and outgoing IP faxes

Figure 10-1 shows the basic structure of an incoming IP fax operation. A TAOS unit receives an *incoming fax* from the PSTN and interacts with the fax server to transfer it to the Internet. The transfer to the Internet is transparent to the person sending a fax, because a hardware device called a *redialer* is connected to the fax machine. The redialer intercepts the number dialed on the fax machine and initiates a call to the TAOS unit instead. When the fax server begins transferring the fax to the Internet, the redialer and the TAOS unit become transparent pipes for the fax data.

Figure 10-1. Incoming IP fax from fax machine to Internet

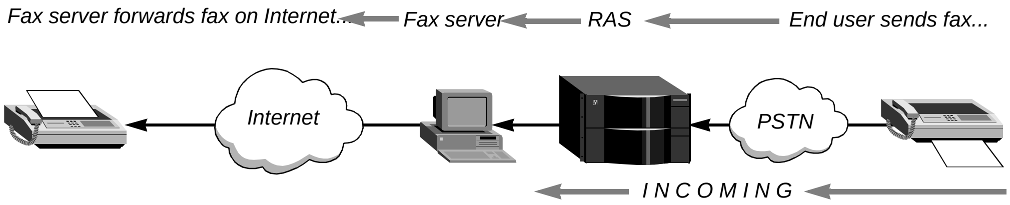
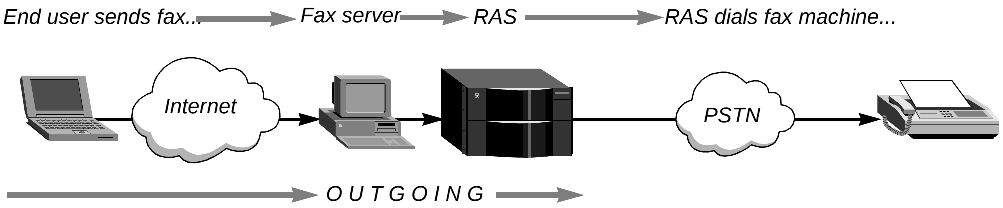


Figure 10-2 shows the basic structure of an outgoing IP fax operation. The fax server receives an *outgoing fax* from the Internet and interacts with the TAOS unit to transfer it to the PSTN. The fax server logs in to the TAOS unit and is authenticated before seizing one of the unit’s modems for dial-out to the destination fax machine.

Figure 10-2. Outgoing IP fax from Internet to fax machine



System parameters for IP fax modem usage

To send faxes, the fax server logs in to the TAOS unit, gains control of one of its modems, and dials out. The fax server configuration specifies the IP address of the TAOS unit and (optionally) one or more trunk groups for IP fax use. In addition to the IP fax login and port parameters that enable the fax server to log in, which are described in the next section, the following parameters in the System profile affect the resources available for outgoing fax calls. (The settings shown are the defaults.)

```
[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
```

Parameter	Specifies
Use-Trunk-Groups	Enable/disable the use of trunk groups in the TAOS unit. With the default setting `no,` the Num-Digits-Trunk-Groups and Trunk-Group settings do not apply. With the `yes` setting, all channels must be assigned trunk-group numbers.
Num-Digits-Trunk-Groups	Number of digits to allow for trunk groups. Currently, the IP fax server supports 2-digit trunk groups, but the trunk-group-number specification must be within the range of 2 to 9. The TAOS unit must agree with the fax server about the number of digits in a trunk-group number. Otherwise, telephone numbers are not parsed correctly and calls fail. For details, see the *APX 8000/MAX TNT Physical Interface Configuration Guide*.

Parameter	Specifies
Parallel-Dialing	Total number of dial-out calls that the TAOS unit can place at the same time.
Default-Call-Type	Default call type for calls on non-ISDN T1 or E1 lines. This parameter must be set to `voice` for IP fax over inband signaling.
Trunk-Group	Trunk-group number (from 2 to 9). For a network line, this parameter assigns channels to a trunk group. In a Call-Route profile, it specifies that calls received on that trunk group will be routed to the shelf, slot, and port specified in the profile's index.

Assigning bandwidth for typical IP fax usage

After the fax server has control of a digital modem, it dials the call on any available channel unless the fax server configuration specifies a trunk-group number. In that case, the fax server uses an available channel within that trunk group. If no channels in that trunk group are available, the TAOS unit returns a `Trunk Group Not Available` code to the fax server, which tries the call again later.

For example, the following commands configure the system to use 2-digit trunk groups, and assign an entire a T1 line to trunk group 5. (Fewer than 24 channels can be assigned to a trunk group, if appropriate.) If the fax server configuration also specifies 2-digit trunk groups and trunk group 5, these channels are available for IP fax usage.

```
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
```

Configuring a typical Call-Route profile

After assigning the trunk group, you must create a Call-Route profile to direct outbound calls to the newly configured line if they are to use trunk group 5. For example:

```
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
```

Specifying the maximum number of parallel dial-outs

The Parallel-Dialing parameter limits the number of dial-out calls that the system can place at one time. If the maximum number of dial-out calls is being processed and a dial-out request is made, the system queues the request and processes it at the earliest possible opportunity.

This operation is transparent to the fax server, except that the modems can time out if a dial-out request is delayed more than 30 to 40 seconds. Following is an example that sets Parallel-Dialing to the maximum value for T1:

```
admin> read system
SYSTEM read
admin> set parallel-dialing = 64
admin> write
SYSTEM read
```

Configuring a TAOS unit for IP fax

Following are the IP fax parameters that enable the TAOS unit to interact with a third-party fax server. (The settings shown are the defaults.)

```
[in IP-FAX]
ip-fax-enabled = yes
outgoing-fax-port = 10002
server-login = ipfax
dialer-type = atlas
server-password = works
incoming-fax-port = 10002
all-calls-are-fax = no
fax-incoming-call-type = did
fax-dnis = [ 8057 8052 8004 "" "" "" "" "" ]
fax-did  = [ 7470000 7775555 "" "" "" "" "" ]
fax-servers = [ 10.40.40.126 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ]
```

```
[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
```

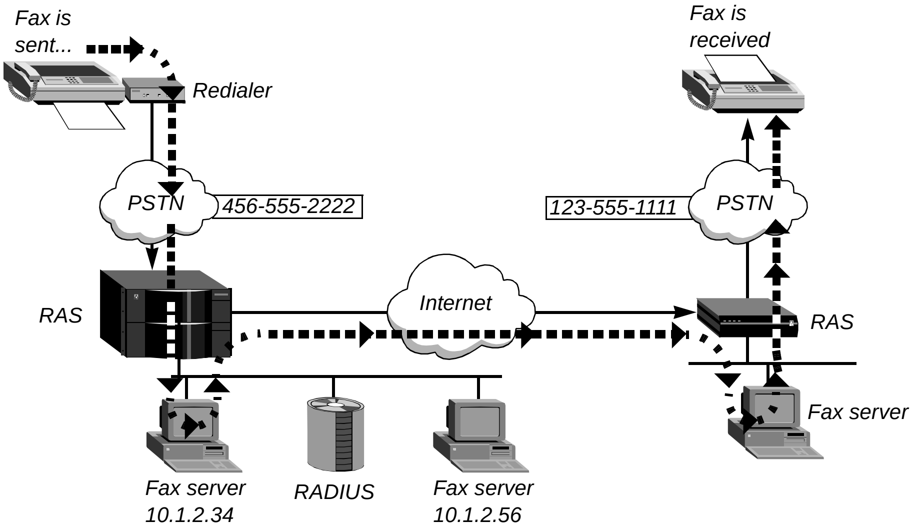
Parameter	Specifies
IP-Fax-Enabled	Enable/disable IP fax support in the TAOS unit. It is disabled by default.
Outgoing-Fax-Port	TCP port on which to accept outgoing fax data from a fax server. (Outgoing fax data is received from the Internet and requires a dial-out to a destination fax machine.) The default is `10001`.
Server-Login Server-Password	Name and password used to authenticate the fax server as part of an outgoing fax session. When the fax server receives a fax from the Internet, it connects to the TAOS unit and sends a name and password. The TAOS unit compares the values to the Server-Login and Server-Password settings.
Dialer-Type	Type of redialer that the TAOS unit uses for incoming fax calls. Specify `mitel` (the default) for a MITEL redialer or `atlas` for an Atlas redialer.
Incoming-Fax-Port	TCP port on which the fax server listens for incoming fax data. (Incoming fax data is received from a fax machine redialer.) The default is zero.

Parameter	**Specifies**
All-Calls-Are-Fax	Enable/disable the handling of all calls as fax calls. Otherwise, the TAOS unit authenticates the incoming call based on DNIS or direct inward dialing (DID). The following values are valid: • `yes`—The TAOS unit receives all calls as fax calls so that IP fax service can be supported where DNIS or DID is not available. • `no` (the default)—The TAOS unit recognizes the call by matching the caller's DNIS number to one of the Fax-DNIS numbers specified by Fax-DNIS [*1*-*8*] or DID numbers, depending on the value specified in the `fax-incoming-call-type` parameter.
Fax-Incoming-Call-Type	Type of fax call that the TAOS unit will accept. The following values are valid: • `redialer`—All fax calls are redialer calls (the default). • `did`—The TAOS unit authenticates the call based on DID entries.
Fax-DID	List of up to eight DID numbers for authentication. A DID number is a dialable string of up to 24 numbers.
Fax-DNIS [*1*–*8*]	Up to eight DNIS numbers. The TAOS unit compares the DNIS number supplied in the PRI setup message of an incoming call to the configured numbers. If the match is not exact, the unit does not start the IP fax functionality.
Fax-Servers [*1*–*5*]	IP address of up to five fax servers. The fax server systems are typically on the local IP network, but local connectivity is not a requirement. The TAOS unit first tries to connect to the fax server at the first specified address. If the unit receives no response, it tries to connect to the second address. If the unit still receives no response, it tries the third, and so forth. Once the TAOS unit connects to a fax server successfully, it continues to use that address for subsequent connections until a connection attempt fails, at which point it tries the next configured address.

Example of an IP fax configuration for incoming faxes

Figure 10-3 shows a TAOS unit receiving an incoming fax across the PSTN. The unit then initiates a TCP session with a fax server, which authenticates the incoming call. (The fax server might use RADIUS, as shown in Figure 10-3, or a method proprietary to that server.) If the fax server authenticates the call successfully, it dials out to the remote fax server on one of the TAOS unit's modems. When the fax transmission is completed, the fax server terminates the TCP session and the TAOS unit regains control of its modem.

Figure 10-3. Receiving and forwarding incoming IP faxes



Following is an example of an IP fax setup that enables a TAOS unit to handle incoming fax calls as shown in Figure 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
```

With this configuration, the IP fax is processed as follows:

1. An end user sends a fax to 123-555-1111.
2. The sending fax machine receives a dial tone from the redialer (which is directly connected to the fax machine) and dials 123-555-1111.
3. The redialer intercepts the call, stores the destination telephone number, and dials its configured number for the TAOS unit (456-555-2222).
4. The TAOS unit receives the call and identifies it as a fax call by comparing the call’s DNIS number to the Fax-DNIS values in the IP-Fax profile.

5. If the DNIS numbers match (or if the unit is configured to treat all incoming calls as IP fax calls), the TAOS unit generates an answer tone at 400 Hz to initiate dual-tone multifrequency (DTMF) communication with the redialer. Then the unit decodes the incoming DTMF sequence from the redialer, which contains the account number of the redialer and the destination telephone number 123-555-1111.
6. The TAOS unit initiates a connection to the fax server, sending the caller's account number and destination telephone number in the first TCP packet.
7. If the fax server authenticates the call successfully with this information, the TAOS unit answers the incoming fax call. If authentication fails, the connection is cleared.
8. Following successful authentication, the TAOS unit and fax server establish a TCP session, and the TAOS unit transfers control of an available modem to the fax server for the incoming call. If no send or receive activity occurs for more than 2 minutes, the session is terminated and resources are freed.

Note: For fax accounting, a fax session starts when a modem resource is allocated and stops when a session is terminated.

Support for direct inward dialing (DID) on inbound IP fax calls

Every DID subscriber, such as a network user or network printer receives a DID number. To send a fax to a network user or device, senders dial the fax subscriber's DID number and are connected to a TAOS unit.

When a TAOS unit detects an incoming fax call, it authenticates the call by matching the DID number received from the DID trunk against the DID numbers set in the `fax-did` parameter of the Ip-Fax profile. If the numbers match, the TAOS unit initiates a connection with the fax server by sending an incoming fax authentication packet (IFAP) to the fax server for authentication. The incoming fax authentication packet includes the following information:

- Line identifier
- DID number
- Caller ID (if available)

In response to the incoming fax authentication packet, the fax server sends a fax connection response packet (FCRP) that contains one of the following:

- FCRP-NACK—The fax server is unable to handle the call.
- FCRP-ACK—The fax server is unable to handle the call.

After successful establishing a connection with the fax server, the TAOS unit forwards the fax to the fax server.

If the first server fails to accept the call, the TAOS unit attempts a connection with the next fax server and so forth. After a connection has been established with a fax server, the TAOS unit continues to use that particular fax server for subsequent calls until the connection to that fax server fails. The TAOS unit then attempts to connect to the next fax server specified in the `fax-server` parameter.

Table 10-1 summarizes how a TAOS unit authenticates a call, based on the settings in the `all-calls-are-fax` and `fax-incoming-call-type` parameters.

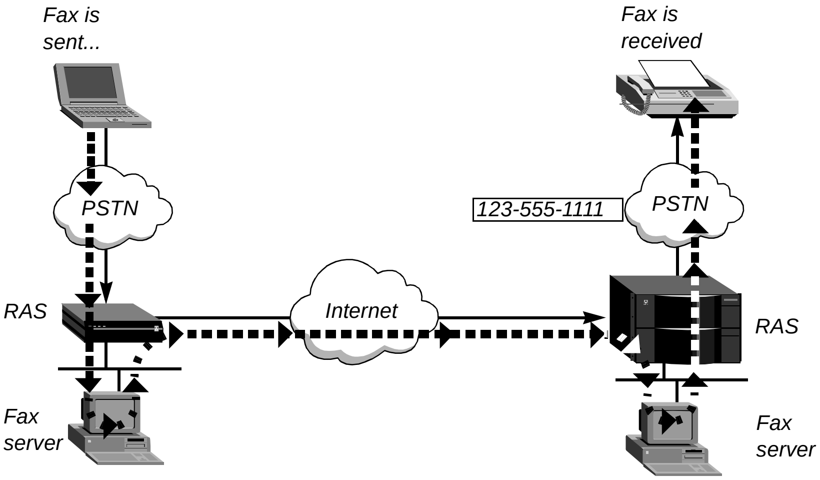
Table 10-1. How IP-Fax settings determine authentication

`all-calls-are-fax`	`fax-incoming-call-type`	TAOS unit behavior
`yes`	`redialer`	Receives all incoming calls as redialer type of fax call.
`yes`	`did`	Treats all incoming calls as DID type fax calls.
`no`	`did`	Authenticates the call against the DID numbers in the `fax-did` parameter.
`no`	`redialer`	Authenticates the call against the DNIS numbers in the `fax-dnis` parameter.

Example of an IP fax configuration for outgoing faxes

Figure 10-4 shows a TAOS unit forwarding a fax received by the fax server from the Internet. The fax server logs in to the TAOS unit, entering the specified Server-Login and Server-Password values, and initiates a modem dial-out session to forward the fax over the PSTN. When the fax transmission is completed, the fax server terminates the TCP session and the TAOS unit regains control of its modem.

Figure 10-4. Sending an outgoing IP fax to a fax machine



Following is an example of an IP fax setup that enables a TAOS unit to handle outgoing fax calls as shown in Figure 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
```

With this configuration, the TAOS unit processes an IP fax as follows:

1. The fax server on the local network receives fax data across the Internet from a remote fax server.
2. The fax server initiates a connection to the TAOS unit, sending its login name and password in the first TCP packet.
3. If the login name and password match the Server-Login and Server-Password values, respectively, in the IP-Fax profile, the TAOS unit establishes a TCP session with the fax server. If authentication fails, the connection is cleared.
4. After authentication, the TAOS unit transfers control of an available modem to the fax server.
5. The fax server sends modem commands encapsulated in TCP packets, initiates a connection to the destination fax machine, and sends the spooled data. If no send or receive activity occurs for more than 2 minutes, the session is terminated and resources are freed.

Note: For fax accounting, a fax session starts when a modem resource is allocated and stops when a session is terminated.

Fax hangup codes and disconnect cause codes

Conexant supplies two fax hangup codes:

- +FHNG 1—when fax tones are recognized but the handshake fails
- +FHNG 11—when no fax tones are recognized at the far end

ISDN disconnect cause codes are returned when fax calls fail, if they are available as part of the fax hangup codes. To avoid conflict with codes returned by modems and with codes returned by other units, the fax cause codes add 1000 to the standard codes so that they are in the range of 1000–1255. For example, Far End Busy (ISDN Code 17) is returned as +FHNG 1017, and Far End Did Not Answer (go off-hook) is returned as +FHNG 1018.

IP fax call accounting

In earlier versions of the software, more accounting information was available for an incoming call than for an outgoing call. Because the IP fax feature creates a large volume of outgoing calls, SNMP, RADIUS, and Syslog call-accounting information has been expanded to include the following additional accounting information for outgoing IP fax calls:

- A call-connected timestamp, showing the length of the call

- The trunk group used for particular channels on an outgoing call
- The destination telephone number dialed from the TAOS unit
- The shelf, slot, line, and channel number at which the call originates
- The total bytes sent and received (in SNMP and RADIUS only)
- The transmit and receive baud rate (in SNMP and RADIUS only)

Note: For accounting purposes, a fax session starts when a modem resource is allocated and stops when the session is terminated.

SNMP changes for IP fax operation

SNMP provides additional call information in the following fields:

MIB field name	Reports
eventCurrentService: ipFax(19)	Service ipFax is available for an IP fax call when the event type is callOriginated(1).
eventTrunkGroup (24)	Trunk group used for outgoing calls only. This information is available when the event type is callCleared(9).
eventCalledPartyID	Telephone number dialed for an outgoing call. Currently, the eventCalledPartyID is equivalent to the DNIS Dialed Number ID for an incoming call. On the outgoing call, this field represents the telephone number dialed. This information is available when the event type is callCleared(9).
eventSlotNumber	Slot number at which the call originated. This information is available when the event type is callCleared(3).
eventSlotLineNumber	Line at which the call originated. This information is available when the event type is callCleared(3).
eventSlotChannelNumber	Channel at which the call originated. This information is available when the event type is callCleared(3).
eventTimeStamp	For an IP fax call, the time that the modem is reserved for an outgoing call request. For any other type of call, this field reports the actual connected time. This information is available when the event type is callCleared(3).
eventInOctets	Total received bytes for the call. This information is available when the event type is callCleared(3).
eventOutOctets	Total transmitted bytes for the call. This information is available when the event type is callCleared(3).
eventXmitRate	Negotiated transmitted baud rate used throughout the call. This information is available when the event type is callCleared(3). For IP fax, transmitted and received baud rates are the same.
eventDataRate	Negotiated received baud rate used throughout the call. This information is available when the event type is callCleared(3). For IP fax, transmitted and received baud rates are the same.
eventUserIPAddress	User’s IP address. This information is available when the event type is nameChanged(5).

MIB field name	Reports
eventUserName	Username. This information is available when the event type is callOriginated(1).
eventModemSlotNumber	Slot in which the modem is located. This information is available when the event type is callOriginated(1).
eventModemOnSlot	Modem in use. This information is available when the event type is callOriginated(1).
ssnActiveUserName	Active username.
ssnActiveUserIPAddress	Active user's IP address.
ssnActiveCurrrentService: ipFax(19)	ipFax(19) service is in use for an outgoing IP fax call.

RADIUS support for IP fax operation

The following RADIUS attributes, which appear in Accounting Stop packets, provide outgoing and incoming call values for IP fax calls:

RADIUS attribute	Value
NAS-Port	Shelf, slot, line, and channel number from which the outgoing call originates. The value appears in the following binary format: `FFSS SSLL LLLC CCCC` `FF` specifies the shelf number. `SSSS` specifies the slot number. `LLLLL` specifies the line number. `CCCC` specifies the channel number. Each value is zero-based. For example, given the decimal number 13348, whose binary equivalent is `0011 0100 0010 0100`: `00`=shelf number 1 `1101`=slot number 14 `00001`=line number 2 `0100`=channel number 5
Acct-Session-Time	Total connection time for a call. For an outgoing IP fax call, the time period begins when the modem is reserved, and ends when the call is terminated.
Client-Port-DNIS	Called number for an outgoing call.
Ascend-Modem-PortNo	Modem port used for the call.
Ascend-Modem-SlotNo	Number of the slot in which the modem card is physically located.
Ascend-Modem-ShelfNo	Number of the shelf on which the modem card in located.
Acct-Input-Octets	Total received bytes for the call.
Acct-Output-Octets	Total transmitted bytes for the call.
Ascend-Xmit-Rate	Negotiated transmitted baud rate for the call. For IP fax, transmitted and received baud rates are the same.

RADIUS attribute	Value
Ascend-Data-Rate	Negotiated received baud rate for the call. For IP fax, transmitted and received baud rates are the same.

In addition, the Ascend-CBCP-Trunk-Group attribute (115) applies to outgoing IP fax calls.

Attribute	Value
Ascend-CBCP-Trunk-Group(115)	Assigns the callback or outgoing IP fax call to a TAOS unit trunk group. The value of Ascend-CBCP-Trunk-Group is prepended to the number that the TAOS unit dials for callback or an outgoing fax call. Specify a trunk-group number from `1` to `9`. Ascend-CBCP-Trunk-Group applies only if one or both of the following conditions are true: • Calback Control Protocol (CBCP) is negotiated for a connection. • The call is an outgoing IP fax call and trunk groups are enabled in the System profile.

Syslog support for IP fax operation

The following Syslog message reflects the time at which a modem was reserved:

```
LOG info, Shelf 1, Controller, Time: 15:36:40--
[1/1/13/0] [MBID 13] Assigned to Port
```

The following message displays the dial-out number, trunk group, modem slot, and modem number when a call is placed:

```
LOG info, Shelf 1, Controller, Time: 15:37:07--
[1/1/13/0] [MBID 13; ->97476799] Outgoing Call, 97476799, Trunk 8
```

When the call is connected, its shelf, slot, line, and channel are displayed in the following message:

```
LOG info, Shelf 1, Controller, Time: 15:37:13--
[1/14/2/5] [MBID 13; ->97476799] Call Connected
```

When the call is terminated, the time, modem slot, and modem number are displayed.

```
LOG info, Shelf 1, Controller, Time: 15:38:00--
[1/1/13/0] [MBID 13; ->97476799] Call Terminated
```

Redialer support on MultiDSP slot cards for store-and-forward fax

When a redialer device is attached to a fax machine, it waits for a tone at 400 Hz. After receiving the tone, the redialer transmits the destination fax number to the TAOS unit as DTMF digits. With the current software version, MultiDSP cards transmit the 400-Hz tone and detect incoming DTMF digits.

Short-Duration Transaction Networks (SDTNs)

11

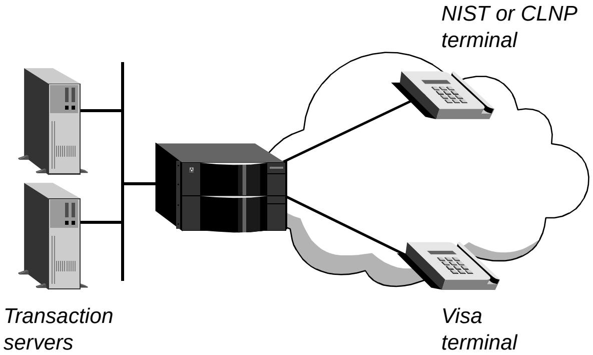
Overview of SDTNs

TAOS units support interaction with transaction servers to conduct short-duration transactions over IP-based networks. SDTN is a feature protected by a special software license. The related parameters might be visible in the command-line interface but are not enabled unless the appropriate software license has been purchased from Lucent Technologies. You can verify that the SDTN license is enabled in your default Transaction-Server profile by entering the following command:

```
admin> get transaction-server enabled
enabled = yes
```

To support short-duration transactions, the TAOS unit receives calls from transaction client applications and transparently forwards them to a transaction server. Figure 11-1 shows a sample SDTN setup, with transaction servers on a local 100-Mbps Ethernet interface.

Figure 11-1. Sample SDTN setup



Transaction data calls come in from National Institute of Standards and Technology (NIST) or Connectionless Network Protocol (CLNP) terminals, or Visa terminals. The TAOS unit answers the calls and forwards them to the transaction server by means of the Quick Transaction Protocol (QTP).

QTP is a symmetrical protocol that operates over UDP in both directions between the TAOS unit and transaction servers. QTP establishes and releases the virtual connection between systems, transports transaction traffic, and exchanges periodic Status Report messages.

To determine which server to use for a particular transaction processing request, the TAOS unit uses a selection table. The system keeps the table up-to-date on server availability and status by applying configurable metrics to information obtained from QTP Status Report messages and from real-time events, such as failure to receive a response to a call request.

Transaction-Server profiles

The Transaction-Server profile sets parameters that affect the metrics used in the server selection table. The table contains a primary and secondary list of transaction servers that have been entered into the list through QTP. A TAOS unit uses only the primary list unless no available servers are left in the primary list, in which case it begins using the secondary list. When a server adds itself to the list, the TAOS unit generates one of the following Syslog messages:

```
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
```

Each list entry specifies a transaction server's IP address, the UDP port used by QTP on that server, and a metric that indicates the server's availability to the TAOS unit. In the current software version, the TAOS unit searches the list in cyclic order and chooses the first available server. (The metric is currently not used to weight the selection. It is used to remove servers from the list when their status or availability crosses a metric threshold. Future software versions will support additional hunt mechanisms.) When the TAOS unit removes itself from the list, it generates one of the following Syslog messages:

```
TS Address [x.x.x.x] has been removed from Primary List
TS Address [x.x.x.x] has been removed from Secondary List
```

The parameter settings in the Transaction-Server profile are used to associate metrics with the events that keep the table up-to-date: QTP Status Report messages, events such as call requests and responses, and periodic receipt of QTP Status Reports. If these events do not occur as expected, the system can change a transaction server metric on that basis.

The QTP Status Report messages from transaction servers can contain the following flow control attributes, indicating how busy the server is:

- Available (0x01)
- Partly Congested (0x02)
- Congested (0x03)
- Shutdown (0x04)

QTP Status Report messages can also contain the Primary Station (0x01) or Secondary Station (0x02) status attribute, indicating whether the server is on the primary or secondary list.

Configuring transaction server settings

The following parameters (shown with default values) are used to configure the metric algorithms and thresholds used for transaction server selection:

```
[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
```

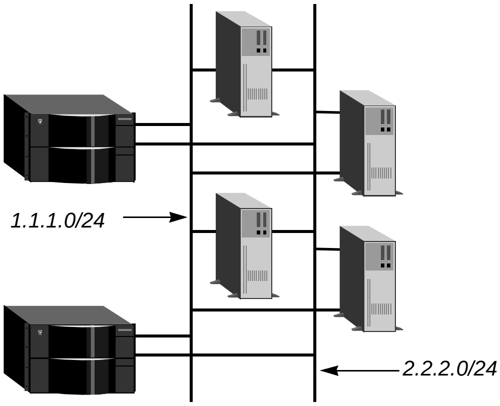
Parameter	**Specifies**
Enabled	Status of the SDTN license (read-only). Set to `yes` when the license is enabled. If this value is No, the license is disabled and this profile has no effect.
Hunting-Mechanism	Method by which to search the Primary list (or Secondary list) of transaction servers. The current software version supports only the `cyclic` setting, which indicates that the list is searched in cyclic order.
Selection-Timeout	Number of milliseconds (from 0 to 65000) before the attempt to establish a QTP connection with a transaction server times out. The default is `10000` milliseconds.
Data-Ack-Timeout	Number of milliseconds (from 500 to 30000) that the TAOS unit waits for a transaction server to send a QTP Acknowledge message in response to a QTP data message. The default is `10000` milliseconds.
Keep-Alive-Timeout	Number of seconds (from 1 to 300) that the TAOS unit waits for a QTP Status update from a transaction server. The default is `30` seconds.
QTP-Port	UDP port for QTP to listen for incoming QTP connections. UDP port numbers can be from 0 to 65535. The default port number for QTP is `3350`.
Metric-Max	Number from 0 to 255 indicating the maximum metric, beyond which a transaction server is removed from an active list. The default maximum metric is 15.
No-Conn-Ack-Increment	Number from 0 to 255 by which to increase a transaction server’s current metric if it does not send a QTP Connect Acknowledgement in response to a QTP Connect Request sent by the TAOS unit. The default setting is `8`.
Call-Reject-Increment	Number from 0 to 255 by which to increase a transaction server’s current metric if it sends a QTP Call Reject message in response to a QTP Connect Request sent by the TAOS unit, to indicate that a QTP connection attempt failed. The default setting is `4`.

Parameter	Specifies
Call-Ack-Decrement	Number from 0 to 255 by which to decrease a transaction server's current metric if it sends a QTP Call Ack message in response to a QTP Connect Request sent by the TAOS, to indicate that a QTP connection attempt succeeded. The default setting is `1`.
Available-Metric	Number from 0 to 255 to use as a transaction server's current metric if it sends a QTP Status Message with a Flow Control Attribute set to Available. The default setting is `1`.
Partly-Congested-Metric	Number from 0 to 255 to use as a transaction server's current metric if it sends a QTP Status Message with a Flow Control Attribute set to Partly-Congested. The default setting is `4`.
Congested-Metric	Number from 0 to 255 to use as a transaction server's current metric if it sends a QTP Status Message with a Flow Control Attribute set to Congested. The default setting is `10`.
Shutdown-Metric	Number from 0 to 255 to use as a transaction server's current metric if it sends a QTP Status Message with a Flow Control Attribute set to Shutdown. The default setting is `14`.
No-First-Status-Metric	Number from 0 to 255 to use as a transaction server's current metric the first time it does not send a QTP Status Message within the timeout interval. The default setting is `10`.
No-Second-Status-Metric	Number from 0 to 255 to use as a transaction server's current metric the second time it does not send a QTP Status Message within the timeout interval. The default setting is `16`.
Max-QTP-PDU-Size	Maximum number of bytes (from 1 to 1460) a QTP message sent by the TAOS unit can contain. The default is `512` bytes.

Example of a transaction server configuration

Figure 11-2 shows a sample SDTN setup with two TAOS units. For redundancy purposes as well as speed of access, each TAOS unit and transaction server supports a 100-Mbps Ethernet interface on two local subnets. Because QTP Status Reports from the transaction servers contain the IP addresses of both Ethernet interfaces on each server, a single server appears as two addressable entities in the server selection table. These connections provide some redundancy if a failure occurs on one subnet or Ethernet port, because the server is still reachable on the other subnet or port.

Figure 11-2. Transaction servers with redundant Ethernet connections



For most sites, the default settings in the Transaction-Server profile are the most effective SDTN setup.

Dial-in connections for transaction clients

A TAOS unit recognizes HDLC-Normal Response Mode (HDLC-NRM) and Visa-II dial-in connections for transaction processing.

Any transaction client connection requires quick handling to avoid timeouts. If the call is made by modem, you can configure a custom AT string that specifies the required modem timings, modulation types, speed, and other modem parameters. This customization helps to prevent delays caused by modem training.

Answer-Defaults profile settings

The Answer-Defaults profile contains two subprofiles for the HDLC-NRM and Visa-II-link-layer encapsulation protocols. Following are the relevant parameters (shown with default settings):

```
[in ANSWER-DEFAULTS:hdlc-nrm-answer]
enabled = yes

[in ANSWER-DEFAULTS:visa2-answer]
enabled = yes
```

By default, the system does not reject HDLC-NRM or Visa-II calls on the basis of their encapsulation types. With the default settings, the system answers the calls if they pass authentication.

For HDLC-NRM and Visa-II connections, CLID or DNIS authentication is required. For example, the following commands configure the unit to require DNIS:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set clid-auth-mode = dnis-require

admin> write
ANSWER-DEFAULTS written
```

Configuring HDLC-NRM connections

TAOS units support HDLC-NRM as a link-layer encapsulation protocol. When it receives an HDLC-NRM call, the system must first authenticate the call through CLID or DNIS. If the call passes authentication, the system answers it, completes HDLC negotiations, and forwards the packets to its QTP software, which encapsulates them in UDP and routes them to a transaction server.

HDLC-NRM is similar to the Link Access Procedure, Balanced (LAPB) protocol and other Layer 2 HDLC protocols. The initial HDLC-NRM packet is an SNRM (Set Normal Response Mode) packet. Unlike LAPB, in which the connected stations are peers and each has the right to send data at any time, HDLC-NRM is a half-duplex protocol, so only one station is allowed to send data at a time. One of the connected stations is the primary station (typically the TAOS unit) and the other is the secondary station (typically the NIST or CLNP terminal). The primary station can send data packets at any time. The secondary station must be polled (through RR) before it can send data packets as synchronous I-frames. By default, the primary station drops data packets it receives from the secondary station when that station has not been given the right to transmit (asynchronous I-frames).

Overview of HDLC-NRM settings

The following parameters (shown with default values) are used to configure HDLC-NRM connections:

```
[in CONNECTION/dgtnt]
encapsulation-protocol = hdlc-nrm
sdtn-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
station-poll-address = 255
```

Parameter	**Specifies**
Encapsulation-Protocol	Encapsulation protocol to use for this connection. This parameter must be set to `hdlc-nrm` for HDLC-NRM clients.
SDTN-Packets-Server	Enable/disable forwarding packets to a transaction server through QTP. Set this parameter to `yes` for HDLC-NRM connections. If the setting is `no` (the default) for an HDLC-NRM connection, the system establishes the connection but drops the data.
Enabled	Enable/disable answering of an HDLC-NRM call that matches this profile.
SNRM-Response-Timeout	Number of milliseconds (50 to 5000) to wait for a response sent in an SNRM (Set Normal Response Mode) packet, which is the initial HDLC-NRM packet sent. The default is `2000`.
SNRM-Retry-Counter	Number of times (from 0 to 255) to retry sending an SNRM packet following a response timeout. The default setting is `2`.
Poll-Timeout	Number of milliseconds (from 0 to 255000) to wait for a response from the caller (the secondary station) to a poll sent by the TAOS unit (the primary station). The default setting is `60000`.
Poll-Rate	Number of milliseconds (from 50 to 5000) between polls. The default setting is `5000`.
Poll-Retry-Count	Number of times (from 1 to 10) to retry the poll after a response timeout. The default setting is `2`.
Primary	Primary or secondary station status of the dial-in unit. The default is `no` because dial-in terminals usually act as secondary stations. Setting this parameter to `yes` causes the TAOS unit to act as the secondary station for this connection (usually for test purposes).

Parameter	Specifies
Async-Drop	Drop asynchronous I-frames received from a secondary station. The primary station must drop such frames, because HDLC-NRM is a half-duplex protocol. When this parameter is set to `yes` (the default) and the TAOS unit is the primary station, the system drops I-frames received from the secondary station. If the parameter is set to `no`, the system processes the I-frames it receives normally. Setting the parameter to `no` enables back-to-back testing on the TAOS unit.
Set Station-Poll-Address	Address used by a TAOS unit in an HDLC-NRM-SNRM packet request to poll a secondary transport protocol data unit (TPDU) station. Specify an integer from 0 through 255. The default is 255, which is the all-stations address. For HDLC-NRM support, `encapsulation-protocol` must be set to `hdlc-nrm` and `sdtn-packets-server` must be set to `yes` in the Connection profile.

A TPDU terminal uses the HDLC-Normal Response Mode (HDLC-NRM) protocol to access an SDTN as follows:

- TPDU terminals use the all-stations HDLC-NRM address as the secondary address.
- The TAOS unit polls the TPDU terminals using its secondary address at link startup.

The value written to this poll address is the value used in the initial Set Normal Response Mode (SNRM) request from the TAOS unit. Thereafter, the HDLC-NRM protocol implementation uses the address returned by the secondary station.

Example of a typical HDLC-NRM client configuration

The following commands create and configure a Connection profile for an HDLC-NRM client:

```
admin> new conn hstation-1
CONNECTION/hstation-1 read

admin> set active = yes

admin> set encapsulation-protocol = hdlc-nrm

admin> set sdtn-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
```

Configuring Visa-II connections

TAOS units support Visa-II as a link layer encapsulation protocol. When it receives a call from a Visa terminal, the system must first authenticate the call via CLID or DNIS. If the call passes authentication, the system answers it and forwards the packets to its QTP software, which routes the packets via UDP to a transaction server.

For Visa-II connections, protocol handling occurs between the transaction server and the Visa terminal. For incoming data from the terminal, the TAOS unit performs some minimal parsing as defined by the Visa-II settings in the caller's Connection profile. For data from the server to the terminal, the TAOS unit simply passes the data transparently.

Overview of Visa-II settings

The following parameters, shown with default values, are used to configure 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
```

Parameter	**Specifies**
Encapsulation-Protocol	Encapsulation protocol to use for this connection. Must be set to `visa2` for Visa terminal connections.
SDTN-Packets-Server	Enable/disable forwarding packets to a transaction server via QTP. Set this parameter to `yes` for Visa terminal connections. If set to `no` (the default) for a Visa terminal connection, the system establishes the connection but drops the data.
Enabled	Enable/disable answering of an Visa-II call that matches this profile.
Idle-Character-Delay	Number of milliseconds of idle time to wait after receiving a character before forwarding data. The range is 0 to 30,000 ms. The default setting is 10,000 ms.
First-Data-Forward-Character	Hexadecimal value of a character to be used as a trigger to forward data. The default setting is 04.
Second-Data-Forward-Character	Hexadecimal value of a character to be used as a trigger to forward data. The default setting is 06.
Third-Data-Forward-Character	Hexadecimal value of a character to be used as a trigger to forward data. The default setting is 15.
Fourth-Data-Forward-Character	Hexadecimal value of a character to be used as a trigger to forward data. The default setting is 05.

Parameter	Specifies
1-Char-Sequence	Hexadecimal value of a character to be used as a trigger to forward data and the next following character. The default setting is 03.
2-Char-Sequence	Hexadecimal value of 2-character sequence to be used as a trigger to forward data and the two characters following the sequence. The default setting is 0x00:0x03. Note that only the first two character values in this sequence have meaning. The last two values are ignored.

Example of a typical Visa-II terminal configuration

The following commands configure a Connection profile for a Visa terminal or terminal emulator:

```
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
```

Preventing training delays for modem transaction calls

When a transaction call is initiated or answered by a modem, the TAOS unit must train the modem before establishing the connection. To enable dial-in terminals for transaction processing to connect quickly with as little modem training as possible, you can specify an AT string that sets the required modem timings, modulation types, speed, and other modem parameters. This customization helps to prevent delays caused by modem training.

Parameter for customizing the AT string

To specify an AT string, set the following parameter (shown with its default value):

```
[in CONNECTION/""]
at-string = ""
```

With the default "null" value, the system performs modem training as usual. The value of this parameter can be set to valid AT commands of up to 58 characters.

Note: Do not begin the string with AT. An AT is automatically appended to the beginning of this string before it is sent to the modem. Also, do not include an A (answer) or a D (dial) command anywhere in the string. An A command is automatically appended this string for incoming calls, and a D command in the answer string causes the call to fail. A D command is automatically appended to the specified string for outgoing calls. Also, be very careful when entering AT commands in this parameter. The system does not prevent you from entering incorrect strings.

Example of a customized AT string

The following commands configure an HDLC-NRM connection and set the AT-String to force the modem to answer as a Bell 212A type modem:

```
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
```

The sample AT-String setting causes the following string to be sent to the modem, forcing it to answer as a Bell 212A type modem in automode:

```
ATB1+MS=69,1,1200,1200;
```

Authentication Methods

A

Authentication overview

Authentication is the first line of defense against unauthorized access to your network. It uses an exchange of information to verify the identity of a user. The information is usually encrypted at both ends.

In determining which type of authentication to use, you should consider whether the call is between two machines or between a human being and a machine, and then decide how strong the authentication mechanism must be.

For example, if the connection is negotiated between two machines, you should consider whether the other location is trusted, whether that machine protects its own networks against security attacks, and whether it is physically accessible to many users.

If the connection is negotiated with a user who must type in a token or password, you should consider how secure the password is and how frequently you want it to change. Once the user’s connection is authenticated, you can use authorization restrictions to prevent the caller from accessing systems or networks you want to protect. (For details about authorization options, see Appendix B, “Authorization Options.”)

Password authentication for framed protocol sessions

For framed protocol sessions, the authentication process is typically handled by access protocols such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft’s extension of CHAP (MS-CHAP). All of the available authentication protocols except PAP include password encryption. Password encryption protects against passive attacks, in which an unauthorized user monitors information being transmitted, with the intent to use the information to establish what appears to be a valid session.

Authentication of terminal-server logins

For login sessions, in which users dial in to the terminal-server software to access local hosts, administrators often set up Expect-Send scripts to automate the process of prompting for and receiving a name and password. For RADIUS-authenticated login sessions, you can make use of password expiration as an added security measure.

Token card password authentication

The most secure password authentication uses token cards to overcome the limitations of static passwords. Token cards protect against both passive attacks and replay attacks, in which an unauthorized user records valid authentication information exchanged between systems and then replays it later to gain entry. Because token cards provide one-time-only passwords, the password changes many times a day, making replay impossible.

Preauthentication through call information

Calling-Line ID (CLID) and Dial Number Information Service (DNIS) are information elements that can be provided as part of the call by the telco switch. You can use these elements to verify the calling number and dialed number, respectively, before the TAOS unit answers the call.

Using callback for added security

After authentication is complete, the TAOS unit can hang up and call back, ensuring that the connection is made only with a trusted number.

RADIUS password handling

For detailed information about RADIUS, see the *TAOS RADIUS Guide and Reference*.

RADIUS user entries are composed of three parts:

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

The User-Name must be left justified. It is typically the name of the caller (or calling device), but it can also be a telephone number (for CLID or DNIS authentication), a special string indicating a pseudo-user profile, or the string `DEFAULT` (for the default user profile).

Check-Items must be on the same line as the User-Name, and must be separated by white space (space or tab) from the User-Name. Check-Items includes zero or more attribute-value pairs that must match the attributes that are present in the Access-Request packet for the user to be authenticated. Check-Items typically include the password for the entry.

Reply-Items must be indented and separated from the User-Name and Check-Items by a newline. If a Reply-Item is not indented, it is interpreted as the User-Name of a new entry. Reply-Items includes zero or more attribute-value pairs that are returned in Access-Accept messages to authorize services for the user.

Reserved RADIUS passwords

RADIUS servers can reserve certain values of the Password (2) attribute for specific uses. For example, some servers interpret the password `UNIX` as an instruction to use UNIX authentication for the profile. Some RADIUS servers use the passwords `ACE` and `SAFEWORD` to request validation from a Security Dynamics ACE/Server and an Enigma Logic SafeWord server, respectively (see "Token-card authentication" on page A-25).

TAOS reserves the following values for the Password (2) attribute:

Password values	Description
`Ascend`	Used for pseudo-user and other system profiles. When this password is in use, the Service-Type attribute should always specify Outbound-User, to prevent callers from accessing the network by using a well-known password. *Although the system does not reject a profile that does not include the Outbound-User setting, omitting the setting introduces a serious security risk.*

`Ascend-CLID`
or
`Ascend-DNIS`
	Specifies the use of CLID or DNIS information, respectively, to preauthenticate calls. When either of these passwords is in use, the Service-Type attribute should always specify Outbound-User, to prevent callers from accessing the network by using a well-known password. *Although the system does not reject a profile that does not include the Outbound-User setting, omitting it introduces a serious security risk.*

Password expiration

Many RADIUS servers support password aging and expiration, and provide a method for enabling users who dial in to the terminal server to replace expired passwords. Password expiration does not work for passwords that are not stored in the RADIUS database (UNIX-authenticated or token-card passwords), or for reserved passwords (such as `Ascend`).

TAOS uses the following attribute-value pairs to support password aging and expiration:

RADIUS Attribute	Value
Ascend-PW-Expiration (21)	Expiration date for the user's password (a date consisting of a month, day, and year specification.) The value can be updated automatically when a user renews a password. Must be a Check-Item.

RADIUS Attribute	Value
Ascend-PW-Lifetime (208)	Number of days a password can be valid (an integer from 0 to 65535). The default of 0 (zero) disables password expiration. If the attribute is set to a nonzero value, when the user changes the password, the TAOS unit adds the value to the current date and updates the Ascend-PW-Expiration date. This routine provides a method of specifying new expiration dates automatically rather than hard-coding a date.
Ascend-PW-Warntime (207)	Number of days a user will be warned that his or her password is about to expire (an integer from 0 to 65535).

Following is a sample profile whose password expires on January 1, 2001:

```
brian Password = “localpw”, Ascend-PW-Expiration = “Jan. 1, 2001"
   Ascend-PW-Lifetime = 30,
   Ascend-PW-Warntime = 2,
```

A user dialing in on December 30, 1998, receives a message that the password will expire in two days. If the user changes the password at that time (by using the terminal-server Password command in the terminal server), the RADIUS server updates the password, adds 30 days to the current date, and updates the Ascend-PW-Expiration date to January 29, 2001.

A user dialing in on January 1, 2001, receives a message that the password has expired, and is prompted to enter both the expired password and a new one. The system prompts twice for the new password to verify the entry. If the user enters the information incorrectly, the system displays another prompt and the user can try again, for a total of up to three attempts.

If the update is successful, the system sends the new password to the RADIUS server and displays the following message, immediately followed by the terminal-server prompt:

```
Password Updated

ascend%
```

If the update fails for any reason, the following message appears:

```
Password NOT Changed
```

There is no indication of why the password change failed. The RADIUS server can reject the password change for any of the following reasons:

- The file system containing the RADIUS `users` file is full.
- The RADIUS `users` file is locked against writing.
- The user’s password is stored in UNIX.

DEFAULT user profile

A special user profile named `DEFAULT` can be placed at the end of the `users` file to specify what to do with users who do not have a profile in the `users` file. Only one `DEFAULT` entry is allowed, and it must be the last entry in the file. For example, the following entry allows terminal-server users to log in with their UNIX account name and password:

```
DEFAULT Password = "UNIX"
   Service-Type = Login-User,
   Login-Service = Telnet
```

Shared secrets and secure exchanges

A shared secret is used to authenticate packets exchanged between the TAOS unit and the RADIUS server, and to encrypt passwords from dial-in callers before sending them across the local network. A shared secret is a single value known to both systems.

On the RADIUS server, shared secrets are specified in the `clients` file. For example, for a system named TAOS-01, the following entry in the `clients` file specifies a shared secret of `nas-secret`:

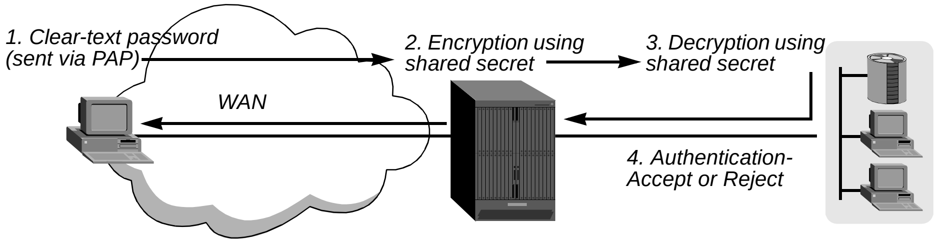
```
TAOS-01 nas-secret
```

The TAOS unit specifies the same shared-secret string as the value of the Auth-Key parameter in the External-Auth profile. For example:

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

admin> set rad-auth-client auth-key = nas-secret

admin> write
EXTERNAL-AUTH written
```

Figure A-1 shows a basic example of how passwords presented by incoming calls are handled between the systems.

Figure A-1. Shared secret used between a TAOS unit and a RADIUS server


1. Clear-text password (sent via PAP)
2. Encryption using shared secret
3. Decryption using shared secret
WAN
4. Authentication-Accept or Reject

The TAOS unit uses the shared secret to encrypt the password from the dial-in call before the unit sends the password across the local network to a RADIUS server. The encryption makes use of the shared secret, the Authenticator field, and an encoding method, such as MD5, CHAP, or DES.

For dial-out calls, the RADIUS server sends the far-end password to the Network Access Server (NAS). The RADIUS server must encrypt passwords before sending them to the NAS if the dial-out profile uses the Ascend-Send-Secret (214) attribute to specify the password. If the profile specifies a value for Ascend-Send-Secret and the RADIUS server does not encrypt the password, authentication fails.

If the dial-out profile uses the Ascend-Send-Passwd (232) attribute to specify the password instead, the RADIUS server performs no encryption before sending the password to the NAS. This setting might be required if you are using a RADIUS server that does not support outbound password encryption.

Unless you are using a RADIUS server that does not support Ascend-Send-Secret, the use of this attribute is recommended in place of Ascend-Send-Passwd to protect against local sniffers detecting dial-out passwords.

Authenticating framed protocol sessions

During establishment of a PPP data link, the dialing and answering units use Link Control Protocol (LCP) packets to negotiate the authentication protocol. After completing LCP negotiations, the TAOS unit uses the agreed-upon authentication protocol to authenticate the user. It then negotiates the upper layer Network Control Protocols (NCPs) to set up the link's network-layer protocols.

If the link is configured to require authentication, the units at the two ends of the link negotiate an authentication protocol. The answering unit always determines which authentication method to use for the call. A multilink connection begins with authentication of a base channel, and subsequent channels are authenticated separately when they are added to the call.

Specifying an authentication protocol required for dial-in calls

To specify an authentication protocol to be required for name and password authentication of framed sessions, you must set the following parameter (shown with its default setting):

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

Parameter	**Specifies**
Receive-Auth-Mode	Authentication protocol required for authentication of inbound calls. Valid values are No-PPP-Auth (the default), PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, and Any-PPP-Auth.

The Receive-Auth-Mode parameter typically specifies a general setting to support the widest range of authentication protocols. For example:

```
admin> read answer
ANSWER-DEFAULTS read

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

admin> write
ANSWER-DEFAULTS written
```

If you set this parameter to a value other than the default of No-PPP-Auth, the TAOS unit uses LCP to request certain authentication options, and the caller must accept one of the options the system offers. With the default setting, the TAOS unit does not request authentication.

PAP-PPP-Auth specifies the Password Authentication Protocol (PAP), which provides a simple method for the TAOS unit to establish its identity in a two-way handshake. The remote device must support PAP.

CHAP-PPP-Auth specifies the Challenge Handshake Authentication Protocol (CHAP), which is more secure than PAP. When the TAOS unit is using CHAP to authenticate the remote device, the system can periodically verify the identity of the remote device by means of a three-way handshake and encryption. The remote device must support CHAP.

MS-CHAP-PPP-Auth specifies the Microsoft extension of CHAP, which uses DES and MD4 encryption. It is used primarily by Windows NT and LAN Manager systems.

Any-PPP-Auth specifies that any authentication protocol is acceptable. The TAOS unit accepts incoming PPP calls that support any of the authentication methods, but it drops connections that do not accept any authentication protocols during LCP negotiation.

Specifying an authentication protocol with RADIUS

You can also use the Ascend-Auth-Type (81) vendor-specific attribute (VSA) in a RADIUS user profile to specify the type of PPP authentication to use, overriding the Answer-Defaults specification.

Some customers and providers who buy access from ISPs want to use CHAP authentication for their PPP calls, while other customers want to use PAP. In most cases, making both PAP and CHAP available to customers presents no problem. However, customers that use Microsoft Windows 95, Windows 98, or Windows NT clients cannot configure their units to reject CHAP. When Receive-Auth-Mode is set to `any-ppp-auth`, the TAOS unit offers CHAP authentication before PAP. Therefore, the Windows clients always use CHAP, but you can configure RADIUS to select a different type of PPP authentication.

The Ascend-Auth-Type attribute is returned as part of the authorization resulting from DNIS or CLID first-tier authentication. If you specify a value for Ascend-Auth-Type, it overrides the Receive-Auth-Mode setting in the Answer-Defaults profile.

RADIUS Attribute	Value
Ascend-Auth-Type (81)	Specifies the type of PPP authentication the connection uses during first-tier CLID or DNIS authentication. Specify one of the following values: • Auth-None (0)— No second-tier name and password authentication is required. Specifying this value has the same effect as setting Ascend-Require-Auth to Not-Require-Auth. • Auth-Default (1)—The connection uses the Receive-Auth-Mode setting. • Auth-Any (2)—The connection must use PAP, CHAP or MS-CHAP. • Auth-PAP (3)—The connection must use PAP. The remote end sends its password in the clear. The password is not encrypted. • Auth-CHAP (4)—The connection must use CHAP. The remote end does not send its password in the clear. A Message Digest Algorithm 5 (MD5) digest, calculated from the password, and a random challenge are sent instead. • Auth-MS-CHAP (5)—The connection must use MS-CHAP. If values other than those described above are passed from RADIUS to the TAOS unit, the TAOS unit uses the Answer-Defaults profile settings (if the Use-Answer-For-All-Defaults parameter in the Answer-Defaults profile is set to Yes) or the factory default (if the Use-Answer-For-All-Defaults parameter is set to No).

Requiring no authentication from asynchronous framed users

You can configure a TAOS unit to require no user authentication for incoming calls from asynchronous framed users during LCP negotiation, while continuing to restrict access to other types of users. The TAOS unit assigns users (that are not authenticated) to an IP address pool reserved only for their sole use. In addition, a user who fails Password Authentication Protocol (PAP) authentication for the network connection can attempt the connection again up to five times. Consider allowing users to retry PAP authentication after failures by setting the Max-Pap-Auth-Retry parameter.

Parameter	Specifies
Answer-Defaults > PPP-Options > Auth-for-Async-Framed-User	Enable/disable the authentication requirement for incoming asynchronous framed users. Specify one of the following values: • Not-Required—Disables the authentication requirement. You must assign a pool number in the Pool-for-Async-Framed-User parameter to provide IP addresses for incoming asynchronous framed users without authentication. • Required (the default)—Enables the authentication requirement for incoming asynchronous framed users. A read-only copy of this parameter appears in the IP-Options subprofile.
Answer-Defaults >IP-Options > Pool-for-Async-Framed-User	An IP address pool number assigned to incoming asynchronous framed users without authentication. Because this pool is for the sole use of asynchronous framed users without authentication, the TAOS unit does allocate an IP address from this same pool to incoming users *with* authentication. Specify an integer from 0 to 512.
Answer-Defaults > PPP-Answer > Max-Pap-Auth-Retry	Maximum number of retries allowed if PAP authentication for network connection fails. Specify a number between 0 and 5. The default is 0 retries. A read-only copy of this parameter appears in the IP-Options subprofile.

To implement this feature, configure the TAOS unit as follows:

```
[in ANSWER-DEFAULTS:ppp-answer]
admin> set auth-for-async-framed-users = not-required
admin> set max-pap-retry = 1

[in ANSWER-DEFAULTS:ip-answer]
admin> set pool-for-async-framed-user = 1
admin> write
ANSWER-DEFAULTS written
```

How PAP works

PAP is a two-way handshake method of establishing a caller's identity. Used only once, during the initial establishment of the data link, it is not a strong authentication method. Passwords are sent as plain text across the WAN, so eavesdroppers with the proper equipment and software could potentially detect and reuse correct passwords.

PAP authentication is typically used because the available password method or database requires it. For example, if the UNIX password file is used to authenticate (via RADIUS), the TAOS unit forces the peer to use PAP.

When PAP is used with RADIUS authentication, the TAOS unit uses the shared secret to encrypt the text password it receives from the caller before sending the password across the network to the server. The RADIUS server uses the same shared secret to decrypt the password before performing authentication or passing it to another authentication server, such as a UNIX host or token-card server.

How CHAP and MS-CHAP work

CHAP authentication verifies the caller's identity by using a three-way handshake upon initial link establishment and possibly repeating the handshake any number of times. The authenticator sends a challenge to the caller, which responds with an MD5 digest calculated from the password. The authenticator then checks the digest against its own calculation of the expected hash value to authenticate the call. A new challenge can be sent at random intervals.

CHAP is a stronger authentication method than PAP, because the password is not sent as plain text. In addition, the use of repeated challenges limits the time of exposure to any single attempt to break the encryption code, and the authenticator is in control of how often and when challenges are sent.

Microsoft CHAP (MS-CHAP) is a close derivative of CHAP. However, CHAP is designed to authenticate WAN-aware secure software. It is not widely used to support remote workstations. Such use might require insecure plain text login. MS-CHAP addresses this issue, and also integrates the encryption and hashing algorithms used on Windows networks. Microsoft Windows NT and LAN Manager platforms implement MS-CHAP.

MS-CHAP authentication is supported in local Connection profiles or in RADIUS profiles. The current software version provides a key for DES encryption of passwords when MS-CHAP authentication is used. No parameters are required in local profiles.

When CHAP or MS-CHAP is used with RADIUS authentication, the following events occur:

1. The TAOS unit sends a random, 128-bit challenge to the calling unit.
2. The calling unit calculates an MD5 digest by means of its password, the challenge, and the PPP packet ID.
3. The calling unit sends the MD5 digest, the challenge, and the PPP packet ID (but not the password) to the TAOS unit. The TAOS unit never has the caller's password.
4. The TAOS unit forwards the digest, along with the original challenge and PPP packet ID, to the RADIUS server. No encryption is necessary, because MD5 creates a one-way code that cannot be decoded.

5 The RADIUS server looks up the caller’s password in a local database and calculates an MD5 digest that is based on the local version of the remote secret, the challenge, and the PPP packet ID received from the TAOS unit.

6 The RADIUS server compares the calculated MD5 digest with the digest it received from the TAOS unit. If the digests are the same, the passwords matched, and the call is accepted.

How bidirectional CHAP works

Bidirectional CHAP between the calling PPP device and the called PPP device increases compliance with the RFC 1994 standard for PPP CHAP authentication. Note that the feature is not implemented for PAP-based authentication (PAP, PAP-TOKEN, or PAP-TOKEN-CHAP).

Note: As noted in RFC 1994, a security hole can occur when you use bidirectional authentication for an incoming call if the secrets used in both directions are identical. Bidirectional authentication in TAOS has been developed to avoid the security hole, even if the secrets are identical. For best results, however, Lucent Technologies recommends that you specify a different secret for each authentication direction.

Bidirectional CHAP is supported locally and through RADIUS.

Configuring bidirectional CHAP on a TAOS unit

The following sections describe how to configure bidirectional CHAP in local profiles. You can choose one or more of the following configurations:

- Setting up bidirectional CHAP for all incoming calls
- Setting up bidirectional CHAP for selected incoming calls
- Setting a CHAP challenge name for incoming calls
- Setting up bidirectional CHAP for outgoing calls

All the configurations involve setting the Bi-Directional-Auth parameter in the Answer-Defaults > PPP-Options profile and/or in Connection > PPP-Options profiles, to specify whether CHAP authentication must be bidirectional. Specify one of the following values:

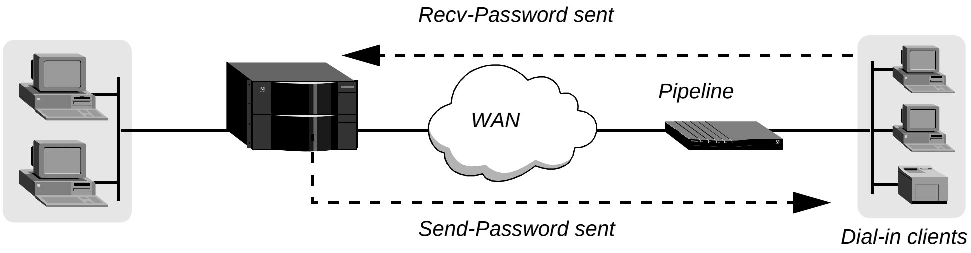
- None—authentication is unidirectional. The called device identifies the calling one. The TAOS unit prevents the authentication in which the calling party identifies the called party. This is the default.
- Allowed—authentication can be bidirectional. When the TAOS unit is the called device, it identifies the calling device. The system also allows the calling device to authenticate the TAOS unit, but this authentication is not mandatory. Therefore, if the calling device does not authenticate the TAOS unit, the TAOS unit can still accept the call.

  When the TAOS unit is the calling device, it answers the authentication initiated by the called device. The TAOS unit tries to negotiate authentication in the opposite direction as well, but if the called device refuses this second authentication option, the call is still established.
- Required—authentication must be bidirectional. The TAOS unit requires that both the calling and called devices authenticate each other. If authentication is not performed in both directions, the TAOS unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).

Setting up bidirectional CHAP for all incoming calls

Figure A-2 shows a configuration in which a TAOS unit and its dial-in clients authenticate each other by means of bidirectional CHAP. One or more clients can dial into the TAOS unit. The TAOS unit authenticates each calling device by means of a Connection profile, and each dial-in client authenticates the TAOS unit by means of the Send-Password value.

Figure A-2. Bidirectional CHAP for all incoming calls to a TAOS unit



To configure bidirectional CHAP on a TAOS unit for all incoming calls, proceed as follows:

1 Make Answer-Defaults the working profile.

2 List the PPP-Answer subprofile.

3 Set Receive-Auth-Mode to `any-ppp-auth` or `chap-ppp-auth`.

4 Set Bi-Directional-Auth to `required` or `allowed`. Required specifies that bidirectional authentication must be carried out or the call is dropped. Allowed specifies that authentication *can* be bidirectional. The TAOS unit identifies the calling device, and the calling device can identify the TAOS unit, but the calling device need not do so for the call to be accepted.

5 Write the Answer-Defaults profile.

6 For each incoming call, create or read a Connection profile, and make it the working profile.

7 List the PPP-Options subprofile.

8 Set Send-Password to any text string. The password you specify is the one sent to the calling unit during the authentication initiated by the calling unit.

9 Set Recv-Password to any text string. The password you specify is the one sent by the calling unit during the authentication initiated by the TAOS unit.

10 Write the Connection profile.

Note: When the Receive-Auth-Mode parameter is set to `any-ppp-auth`, the TAOS unit can accept both Password Authentication Protocol (PAP) and CHAP authentication. The Bi-Directional-Auth setting is used only if a form of CHAP authentication has been negotiated during Link Control Protocol (LCP) negotiation. If any form of PAP authentication has been negotiated, and Bi-Directional-Auth is set to `required`, the TAOS unit authenticates the calling unit, and authentication takes place in one direction only.

Following is a partial example of configuring bidirectional CHAP for all incoming calls:

```
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
```

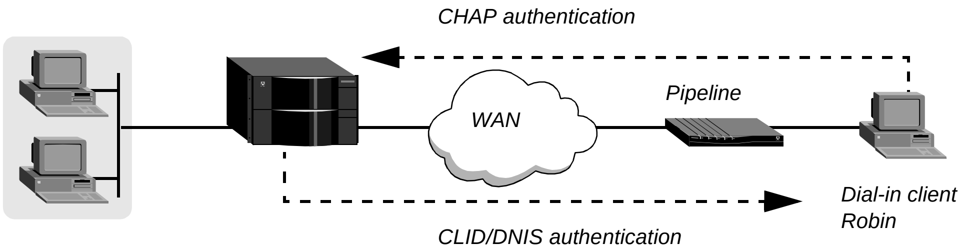
```
admin> set ppp-options recv-password = recvpw
```

```
admin> write
CONNECTION/robin written
```

Setting up bidirectional CHAP for selected incoming calls

Figure A-3 shows a configuration in which the TAOS unit authenticates the calling device by means of Calling Line ID (CLID) or Dialed Number Information Service (DNIS) authentication. The dial-in client and the TAOS unit then authenticate each other by means of CHAP.

Figure A-3. Bidirectional CHAP for selected calls



To configure bidirectional CHAP on the TAOS unit for selected incoming calls, proceed as follows:

1 Make Answer-Defaults the working profile.

2 Set Profiles-Required to `yes`.

3 Set CLID-Auth-Mode to `clid-require`, `clid-prefer`, `dnis-require`, or `dnis-prefer`.

4 List the PPP-Answer subprofile.

5 Set Bi-Directional-Auth to `none` or `allowed`.

6 Write the Answer-Defaults profile.

7 Select or create the Connection profile for which you want to set up bidirectional CHAP, and make it the working profile.

8 If CLID-Auth-Mode is set to `clid-require` or `clid-prefer`, set the CLID value to the calling device’s telephone number.

9 If CLID-Auth-Mode is set to `dnis-require` or `dnis-prefer`, set the CalledNumber value to the number the calling party dials.

10 List the PPP-Options subprofile.

11 Set Send-Password to any text string. The password you specify is the one sent to the calling unit during the authentication initiated by the calling unit.

12 Set Recv-Password to any text string. The password you specify is the one sent by the calling unit during the authentication initiated by the TAOS unit.

13 Set Send-Auth-Mode to `chap-ppp-auth`. This value indicates the mode for both incoming and outgoing authentication.

14 Set Bi-Directional-Auth to `required` or `allowed`. Required specifies that bidirectional authentication must be carried out or the call is dropped. Allowed specifies that authentication *can* be bidirectional. The TAOS unit identifies the calling device, and the calling device can identify the TAOS unit, but the calling device need not do so for the call to be accepted.

15 Write the Connection profile.

Following is an example of configuring bidirectional CHAP for selected incoming calls:

```
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
```

Setting a CHAP challenge name for incoming calls

You can specify a CHAP challenge name for bidirectional CHAP authentication of incoming calls by setting the Substitute-Send-Name parameter in the PPP-Answer subprofile of the Connection profile. The Substitute-Send-Name parameter is a unique, substitute name for the calling host to which the TAOS unit connects during incoming calls.

Because bidirectional CHAP authentication provides a way to formally authenticate the calling device during an incoming call, the name of the device must be checked against a locally defined name. The name can be the dial-in profile name or the substituted name provided by the Substitute-Send-Name parameter. Following are the relevant settings for configuring the unit to use the CHAP challenge name:

```
[in ANSWER-DEFAULTS:ppp-answer]

admin> set substitute-send-name = groupb

admin> write
ANSWER-DEFAULTS written
```

Parameter	Specifies
`substitute-send-name`	Name of the PPP calling device during incoming calls to the TAOS unit, a string of up to 23 characters. The default is a null string. If no value is entered, the global system name is used. The PPP-Options subprofile in the Connection profile includes a copy of this setting.

Setting up bidirectional CHAP for outgoing calls

In addition to setting the Bi-Directional-Auth parameter, you must set the Substitute-Recv-Name parameter in PPP-Options subprofile to identify the PPP called device's name during outgoing calls. Because bidirectional authentication provides a way to formally authenticate the called device during an outgoing call, the name of the device must be checked against a locally defined name. The name can be the dial-out profile name or a substituted name. Specify a string of up to 23 characters. The default is null.

To set up bidirectional CHAP on the TAOS unit for outgoing calls, proceed as follows:

1 Make the Connection profile the working profile.

2 List the PPP-Options subprofile.

3 Set Send-Auth-Mode to `chap-ppp-auth`, `cache-token-ppp-auth`, or `ms-chap-ppp-auth`. If you specify any other authentication mode, bidirectional authentication does not take place, even if Bi-Directional-Auth is set to `allowed` or `required`.

4 Set Bi-Directional-Auth to `required` or `allowed`. Required specifies that bidirectional authentication must be carried out or the call is dropped. Allowed specifies that authentication *can* be bidirectional. The TAOS unit identifies the called device if the called device accepts the authentication. The called device can identify the TAOS unit, but the called device need not do so for the call to be accepted.

5 Set Send-Password to a text string specifying the password sent to the called device during the authentication initiated by the TAOS unit.

6 Set Recv-Password to a text string specifying the password sent by the called unit during the authentication initiated by the called unit.

7 Set Substitute-Recv-Name to a text string. The called party's name is compared against the value you specify. If the called party's name is different, the call is not established. If you do not specify a value for Substitute-Recv-Name, the called party's name is compared against the dial-out profile name.

8 Write the Connection profile.

Following is a sample configuring bidirectional CHAP for outgoing calls:

```
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

admin> set ppp-options recv-password = recvpw

admin> set ppp-options substitute-recv-name = subname
admin> write
CONNECTION/robin written
```

Configuring bidirectional CHAP in RADIUS

The following sections describe how to configure bidirectional CHAP in RADIUS. You can use one of the following configurations:

- Setting up bidirectional CHAP in RADIUS for incoming calls
- Setting up bidirectional CHAP in RADIUS for outgoing calls
- Setting up selective bidirectional CHAP with callback
- Setting up an outgoing call with double RADIUS lookups

Setting up bidirectional CHAP in RADIUS for incoming calls

You can configure selective bidirectional authentication by using CLID or DNIS preauthentication in a pseudo-user profile and then specifying two passwords in the user profile.

In the pseudo-user profile, specify CLID or DNIS authentication and then set the Ascend-Bi-Directional-Auth attribute to Bi-Directional-Auth-Allowed or Bi-Directional-Auth-Required:

- Bi-Directional-Auth-Allowed specifies that authentication can be bidirectional. The TAOS unit identifies the calling device. The system also allows the calling device to authenticate the TAOS unit, but this authentication is not mandatory. Therefore, if the calling device does not authenticate the TAOS unit, the TAOS unit can still accept the call.
- Bi-Directional-Auth-Required specifies that authentication must be bidirectional.

In the following pseudo-user profile, bidirectional authentication is required:

```
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
```

In the user profile, Ascend-Send-Secret is set to the password sent to the called device during the authentication initiated by the TAOS unit:

```
Mike1 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
```

Note that the Answer-Defaults profile must contain the desired bidirectional authentication mode (`none`, `required`, or `allowed`) if CLID or DNIS preauthentication is not in use. The pseudo-user profile can be suppressed (unused), and the user profile must contain the Ascend-Bi-Directional-Auth attribute.

Setting up bidirectional CHAP in RADIUS for outgoing calls

To configure a RADIUS dial-out profile that makes use of bidirectional authentication, proceed as follows:

1 Set User-Name to the name of the called party, and set Password to to specify the password that the user must provide.

2 Set Ascend-Send-Auth to `send-auth-chap.`

3 Set Ascend-Send-Secret to the text of the secret sent to the called device.

4 Set Ascend-Receive Secret to the text of the secret received from the called device.

5 Set Ascend-Bi-Directional-Auth to `bi-directional-auth-allowed` or `bi-directional-auth-required.`

6 Set Ascend-Recv-Name to the name of the called party.

For example:

```
Mike1-out Password = "ascend"
     Service-Type = Outbound,
     User-Name = "Mike1",
     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 Mike1-out"
```

Setting up selective bidirectional CHAP with callback

To configure bidirectional CHAP with callback, you must carry out the following steps:

- Create a first-tier pseudo-user profile.
- Create a second-tier user profile.

In the first-tier pseudo-user profile, proceed as follows:

1 Set User-Name to the name of the called party, and Password to specify the password that the user must provide.

2 Set Ascend-Require-Auth to `require-auth`.

3 Set Ascend-Send-Auth to `send-auth-chap.`

4 Set Ascend-Bi-Directional-Auth to `bi-directional-auth-allowed` or `bi-directional-auth-required.`

For a global bidirectional CHAP callback, the first-tier pseudo-user profile is not used. In the second-tier user profile, proceed as follows:

1. Set Ascend-Send-Auth to `send-auth-chap`.
2. Set Ascend-Bi-Directional-Auth to `bi-directional-auth-allowed` or `bi-directional-auth-required`.
3. Set Ascend-Callback to `callback-yes`.

The following example shows the configuration required for callback. In the first-tier pseudo-user profile, bidirectional authentication is selectively determined during DNIS preauthentication, and the system performs bidirectional authentication for both incoming and outgoing calls. The second-tier user profile is configured for bidirectional CHAP with callback.

```
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

Mike1_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
```

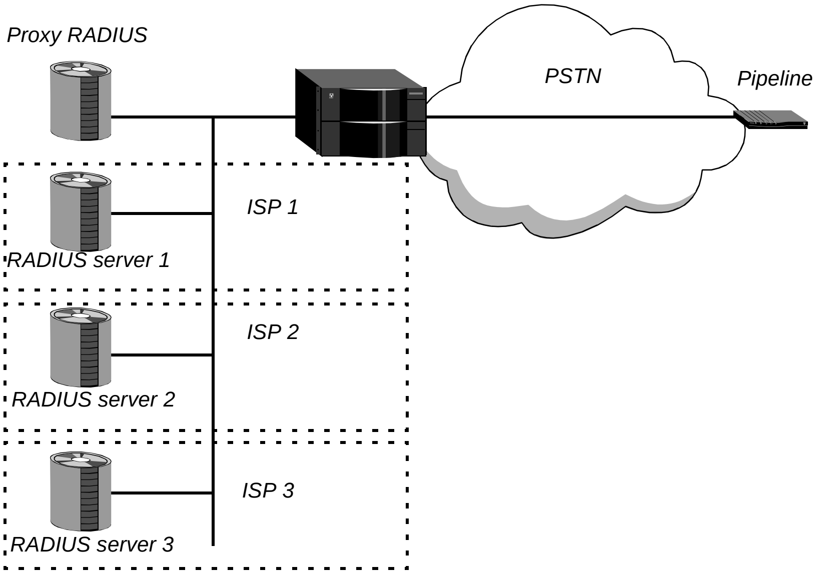
Setting up an outgoing call with double RADIUS lookups

This section discusses the following topics:

- The circumstances under which you might use double RADIUS lookups
- The procedure for setting up RADIUS lookups
- The message sequence during RADIUS lookups

In larger networks, several ISPs might be hosted on a single physical network, such as the one shown in Figure A-4. Each ISP typically has its own RADIUS server, while the network provider uses a proxy RADIUS server. The TAOS unit interacts only with the proxy RADIUS server. The proxy server can answer some requests locally and forward other requests to the RADIUS server of an ISP. Typically, an ISP requires that all of its users be authenticated by its own RADIUS server, and not by the network provider’s equipment.

Figure A-4. Bidirectional CHAP in a multiprovider network



During an outgoing call with bidirectional authentication, the TAOS unit first recovers the dial-out profile. Once the call is brought up, the TAOS unit must authenticate the called party, in this case, a Pipeline unit. The authentication decision must be made by the ISP's RADIUS server, requiring a second RADIUS lookup.

When you set up double RADIUS lookups, the dial-out profile is split into two profiles—the first-tier dial-out profile and the second-tier user profile. The dial-out profile contains all dialout parameters needed to establish the outgoing call, and the user profile contains information for authenticating the called device.

Consider the following first-tier dial-out profile, configured for bidirectional CHAP authentication:

```
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
```

To enforce the second RADIUS lookup, the dial-out profile name (`pipe-pat-out` in this example) must be different from the name of the called device in the user profile. The Ascend-Recv-Name attribute specifies the name of the called device, in this case `pipe-pat`.

In the following second-tier user profile, the called party's name is `pipe-pat` and the receive-password is `pass`.

```
pipe-pat Password = "pass"
     Service-Type = Framed,
     Ascend-Route-IP = 1"
```

You can disable the double RADIUS lookup by naming the dial-out profile with the peer's name and by omitting the Ascend-Recv-Name attribute. Use the User-Name attribute to rename the profile (in this case to `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
```

A call using two RADIUS lookups passes through the following messaging sequence:

1. The TAOS unit requests a dial-out profile from RADIUS.
2. RADIUS sends the dial-out profile to the TAOS unit.
3. The TAOS unit makes an ISDN call to the remote device.
4. The ISDN call is connected.
5. The TAOS unit and the called party perform LCP exchanges.
6. The called party sends a challenge request to the TAOS unit.
7. The TAOS unit responds with a challenge response.
8. The called party informs the TAOS unit about whether the first level of authentication has been successful.
9. If the first authentication was successful, the TAOS unit sends a challenge request to the called party.
10. The called party responds with a challenge response.
11. The TAOS unit sends the authentication request to RADIUS, which performs the second lookup.
12. The RADIUS server informs the TAOS unit about whether the authentication was successful.
13. If the authentication was successful, the TAOS unit informs the called party that it has been authenticated.

RADIUS uses the following attribute-value pairs for bidirectional CHAP configuration. (For additional information about these attributes, see the *TAOS RADIUS Guide and Reference*.)

RADIUS Attribute	Value
Ascend-Bi-Directional-Auth (46)	Specifies whether CHAP authentication must be bidirectional.
Ascend-Recv-Name (45)	Name of the PPP called device that is compared against a locally defined name. Can be the dial-out profile name or a substituted name.

Requesting a protocol for use in dial-out calls

Connection profiles and dial-out RADIUS profiles can specify the authentication protocol and password used to send authentication information to the far end.

Settings in Connection profiles

Following are the Connection profile parameters (shown with default settings) for requesting an authentication protocol on a dial-out call:

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

Parameter	Specifies
Send-Auth-Mode	Authentication protocol requested for a dial-out call. With the default setting, No-PPP-Auth, no authentication is negotiated. Valid values are PAP-PPP-Auth, No-PPP_Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, and Any-PPP-Auth.
Send-Password	Password the TAOS unit sends to the far end as part of the initial handshake.

Settings in RADIUS profiles

RADIUS uses the following attribute-value pairs to request an authentication protocol in a dial-out profile.

RADIUS Attribute	Value
Ascend-Authen-Alias (203)	Login name for the TAOS unit, to be sent as part of the authentication process of a dial-out call. The default is the value of the Name parameter in the System profile.
Ascend-Send-Auth (231)	Authentication protocol requested for a dial-out call. With the default value of Send-Auth-None (0), no authentication is negotiated. Other values are Send-Auth-PAP (1) and Send-Auth-CHAP (2).

RADIUS Attribute	Value
Ascend-Send-Secret (214)	Password sent to the far end during authentication of the dial-out call. If the server does not support this attribute, use Ascend-Send-Passwd (232) instead. For details, see “Shared secrets and secure exchanges” on page A-5.

Examples of requesting CHAP for a dial-out call

The following commands create a profile that requests CHAP when dialing out to the far end:

```
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
```

Following are comparable RADIUS profiles:

```
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"
```

Authenticating user login sessions

A terminal-server connection is initiated by an analog modem or ISDN modem (such as a V.120 terminal adapter). Depending on the client software used to initiate the link, the connection can be used for an asynchronous PPP call or a user login session.

When it receives a call, the terminal server waits briefly to receive a PPP packet. If it times out waiting for PPP, it sends its login prompt. If it receives a name and password that match a configured profile, it authenticates the call and provides the user with the authorized level of access to the terminal server itself or to a network host. For details about authorizing access for login sessions, see Appendix B, “Authorization Options.”

If the terminal server receives a PPP packet, it responds with a PPP packet. LCP negotiations begin, including PPP authentication. If authentication is successful, the TAOS unit forwards the call to the router software and establishes a regular PPP session. Except for the initial processing, the TAOS unit handles an asynchronous PPP call as any regular PPP call. For details about authenticating framed protocol sessions, see “Authenticating framed protocol sessions” on page A-6.

Expect-Send login scripts

If a caller dials in using a communications package and a modem or ISDN TA with PPP turned off, the TAOS unit times out on PPP and sends login and password prompts such as the following:

```
Login:
Password:
```

The client software either displays the login prompt, allowing the user to login manually, or executes an Expect-Send script such as the following:

```
expect "Login:" send $username expect "Password:" send $password
```

After it has received all the required authentication information, the TAOS unit authenticates the information by comparing it to the information in the caller’s profile. The details of what happens after the session is successfully authenticated depend on a variety of factors that come under the heading of *authorization*.

Terminal-server security mode

The following parameters (shown with default settings) are used to password-protect the terminal-server command line:

```
[in TERMINAL-SERVER]
security-mode = none
```

```
[in TERMINAL-SERVER:terminal-mode-configuration]
system-password = ""
```

Parameter	Specifies
Security-Mode	Requirement for entering a password to access the terminal server.
System-Password	Password (up to 23 characters) for accessing the terminal server.

If Security-Mode is set to None (the default), users are immediately presented with a terminal-server prompt when they connect by means of an asynchronous interface. For example:

```
ATDT961234
CONNECT 115200
** TAOS Terminal Server **
```

```
ascend%
```

If Security-Mode is set to Partial, users are prompted for their own name and password, as configured in the caller's profile.

If Security-Mode is set to Full, users are prompted for both a system password and their own name and password before the terminal-server prompt appears.

The following commands specify full password security in the terminal server and set the system password to `secret`:

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

admin> set security-mode = full

admin> set terminal system-password = secret

admin> write
TERMINAL-SERVER written
```

With these settings, users must respond to the following prompts to log in to the terminal server:

```
System Password:

Name:
Password:
```

Customizing the login sequence

The following parameters (shown with default settings) specify which strings are sent to and expected from a dial-in user during the login process:

```
[in TERMINAL-SERVER:terminal-mode-configuration]
banner = "** TAOS Terminal Server **"
login-prompt = "Login: "
password-prompt = "Password: "
third-login-prompt = ""
third-prompt-sequence = last
prompt = "ascend% "
login-timeout = 300
```

Parameter	Specifies
Banner	First line sent to the dial-in user. The default banner is `** TAOS Terminal Server **`.
Login-Prompt	Second line sent to the dial-in user, prompting for a username. The system uses the name supplied at this prompt to authenticate the caller's profile.
Password-Prompt	Third line sent to the dial-in user, prompting for a password. The system uses the password supplied at this prompt to authenticate the caller's profile.
Third-Login-Prompt	Third login prompt, required by some RADIUS servers and service provider login sequences.
Third-Prompt-Sequence	Where the third login prompt appears in the login sequence (first or last).

Parameter	Specifies
Prompt	String to use as the command-line prompt in the terminal-server interface.
Login-Timeout	Number of seconds the login prompt appears before the login times out. When a user logs in to the terminal server in terminal mode, a login prompt appears. If the user does not proceed any further than the login prompt within 300 seconds, the login times out. If you set the Login-Timeout parameter to zero, the login never times out.

Specifying the banner and prompts

Following is an example of configuring the banner, login prompts, and command-line prompt:

```
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
```

With these settings, a dial-in user logging in to the terminal-server command line receives the following sequence of prompts:

```
ABC Corp. Terminal Server

System Password:

Name:
Password:
```

If you change the login and command-line prompt default settings, make sure that the users' Expect-Send scripts are written to expect the strings you specify. For example:

```
expect "Name:" send username expect "Password:" send password
expect "ABC Corp. Terminal Server" send "" expect "ABC: " send "telnet
10.1.1.3"
```

When to use the third prompt

Some RADIUS servers require an additional (third) login prompt, specified by the Ascend-Third-Prompt attribute (213). If the call is authenticated by RADIUS, and the profile specifies a value for this attribute, you should configure the terminal server to display the required prompt. If RADIUS expects a third prompt, it always expects it last, after the regular login sequence.

Some ISPs use a terminal server that follows a login sequence different from that used by Lucent Technologies (for example, one that includes a menu selection before login). If such is the case at your site, you should configure the terminal server to display the required prompt, and specify that it be displayed first, thereby minimizing the other terminal server and retaining compatibility with client software in use by subscribers.

The following example shows how to set the Third-Login-Prompt and Third-Prompt-Sequence parameters for a RADIUS server that expects a third prompt:

```
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
```

The next example shows how to set the Third-Login-Prompt and Third-Prompt Sequence parameters to mimic another terminal server that expects users to select a service before login:

```
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
```

Token-card authentication

TAOS units support token-card authentication by using a RADIUS server as the intermediary between the TAOS unit answering the call and an External Authentication Server (EAS), such as a Security Dynamics ACE/Server or an Enigma Logic SafeWord server.

Enhanced security with token cards

Token cards protect against both passive attacks and replay attacks, in which an unauthorized user records valid authentication information exchanged between systems and then replays it later to gain entry. Because token cards provide one-time-only passwords, the password changes many times a day, making replay impossible.

A token card is a hardware device, typically shaped like a credit-card calculator, with an LCD display that provides the user with the current, one-time-only token (password) that will enable access to a secure network. The current token changes many times a day. Token cards keep the changing authentication information continuously up-to-date by maintaining a synchronized clock with an EAS such as an ACE/Server or SafeWord server. Authorized users must have the token card in their possession to gain access to a secure network.

If the EAS is an ACE/Server, the user has a SecurID token card that displays a randomly generated access code, which changes every 60 seconds.

If the EAS is a SafeWord server, the user can have one of the following types of token cards:

- ActivCard
- CryptoCard
- DES Gold
- DES Silver
- SafeWord SofToken

- SafeWord MultiSync
- DigiPass
- SecureNet Key
- WatchWord

TAOS units support the use of token cards only through RADIUS. The RADIUS server must be configured to interact with the EAS modules, which typically run on the same physical system as the RADIUS server.

Note: When RADIUS authentication is in use, the RADIUS server itself acts as the EAS. When token-card authentication is in use, the RADIUS server passes the authentication request on to an ACE/Server or SafeWord server, and that system is referred to as the EAS. This detail does not affect the TAOS unit's External-Auth profile configuration, which must still specify RADIUS as the external server.

Simple method of authenticating token-card calls

A TAOS unit can support token-card authentication from devices that do not run TAOS software. To do so, the unit authenticates the calls in the terminal-server software, using normal PAP authentication to perform the challenge-response token exchanges. For example, the following RADIUS profile specifies authentication from an 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
```

The RADIUS server discards the user's response to the initial terminal-server Password prompt, so the user can enter any value. The RADIUS server generates an Access-Challenge packet with a challenge prompt (typically a Passcode prompt for ACE/Server authentication), and uses the response to that challenge packet to actually authenticate the user with the EAS.

If the caller's profile specifies the following attribute-value pair, the system does not require a challenge-response exchange:

RADIUS Attribute	Value
Ascend-Token-Immediate (200)	Bypasses the challenge-response procedure required by some token-card authentication methods. Valid values are Tok-Imm-No (0), which is the default, and Tok-Imm-Yes (1). If used, must be a Check-Item in the RADIUS profile. **Note:** Setting this attribute to Tok-Imm-Yes makes the profile incompatible with PAP-TOKEN, PAP-TOKEN-CHAP, and CACHE-TOKEN authentication (see "Authenticating token-card connections from TAOS units" on page A-27).

When users have a token card that does not require a challenge-response exchange (such as ACE/Server), you can use Ascend-Token-Immediate to simplify the authentication process. Users respond to the initial Password prompt with the current token. The RADIUS server does not discard this initial response, but uses it to authenticate the call via the EAS.

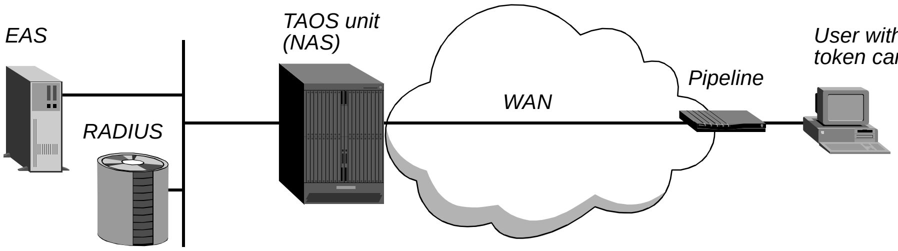
Following is a sample RADIUS profile that implements the Ascend-Token-Immediate attribute:

```
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
```

Authenticating token-card connections from TAOS units

Figure A-5 shows a dial-in connection through a Pipeline unit to a TAOS unit operating as a network access server (NAS) on a secure network. The remote user must use a token card to gain access to the secure network.

Figure A-5. Token-card authentication for dial-in connections



In an arrangement like the one in Figure A-5, a user with a token card initiates a connection through a Pipeline unit to the TAOS unit (NAS).

The NAS sends an Access-Request packet to the RADIUS server to authenticate the incoming call, and the RADIUS server forwards the connection request to the EAS (an ACE/Server or SafeWord server).

The EAS sends an Access-Challenge packet back through the RADIUS server and the TAOS unit to the user dialing in. The user sees the challenge message, obtains the current password from his or her token card, and enters that password in response to the challenge message. The password travels back through the NAS and the RADIUS server to the EAS.

The EAS sends a response to the RADIUS server, specifying whether the user has entered the proper token. If the user enters an incorrect token, the EAS returns another challenge and the user can try again, but only for a total of up to three attempts.

As the last step in authentication, the RADIUS server sends an authentication response to the TAOS unit. If authentication is unsuccessful, the TAOS unit receives an Access-Reject packet and terminates the call. If authentication is successful, the TAOS unit receives an Access-Accept packet containing a list of attribute-value pairs from the user profile in the RADIUS server's database. The TAOS unit uses the attribute-value pairs to create the connection.

Configuring a TAOS unit as a NAS

To configure the TAOS unit to function as a NAS, you must set up the Answer-Defaults profile to allow the appropriate authentication method. For example, you might set the Receive-Auth-Mode parameter to Any-PPP-Auth, as described in "Authenticating framed protocol sessions" on page A-6.

You must also set up the External-Auth profile to authenticate the connections via RADIUS (see “External-Auth profile” on page 1-5).

Specifying digital or analog service for a connection

You can specify digital or analog service on a per-connection basis through the RADIUS NAS-Port-Type (61) attribute or through the local profile. Following is the relevant parameter (shown with its default setting):

```
[in CONNECTION/"":telco-options]
nas-port-type = any
```

Parameter	**Specifies**
Nas-Port-Type	Type of service for the session. The default setting enables unrestricted service. Setting the parameter to `digital` or `analog` restricts service to the specified type.

The NAS-Port-Type settings in the local profile correspond to RADIUS attribute-value pairs for the RADIUS NAS-Port-Type attribute as follows:

RADIUS settings	**Corresponding local profile settings**
`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`

How the dial-in user displays and responds to challenges

The user must be able to display and respond to the challenge from the EAS. The APP Server utility can run on a PC that is accessible to the user, or the user can put the far-end TAOS unit in password mode by executing the Set Password command in the unit’s terminal-server interface. For example:

```
ascend% set password

Entering Password Mode...

[^C to exit] Password Mode>
```

Both of these methods of handling challenges are documented in the Pipeline and MAX documentation.

Configuring RADIUS profiles for token-card authentication

TAOS supports the following token-card authentication modes:

- PAP-TOKEN
- PAP-TOKEN-CHAP
- CACHE-TOKEN

Using PAP-TOKEN authentication

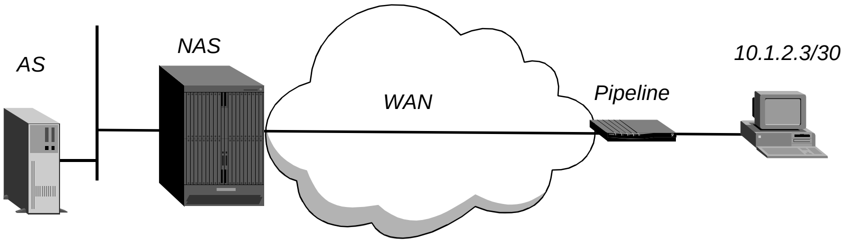
PAP-TOKEN is an extension of PAP authentication. It is not practical for multichannel calls, because if bandwidth requirements cause another channel to come up, the TAOS unit must interrupt the session to challenge the user for another token.

With PAP-TOKEN, the caller’s Send-Password value is sent as part of the initial session negotiation, which triggers a challenge from the EAS. The EAS returns a challenge, and the user types in the current token obtained from the token card. The token is sent in the clear (by means of PAP), but this lack of encryption might not be considered a serious security risk because the token is used only once.

The response to the initial challenge authenticates the base channel of the call. If bandwidth requirements cause another channel to come up, the user is challenged for a password.

Figure A-6 shows a PC user with a SecurID token card dialing in to the TAOS unit through a Pipeline unit. The EAS is a UNIX host running RADIUS and Security Dynamics ACE/Server software.

Figure A-6. PAP-TOKEN with an ACE/Server



When the EAS sends an Access-Challenge packet back through the RADIUS server and the TAOS unit to the user dialing in, the user sees the challenge message, obtains the current token, and enters that password in response to the challenge message. The password travels back through the NAS and the RADIUS server to the EAS, where it is authenticated.

Following is a RADIUS profile for the PC user:

```
Connor Password = "ACE"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.1.2.3,
   Framed-IP-Netmask = 255.255.255.252
```

Following is a far-end Connection profile in the Pipeline unit:

```
   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
```

Using PAP-TOKEN-CHAP authentication

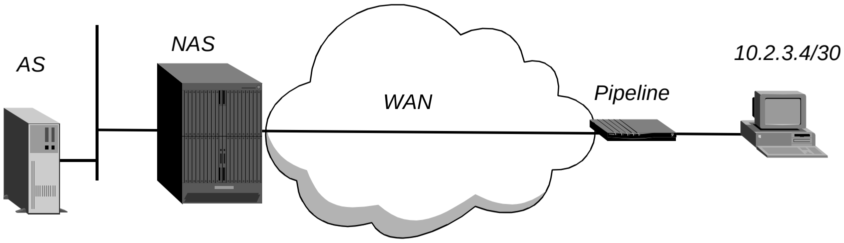
PAP-TOKEN-CHAP is appropriate for token-authenticating multilink calls. Base channel authentication uses PAP-TOKEN. If channels are added to the call, they are authenticated with CHAP and the caller's Aux Send PW. To inform the NAS of the Aux Send PW value to expect for subsequent channels, the RADIUS server sends this value as the Ascend-Receive-Secret value when the initial call is authenticated.

In addition to the requirement that the Password attribute must specify ACE or SAFEWORD, PAP-TOKEN-CHAP authentication requires the following attribute-value pair:

RADIUS Attribute	Value
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the Aux Send PW value sent by the far end to authenticate added channels. The RADIUS server delivers the receive-secret to the NAS when the initial call is authenticated. The NAS stores the receive-secret as the Recv-Password value for the caller, and uses it to create the digest sent to the RADIUS server via CHAP.

Figure A-7 shows a user with a token card dialing into A TAOS unit through a Pipeline unit. The EAS is a UNIX host running RADIUS and Enigma Logic SafeWord server software. After authentication, the user can open a multilink session.

Figure A-7. PAP-TOKEN-CHAP with a SafeWord server



Following is a sample user profile:

```
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
```

Following is a far-end Connection profile in the Pipeline unit:

```
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
```

Using CACHE-TOKEN authentication

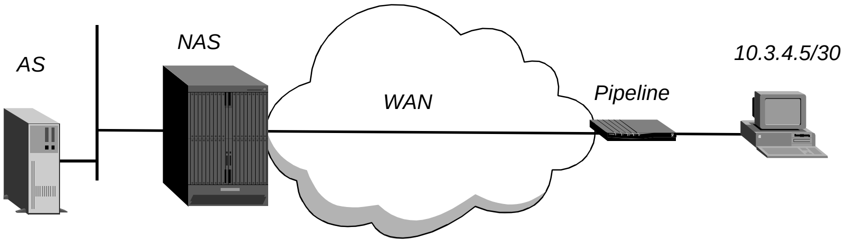
CACHE-TOKEN is another way of token-authenticating multilink calls. The RADIUS server caches an encrypted version of the token for a specified number of minutes. If the caller dials additional channels, the RADIUS server receives the request from the NAS, verifies that the token has not expired, and uses the cached token to authenticate the channels. If the token has expired, the request must be authenticated through the EAS with another challenge token.

In addition to the requirement that the Password attribute must specify ACE or SAFEWORD, CACHE-TOKEN authentication uses the following attribute-value pairs:

RADIUS Attribute	Value
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the Send PW value sent by the far end to authenticate the initial call. The RADIUS server uses this value to decrypt the hashed digest sent by the NAS using a form of CHAP exchange. The hashed digest is derived from the token sent by the caller and the normal Send PW value in the far-end profile.
Ascend-Token-Expiry (204)	Number of minutes a cached token remains valid. The default zero means that token caching is not allowed. This attribute must be a Check-Item. Token expiry is done solely in the RADIUS server. The NAS forwards authentication requests, and if the token has expired, the RADIUS server forwards the request to the EAS, which returns another challenge to the far end.
Ascend-Token-Idle (199)	Number of minutes a cached token remains valid if a call is idle. By default, the token remains alive until the value of the Ascend-Token-Expiry attribute is reached. This attribute must be a Check-Item. This attribute is useful for enforcing authentication when a connection comes up again after an idle period. If you do not specify a value for this attribute, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire. Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Figure A-8 shows a user who dials in using a Pipeline and is authenticated by an EAS, which is a UNIX host running RADIUS and Enigma Logic SafeWord server software.

Figure A-8. CACHE-TOKEN with a SafeWord server



Following is a RADIUS user profile for the dial-in user:

```
Aydin Password="SAFEWORD", 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
```

Following is a far-end Connection profile in the Pipeline unit:

```
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
```

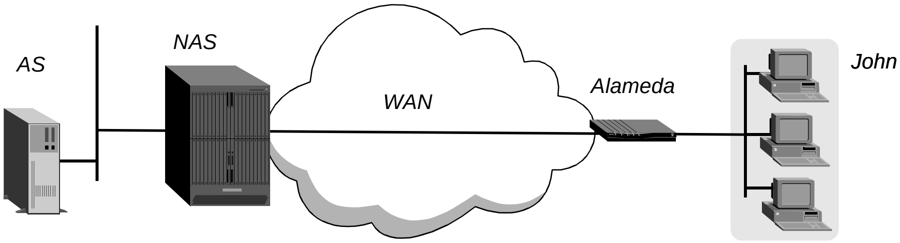
Using ACE authentication for network users

If the EAS is a Secure Dynamics ACE/Server, multiple users on a remote network can be granted dial-in access by a single profile that specifies the remote router name. To dial in, a user must enter the token in the following format:

```
token.username
```

The RADIUS server presents the *username* argument, rather than the name of the router, to the ACE/Server. Token caching still functions normally. All users share the same RADIUS profile, and RADIUS accounting uses the router name, not the real user name. In Figure A-9, multiple remote users are connected to a Pipeline unit named Alameda.

Figure A-9. ACE authentication for remote router users



The user profile specifies the system name of the Pipeline and the password for ACE/Server authentication. For example:

```
Alameda Password = "ACE"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.72.138.1,
   Framed-IP-Netmask = 255.255.255.0
```

A network user named John responds as follows to a password challenge:

```
From: hostname
0-Challenge: challenge
Enter next password: newtoken.John
```

Tunnel authentication

ATMP and L2TP support tunnel authentication. When tunnel authentication is required, the Foreign Agent or L2TP access concentrator (LAC) initiating a tunnel request must supply a password before the Home Agent or L2TP Network Server (LNS) allows registration of the tunnel.

Authenticating ATMP tunnels

The Home Agent ATMP profile contains a Password parameter. If it is not null, mobile client profiles must supply the password to initiate a tunnel. If the Foreign Agent supplies the proper password when requesting a tunnel, the Home Agent returns a RegisterReply message with a number that identifies the tunnel, and the mobile client's tunnel is established. If the password does not match, the Home Agent rejects the tunnel, and the Foreign Agent logs a message and disconnects the mobile client. The following commands configure the Home Agent ATMP profile to require tunnel authentication:

```
admin> read atmp
ATMP read

admin> set password = tunnel-password

admin> write
ATMP written
```

The Password parameter in the mobile-client's Connection > Tunnel-Options profile must specify the same value. For example:

```
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
```

Following is a comparable RADIUS profile:

```
mobile-client Password = "my-password",
   Service-Type = Framed-User
   Tunnel-Type = ATMP,
   Tunnel-Server-Endpoint = "3.3.3.3:8877",
   Tunnel-Password = "tunnel-password"
```

Many RADIUS servers encrypt tunnel passwords before sending them to the Home Agent if the mobile-client profile uses the Tunnel-Password (69) attribute to specify the password. If the profile specifies a value for Tunnel-Password and the RADIUS server does not encrypt the password, tunnel authentication will fail.

If, instead, the mobile-client profile uses the Ascend-Home-Agent-Password (184) attribute to specify the password, the RADIUS server performs no encryption before sending the password to the Home Agent. This option might be required if you are using a RADIUS server that does not encrypt the Tunnel-Password value.

Note: Unless you are using a RADIUS server that does not support tunnel password encryption (or encryption is not required), use of the Tunnel-Password attribute is recommended in place of Ascend-Home-Agent-Password to protect against local sniffers detecting tunnel passwords.

Authenticating L2TP tunnels

L2TP tunnels can be authenticated if the same secret value is in use at both ends of the connection (a shared secret).

If you are using local profiles for mobile-client authentication in the LAC (the TAOS unit), you can specify a single shared secret for authenticating all locally configured tunnels. The following commands specify a single shared secret for the entire LAC Tunnel-Server configuration:

```
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
```

If the LAC uses RADIUS to authenticate mobile clients, the clients' RADIUS profiles can specify a shared secret by using the Tunnel-Password (69) attribute.

Note: The Tunnel-Password value must be encrypted by the RADIUS server. Otherwise, tunnel authentication fails.

In the calling client's RADIUS profile, the following subprofile authenticates the tunnel:

```
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"
```

If you prefer, you can remove the Tunnel-Password attribute from calling clients' profiles and create a profile whose sole purpose is to authenticate L2TP tunnels. This causes an extra RADIUS lookup the first time the tunnel is created, but it simplifies administration when shared secrets change. The RADIUS profile for tunnel authentication must specify the L2TP peer's name, a null password (""), and the Outbound-User setting for Service-Type. For example:

```
lns-sys.domain.org Password = "", Service-Type = Outbound-User
   Tunnel-Password = "tunnel-secret"
```

When an L2TP tunnel is initially established, both the LNS and the LAC issue a RADIUS lookup based on the peer's name. If the system finds a profile such as the one shown in the preceding example, it uses the Tunnel-Password value to authenticate the tunnel.

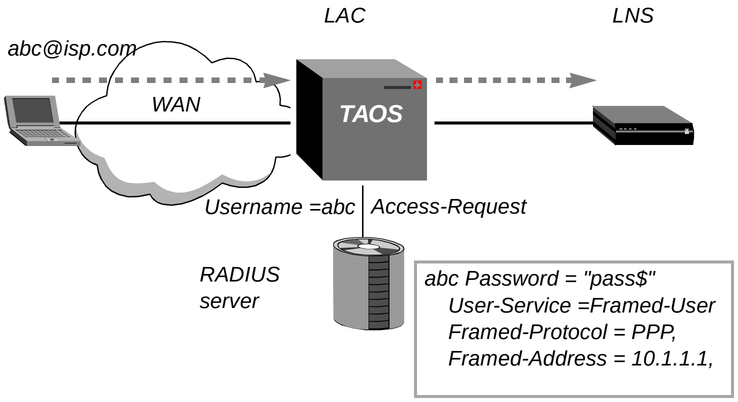
Note: The password in the pseudo-user profile must be null (""). Because the null password represents a security risk, *the profile must specify the Outbound-User setting for Service-Type.*

Stripping portions of the username from RADIUS access requests

You can configure TAOS units to strip off portions of the username sent in the Username attribute-value pair of a RADIUS Access-Request packet. The primary purpose of this feature is to remove the domain name from incoming authentication requests. However, the feature is not limited to that purpose.

Figure A-10 shows a TAOS unit that is functioning as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC). The unit is removing the portion of the username value that follows the *at* sign (@) before forwarding the Username attribute-value pair in a RADIUS Access-Request packet.

Figure A-10. Removal of domain name before RADIUS authentication



```
abc Password = "pass$"
   User-Service =Framed-User
   Framed-Protocol = PPP,
   Framed-Address = 10.1.1.1,
```

The user dialing into the TAOS unit has the following username:

```
abc@isp.com
```

On the RADIUS server, the user profile name is `abc`. To enable the authentication to take place properly, the TAOS unit must remove `@isp.com` before forwarding the Access-Request packet to the RADIUS server. After the client has been authenticated by the TAOS unit operating as a LAC, the LAC forwards the username and password to the L2TP network server (LNS).

Overview of delimiter settings

To provide flexibility in processing Username values to be forwarded to a RADIUS server in Access-Request packets, you can specify one or multiple characters as delimiters, the number of delimiters that must be present in a username for the unit to strip off characters, and whether to strip characters to the left or right side of the specified delimiter characters.

Following are the parameters, shown with default values, for specifying the delimiters and the direction in which the Username value will be modified:

```
[EXTERNAL-AUTH:rad-auth-client]
auth-realm-delimiters = /\@%
auth-req-delim-count = 0
auth-req-strip-side = none
```

Parameter	**Specifies**
Auth-Realm-Delimiters	Character or characters to be recognized as delimiters in a username. In previous releases, the delimiters specified by this parameter were applied to Access-Accept packets only, and were used to define realms. With the current software, the delimiters are also used to define the boundaries of characters to be stripped from the username in Access-Request packets. The default value `/\@%` consists of the characters typically used for delimiting realms and domain names. You can specify up to 7 characters in any order.
Auth-Req-Delim-Count	Number of delimiter characters to delete. With the default zero value, no characters are stripped from the name. If the number of delimiters in the username is greater than or equal to the value of this parameter, the unit strips the characters to the left or right (as specified in the Auth-Req-Strip-Side setting) and sends the remaining string in the Username attribute-value pair. If the number of delimiters in the username is *less than* the value of the Auth-Req-Delim-Count parameter, the unit sends the entire username to RADIUS without stripping any characters.
Auth-Req-Strip-Side	Direction in which to strip characters from a username. The default value is `none`, which specifies that the unit removes no characters before sending the Username attribute-value pair. Other valid values are `left` (strip the delimiter character and characters to the left of it) and `right` (strip the delimiter character and characters to the right of it).

Example of configuring a TAOS unit to remove domain names

In the following example, a user logs in to TAOS unit with the following username:

```
billg@abc.com%xzy^msn.com
```

Following is the user's RADIUS profile:

```
billg Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 1.2.3.4,
    Framed-Netmask = 255.255.255.255
```

The following commands configure a TAOS unit to remove the *at* sign (@) and all characters to the right of it in the name the user presents at login:

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

admin> set rad-auth-client auth-realm-delimiters = @

admin> set rad-auth-client auth-req-delim-count = 1

admin> set rad-auth-client auth-req-strip-side = right

admin> write
EXTERNAL-AUTH written
```

With this configuration, when the TAOS unit receives a RADIUS-authenticated call from a user with the following name, the unit strips the delimiter character and all characters to the right of it and sends the remaining string (`billg`) in the Username attribute-value pair:

```
billg@abc.com%xzy^msn.com
```

Example of configuring a TAOS unit to recognize various delimiters

In the following example, three users log in to a TAOS unit with the following usernames:

```
abc\isp2.com

def@isp3.com

hij/isp4.com
```

Following are the users' RADIUS profiles:

```
abc Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 1.2.3.4,
    Framed-Netmask = 255.255.255.255

def Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 2.3.4.5,
    Framed-Netmask = 255.255.255.255

hij Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 3.4.5.6,
    Framed-Netmask = 255.255.255.255
```

The following commands configure a TAOS unit to remove all characters to the right of one of the specified delimiters in the name the user presents at login:

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

admin> set rad-auth-client auth-realm-delimiters = /\@%

admin> set rad-auth-client auth-req-delim-count = 1

admin> set rad-auth-client auth-req-strip-side = right

admin> write
EXTERNAL-AUTH written
```

With the following sample configuration, when the TAOS unit receives a RADIUS-authenticated call from a user with one of the following names, the unit strips the delimiter character and all characters to the right of it and sends the remaining string (`abc`, `def`, or `hij`) in the Username attribute-value pair:

```
abc\isp2.com

def@isp3.com

hij/isp4.com
```

Example of configuring a TAOS unit to require multiple delimiters in a name

In the following example, two callers log in to a TAOS unit with the usernames `abc@def@isp1.com` and `ghi@jkl%isp2.com.`

Following are the users' RADIUS profiles:

```
abc Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 1.2.3.1,
    Framed-Netmask = 255.255.255.0

ghi Password = "localpw"
    User-Service =Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 2.3.4.5,
    Framed-Netmask = 255.255.255.248
```

The following commands configure a TAOS unit to remove all characters to the right of the first (leftmost) delimiter if the name contains two or more delimiters:

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

admin> set rad-auth-client auth-realm-delimiters = /@%\

admin> set rad-auth-client auth-req-delim-count = 2

admin> set rad-auth-client auth-req-strip-side = right

admin> write
EXTERNAL-AUTH written
```

With this configuration, when the TAOS unit receives a RADIUS-authenticated call from a user with one of the following names, the unit removes the first delimiter character and all characters to the right of it (including the second delimiter character and its following text). The unit then sends the remaining string (`abc` or `ghi`) in the Username attribute-value pair:

```
abc@def@isp1.com
ghi@jkl%isp2.com
```

If a user dials in with the following name, the call fails:

```
abc@isp1.com
```

When the unit determines that the name contains fewer than the specified number of delimiters, it passes the name to the RADIUS server without stripping any characters.

Preauthentication by means of CLID or DNIS

A calling line ID (CLID) is the telephone number of a calling device. You can use a CLID for authentication only if the call information is available end-to-end and automatic number identification (ANI) applies to the call. In some areas, the WAN provider might not be able to deliver CLIDs, or a caller might keep a CLID private. Typically, people use CLIDs to protect against the situation in which an unauthorized user obtains the name, password, and IP address of an authorized user, and calls in from another location.

Dialed Number Information Service (DNIS) is a service that provides the called-party number, which is an information element of the Q.931 ISDN signaling protocol. The DNIS number is the telephone number the remote device calls to connect to the TAOS unit, but without a trunk group or dialing prefix specification. When the profile requires called-number authentication, the number called must match a telephone number in a local Connection profile or RADIUS user profile.

CLID or DNIS verification occurs before a TAOS unit accepts a call and begins the process of authenticating a password.

Setting RADIUS passwords for DNIS and CLID preauthentication

You can configure your TAOS unit with RADIUS passwords for DNIS and CLID preauthentication by setting the `dnis` and `clid` parameters in the Password-Profile subprofile of the External-Auth profile. For example,

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

admin> set password-profile dnis = secretdnis

admin> set password-profile clid = secretclid

admin> write
EXTERNAL-AUTH written
```

Parameter	Specifies
CLID	Calling-Line ID (CLID) specified as the password in a RADIUS profile, up to 21 characters.

Parameter	**Specifies**
DNIS	Dialed Number Information Service (DNIS) value specified as the password in a RADIUS profile, up to 21 characters. The default is `Ascend-DNIS`.

Note: In earlier software releases, you configured DNIS and CLID preauthentication passwords by setting the `dnis-password` and `clid-password` parameters in the `External-Auth` profile. If you are upgrading to the current software version, you must reapply the values of the of the `dnis-password` and `clid-password` parameters set in the previous release to the `dnis` and `clid` parameters, as shown in the preceding example.

Configuring a TAOS unit to extract and use call information

To enable a TAOS unit to extract and use CLID or DNIS information, set the CLID-Auth-Mode parameter in the Answer-Defaults profile. For example, the following commands configure the system to use CLID information if it is available, but to attempt password authentication of the call if CLID authentication fails for any reason:

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

admin> set clid-auth-mode = clid-prefer

admin> write
ANSWER-DEFAULTS written
```

You can set CLID-Auth-Mode to one of the following values:

- Ignore (the default)—The caller-ID or called-number information is ignored unless it is specified as a Check-Item in a RADIUS user profile. See “Example of using Caller-Id as a Check-Item (RADIUS only)” on page A-42.
- CLID-Prefer or DNIS-Prefer—The system preauthenticates by means of the CLID or DNIS number, respectively, if the number is present in the call. After preauthentication, the call can either go on to a second phase of password authentication or immediately establish the connection. However, if the CLID or DNIS is not presented by the telephone company switch, the call is not terminated. In effect, if the number is present, the system behaves as if CLID-Auth-Mode were set to CLID-Require or DNIS-Require. If the number is not present, it behaves as if CLID-Auth-Mode were set to Ignore.
- CLID-First or DNIS-First—If the calling-line ID (CLID) or called number (DNIS) is sent by the telephone company switch, the TAOS unit uses it to authenticate the call. If that level of authentication fails for any reason, or if the telephone company switch does not provide the calling-line ID or called number, the TAOS unit does not drop the call, but allows negotiations to proceed to password authentication.
- CLID-Require or DNIS-Require—The call must be preauthenticated or it fails. If the CLID or DNIS number matches a profile, the call can either go on to a second phase of password authentication or immediately establish the connection. If there is no matching profile, or if the CLID or DNIS number is not present, the call is never answered, and is therefore never billed as a call to the user.
- Fallback (for CLID only)—The CLID is required, but only if the call is authenticated with RADIUS. If the RADIUS server does not respond, the system goes on to perform password authentication instead of dropping the call.

Note: For some types of E1 signaling, the system must explicitly request CLID information from the switch. For those signaling methods, you must set the Caller-ID parameter in the E1 profile to Get-Caller-ID.

Specifying the Disconnect Cause Element (RADIUS only)

If CLID or DNIS authentication fails, a RADIUS server can return either the default, Normal Call Clearing (decimal 16), as the Cause Element in ISDN Disconnect packets, or it can send User Busy (decimal 17), depending on the setting of the following parameters (shown with default settings):

```
[in EXTERNAL-AUTH:rad-auth-client
auth-id-fail-return-busy = no
auth-id-timeout-return-busy = no
```

Parameter	Specifies
Auth-ID-Fail-Return-Busy	Enable/disable sending the User Busy (17) disconnect cause when CLID or DNIS authentication fails. The default setting of No causes the system to send the Normal Call Clearing (decimal 16) cause.
Auth-ID-Timeout-Return-Busy	Enable/disable sending the User Busy (17) disconnect cause when CLID or DNIS authentication times out. The default setting of No causes the system to send the Normal Call Clearing (decimal 16) cause.

For example, to return the User Busy Cause Element on a timeout:

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

admin> set rad-auth-client auth-id-timeout-return-busy = yes

admin> write
EXTERNAL-AUTH written
```

Configuring profiles for CLID or DNIS authentication

When a caller’s profile specifies a caller ID number, the TAOS unit can compare that number to the one presented by the telephone company switch, to verify that the call is coming in from a known location.

Settings in Connection profiles

Following are the parameters (shown with default settings) for specifying CLID and DNIS numbers in a Connection profile:

```
[in CONNECTION/""]
clid = ""
calledNumber = ""
```

Parameter	Specifies
CLID	Telephone number of the calling device. When a user dials in by means of MP or MP+, the calling device might have more than one telephone number associated with it. In such a case, the CLID is the telephone number associated with the channel in use.
CalledNumber	Called-party number, which is an information element of the Q.931 ISDN signaling protocol. It is the telephone number the remote device calls to connect to the TAOS unit, but without a trunk group or dialing prefix specification.

Settings in RADIUS profiles

RADIUS uses the following attribute-value pairs for specifying CLID and DNIS numbers:

RADIUS Attribute	Value
Caller-Id (31)	Telephone number of the calling device (a string value). When a user dials in by means of MP or MP+, the calling device might have more than one telephone number associated with it. In such a case, the CLID is the telephone number associated with the channel in use.
Client-Port-DNIS (30)	Called-party number (a string value), which is an information element of the Q.931 ISDN signaling protocol. It is the telephone number the remote device calls to connect to the TAOS unit, but without a trunk group or dialing prefix specification.
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after called-number authentication. Valid values are Not-Require-Auth (0), which is the default, and Require-Auth (1).

Example of using Caller-Id as a Check-Item (RADIUS only)

For RADIUS-authenticated connections, if the Caller-Id or Client-Port-DNIS number is known, it is included in the Access-Request packet to the RADIUS server. If the Caller-Id number is specified as a Check-Item in the RADIUS user profile (if it is specified on the first line of the profile), as shown in the following example, the Access-Request packet is rejected if the Caller-Id number presented to the server does not match the value of the Caller-Id attribute.

```
emma Password = "test", Caller-Id = "5551213"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 1,
   Ascend-Route-IP = Route-IP-Yes
```

The preceding example shows a normal user profile, but the user is limited to a specific telephone number. This limitation could be used to prevent multiple user connections. Unless the user owns a PBX or other service that always gives out the same number for multiple telephone lines, only one user will be able to connect. The single telephone number limitation is normally used for security, to prevent a system admin or other important account from being abused.

Example of using User-Name for first-tier DNIS authentication

In previous releases, if only first-tier DNIS authentication was performed, no username information was available for SNMP, Syslog, or RADIUS accounting records. In the current software release, if only first-tier DNIS authentication is performed and the profile contains a User-Name attribute-value pair, the RADIUS server returns the value of the User-Name attribute in its DNIS Auth reply. If second-tier user-password authentication is performed, the username information is taken from the login name, as in earlier versions of the software.

Following is a sample DNIS-authenticated RADIUS profile that includes the User-Name attribute:

```
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
```

Examples in which CLID is preferred

The following Connection profile validates the CLID number if it is present in the call. If the CLID number presented by the call does not match, the call is dropped. If the CLID number is not present in the call, the profile proceeds to password authentication.

```
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
```

When CLID-Auth-Mode is set to CLID-Prefer, the TAOS unit sends an Access-Request packet to the RADIUS server with the Caller-Id number as the User-Name value, Ascend-CLID as the password, and Outbound-User specified for Service-Type. If the unit finds a matching RADIUS user entry, such as the one shown in the following example, the call is authenticated and can immediately begin the configured service:

```
5551234 Password = "Ascend-CLID", Service-Type = Outbound-User
   Ascend-Require-Auth = Not-Require-Auth
```

If no matching entry is found, the Access-Reject packet does not cause the call to be terminated. Instead, the user is still permitted to connect but must go through normal user authentication. Similarly, if the system finds a matching entry in which Ascend-Require-Auth is set to Require-Auth, it validates the CLID number and then proceeds to password-authenticate the call. For example, the following profiles enable the user to dial in from any one of the specified CLID numbers:

```
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
```

The following profile limits the user to the specified CLID number:

```
edgar Password = "test", Caller-Id = "5551235"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 1,
   Ascend-Route-IP = Route-IP-Yes
```

Note: The user profile for the second phase of authentication can be a normal user entry such as the one shown in the preceding example, or it can be any other kind of valid user profile. For example, it can specify token-card authentication or UNIX password authentication.

Examples in which DNIS is preferred

The following Connection profile validates the DNIS number if it is present in the call. If the DNIS number presented by the call does not match, the call is dropped. If the DNIS number is not present in the call, the profile is password-authenticated.

```
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
```

When CLID-Auth-Mode is set to DNIS-Prefer, the TAOS unit sends an Access-Request packet to the RADIUS server with the Client-Port-DNIS number as the User-Name, Ascend-DNIS as the password, and Outbound-User for Service-Type. If the finds a matching RADIUS user entry, such as the one shown in the following example, the call is authenticated and can immediately begin the configured service:

```
1212 Password = "Ascend-DNIS", Service-Type = Outbound-User
   Ascend-Require-Auth = Not-Require-Auth
```

If no matching entry is found, the Access-Reject packet does not cause the call to be terminated. Instead, the user is still permitted to connect but must go through normal user authentication. Similarly, if the system finds a matching entry in which Ascend-Require-Auth is set to Require-Auth, it validates the DNIS number and then proceeds to password-authenticate the call. For example, the following profiles enable the user to use any one of the specified DNIS numbers:

```
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
```

The following profile limits the user to the specified DNIS number:

```
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
```

Note: The user profile for the second phase of authentication can be a normal user entry such as the one shown in the preceding example, or it can be any other kind of valid user profile. For example, it can specify token-card authentication or UNIX password authentication.

Examples in which CLID is required

When CLID-Auth-Mode is set to CLID-Require, preauthentication of the telephone call is required. For local Connection profiles, this means that each profile must specify the required CLID number. If a call is received that does not present the required information, the TAOS unit does not even answer the call.

For RADIUS-authenticated calls, the CLID-Require setting means there must be a user entry for every valid caller-ID. If a user dials in from a telephone number that does not have an Ascend-CLID entry, the TAOS unit does not answer the call. The user does not have the opportunity for user authentication, and the call is not billed to the user.

The following commands configure a local Connection profile with a CLID number. When the Answer-Defaults profile specifies that a CLID number is required, the call must present a matching caller-ID.

```
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
```

The following RADIUS entries identify all acceptable calling line IDs when a CLID number is required:

```
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
```

A call received from any other number is rejected. Because additional authentication is required, each call also requires its own user profile, which might or might not limit that particular user to one caller ID. The following example enables the user to dial in from any one of the specified CLID numbers:

```
aydin Password = "test"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 1,
   Ascend-Route-IP = Route-IP-Yes
```

Examples in which DNIS is required

When CLID-Auth-Mode is set to DNIS-Require, preauthentication of the telephone call is required. For local Connection profiles, this means that each profile must specify the required DNIS number. If a call is received that does not present the required information, the TAOS unit does not even answer the call.

For RADIUS-authenticated calls, the DNIS-Require setting means there must be a user entry for every valid DNIS number. For example, if a call comes in on a number that does not have an Ascend-DNIS entry, the TAOS unit does not answer the call. The user does not have the opportunity for user authentication, and the call is not billed to the user.

The following commands configure a local Connection profile with a DNIS number. When the Answer-Defaults profile specifies that CLID is required, the call must present a matching caller-ID.

```
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
```

The following entries identify all acceptable calling line IDs when DNIS is required:

```
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
```

A call that comes in on another number is rejected. Because additional authentication is required, each call requires its own user profile, which might or might not limit that particular user to one DNIS. The following example enables the user to call in on any of the specified DNIS numbers:

```
aydin Password = "test"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Ascend-Assign-IP-Pool = 1,
   Ascend-Route-IP = Route-IP-Yes
```

The following profile limits the user to the specified DNIS number:

```
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
```

Callback

Callback is a feature in which unit A places a call to unit B, which hangs up and calls back unit A. The callback feature helps to make sure that the originating caller does not pay for the call and that the TAOS unit makes a connection with a known caller. Hanging up and calling back adds a level of certainty that the connection is with a trusted user, because the TAOS unit immediately calls back after verifying the user’s name and password. To support callback, the TAOS unit must support both incoming and outgoing calls.

TAOS units support the following three implementations of callback:

- CLID or DNIS callback (previously called Ascend CLID/DNIS Callback)—A TAOS unit detects callback during the ringing state of an incoming call by means of the CLID or DNIS information element. The TAOS unit does not answer the call (go off hook), and the originating caller is not charged for the call.
- Ascend callback—Similar to CLID or DNIS callback except that the TAOS unit detects callback during the authentication phase (after going off hook), by means of the username and password in the Connection profile. The originating caller is charged for the *initial* call.
- Callback Control Protocol (CBCP)—Developed by Microsoft to address a need for greater security with PPP connections. The callback option defined in RFC 1570 is not as secure as other forms of callback, because authentication is performed only during the initial call and *not* during the callback. CBCP callback, like Ascend callback, supports a more secure connection, because the callback occurs *after* authentication.

  CBCP offers features not available with the standard callback defined in RFC 1570. The client side supports a configurable time delay to allow users time to initialize modems or enable supportive software before the TAOS unit calls the client. The TAOS unit does not allow a Connection profile or CBCP RADIUS profile to be shared by more than one Windows client.

  The TAOS unit detects and negotiates CBCP callback by means of the CBCP protocol during PPP negotiation. You can configure the TAOS unit so that the user can negotiate the callback telephone number. CBCP callback takes the place of the remote access server (RAS) server for callback to the RAS client (Windows 95).

Callback characteristics

Callback on the TAOS unit has the following characteristics:

- *Local or external authentication*—Connection profiles for configuring authentication can be either local or external (on the RADIUS server). For each implementation of callback, a TAOS unit accesses RADIUS once during external authentication. The unit does not request RADIUS attributes during the callback dialout process.
- *Nailed, Frame Relay, or X.25 connections*—TAOS units do not support callback through nailed, Frame Relay, or X.25 connections.
- *Security involving external filters and routes*—TAOS units support callback and external filters and external routes, but connections are restricted to a maximum of 16 external filters and 10 external routes per Connection profile.
- *ATMP tunnel security*—The TAOS unit supports Ascend Tunnel Management Protocol (ATMP) tunneling and all three callback implementations. The TAOS unit (Foreign Agent) does not create the tunnel during the initial call. Instead, the unit creates the tunnel it calls back the mobile source.
- *Security*—You can use callback to extend security, and the TAOS unit clears all incoming calls that have callback enabled. If the unit cannot register the callback connection (for example, because of a lack of internal resources), the unit clears the call.
- *Expect callback*—This feature provides callback in reverse on a TAOS unit. The unit calls a remote unit, which hangs up and calls back the TAOS unit. When the remote unit rejects the call, the TAOS unit disables its dialout process to the dialed unit until the unit calls back or 90 seconds have expired.
- *Callback log messages created*—Five log messages provide information about callback processes. (See the *APX 8000/MAX TNT Administration Guide*.)
- *Disconnect cause codes*—Incoming calls registered for callback are cleared with cause code 6 or 102. (See the *APX 8000/MAX TNT Administration Guide*.)
- *Callback debug commands*—TAOS units support callback commands to provide diagnostic information. (See the *APX 8000/MAX TNT Administration Guide*.)
- *Special routing*—A TAOS unit can route a callback through a resource type different from the one used for the initial call. For example, the unit can accept the initial call from a modem card and make the outgoing call through a Hybrid Access card.

General information about configuring callback

Although you can mix callback implementations for a particular platform, you cannot mix callback types within the same connection profile. If you select more than one callback type, a TAOS unit performs callback in the following order: CLID or DNIS callback, then Ascend callback, then CBCP callback. TAOS units support CLID or DNIS authentication in combination with CBCP callback. Callback and the expect-callback feature cannot be mixed inside the same profile, because you cannot simultaneously wait and perform a callback for a given profile.

For each callback implementation, an IP address pool index can be selected in place of a static IP address. The pool index enables the user to have a dynamic IP address taken from a pool. The TAOS unit assigns the IP address when it calls back the user.

Configuring CLID or DNIS callback

With CLID, a call comes in and the TAOS unit retrieves the matching profile with the Calling-Station-ID information from the ISDN Setup packet. The TAOS unit terminates the incoming call without answering it and initiates the callback. The devices negotiate PPP. With DNIS, the TAOS unit retrieves the matching profile with the Called-Station-ID. The originating caller cannot detect that the reason for the call termination is the pending callback, unless its administrator has enabled the expect-callback feature. The expect-callback feature allows you to delay the originating caller from redialing the connection for 90 seconds.

Global parameter configuration for CLID or DNIS callback

You must configure global configuration for CLID or DNIS callback within the Answer-Defaults profile:

Answer-Defaults parameter	**Required settings**
CLID-Auth-Mode	CLID-Require or DNIS-Require

Local Connection profile configuration CLID or DNIS callback

You can configure local configuration through the Connection profile. Following are typical (and mandatory if indicated) Connection profile settings for CLID or DNIS callback, for a particular user:

Connection profile parameter	**Typical setting**
Active	Yes
Encapsulation-Protocol	PPP. Alternatively, you can select MP or MPP.
Dial-Number	Number to be dialed during the callback dialout phase.
CLID	CLID number. To support CLID callback, you must specify a valid value for CLID.
Telco-Options > Callback	Yes.
Telco-Options > Data-Service	For example, Modem.
Telco-Options > Dialout-Allowed	Yes.
Telco-Options > Delay-Callback	For example, 10. This setting specifies the number of seconds that must elapse before the TAOS unit calls back the user.
CalledNumber	The DNIS number. To support DNIS callback, you must specify a valid value.

External Connection profile configuration CLID or DNIS callback

Following are typical (and required, if indicated) RADIUS Connection profile settings for CLID or DNIS callback:

RADIUS attribute	**Typical setting**
Password (2)	Password for CLID number. For example, Ascend-CLID.
User-Service (6)	Dialout-Framed-User (5).

RADIUS attribute	Typical setting
Ascend-Require-Auth (201)	Require-Auth (1).
Ascend-Callback (246)	Callback-Yes (1).
Caller-Id (31)	Calling-party number for calling-line ID (CLID) authentication, the telephone number of the user that wants to connect with the TAOS unit.
Framed-Protocol (7)	PPP (1), MP, or MPP (256).
Framed-Address (8)	IP address of a caller. RADIUS can authenticate an incoming caller by matching the user's IP address to the one specified in the user profile. For example, 192.168.143.2.
Framed-Netmask (9)	Subnet mask for the caller at Framed-Address. For example, 255.255.255.255.
Ascend-Dial-Number (227)	Telephone number that the TAOS unit dials.
Ascend-Data-Svc (247)	Switched-Modem (42). Specifies the type of data service that the link uses for outgoing calls.
Ascend-Send-Auth (231)	Send-Auth-PAP (1).
Ascend-Send-Passwd (232)	Password that the RADIUS server sends to the remote end of a connection on an outgoing call. For example, `Ascend`.
Ascend-Route-IP (228)	Route-IP-Yes (1) or Route-IP-No (0). Route-IP-Yes (the default), enables IP routing for the profile. Route-IP-No disables IP routing for the profile.

Because the TAOS unit makes only one RADIUS request, all parameters must be present in the profile.

Expect-callback configuration

With CLID or DNIS callback, the TAOS unit hangs up on an incoming caller and immediately initiates callback. Callback ensures that a connection is made with a known destination. For outgoing calls, the call originator can be configured to expect a callback from the machine that is called. The expect-callback feature prevents the call originator from dialing out more than one time before being called back.

For example, a call is initiated by a TAOS unit to a Pipeline unit. The Pipeline unit receives an incoming ISDN Setup message, recognizes the CLID, and rejects the incoming call with a Disconnect message. If the expect-callback feature is set on the TAOS unit, waits ninety seconds for the Pipeline to call back. If the feature is not set, the unit might determine that the call never got through and redial the call immediately.

When you set Expect-Callback to Yes on the calling device, all dialout calls that do not connect for any reason are put on a list that disallows further calls to that destination for 90 seconds. This delay gives the called device an opportunity to complete the callback.

To configure CLID or DNIS callback for expect-callback, you must set two local Connection profiles:

Connection profile parameter	**Setting**
Telco-Options>Callback	No
Telco-Options>Expect-Callback	Yes

Following are typical external Connection profile settings for expect-callback:

RADIUS attribute	**Typical setting**
Password (2)	Ascend.
User-Service (6)	Dialout-Framed-User (5).
Ascend-Dial-Number (227)	The telephone number that the TAOS unit dials.
Framed-Protocol (7)	PPP (1).
Ascend-Data-Svc (247)	Switched-64K (2). Specifies the type of data service that the link uses for outgoing calls.
Ascend-Dialout-Allowed (131)	Dialout-Allowed (1).
Framed-Address (8)	IP address of a caller. RADIUS can authenticate an incoming caller by matching the user’s IP address to the one specified in the user profile. For example, 4.5.6.7.
Framed-Netmask (9)	Subnet mask for the caller at Framed-Address. For example, 255.255.255.0.
Ascend-Metric (225)	Integer that specifies the virtual hop count of an IP route. The default setting is 7.
Ascend-Send-Auth (231)	Send-Auth-PAP (1).
Ascend-Send-Passwd (232)	Password that the RADIUS server sends to the remote end of a connection on an outgoing call. For example, Ascend.
Ascend-Expect-Callback (149)	Expect-Callback-Yes (1).
Ascend-Route-IP (228)	Route-IP-Yes (1) or Route-IP-No (0). Route-IP-Yes (the default), enables IP routing for the profile. Route-IP-No disables IP routing for the profile.

Configuring Ascend callback

A TAOS unit performs Ascend callback after fully negotiating the PPP connection. When a TAOS unit is the called device, the call comes in and normal authentication occurs. The TAOS unit then terminates the call and initiates callback, the call is terminated, and the call negotiates PPP. When a TAOS unit is the calling device, it waits for a callback if the connection proceeds normally and is disconnected before any data passes. The TAOS unit does not redial for a specified number of seconds.

Global parameter configuration for Ascend callback

Implement the global configuration for Ascend callback within the Answer-Defaults profile. Following are typical global configuration settings for Ascend callback:

Answer-Defaults parameter	**Typical setting**
CLID-Auth-Mode	Cannot be set to CLID-Require or DNIS-Require. If the parameter is set to either of these, CLID or DNIS callback is performed instead of Ascend callback.
PPP-Answer > Enable	Yes.
PPP-Answer > Receive-Auth-Mode	Any-PPP-Auth.
PPP-Answer > CBCP-Enable	Required for Ascend callback.

Local Connection profile configuration for Ascend callback

You implement a local configuration within the Connection profile. Following are typical Connection profile settings for Ascend callback:

Connection profile parameter	**Typical setting**
Active	Yes.
Encapsulation-Protocol	PPP. Encapsulation-Protocol can also be set to MP or MPP.
Dial-Number	Number to be dialed during the callback dialout phase.
Telco-Options > Callback	Yes. If you specify CBCP-Enable, Telco Options > Callback takes precedence.
Telco-Options > Data-Service	Modem.
Telco-Options > Dialout-Allowed	Yes.
Telco-Options > Delay-Callback	For example, 10. This setting specifies the number of seconds that must elapse before the TAOS unit calls back the user.
PPP-Options > Send-Auth-Mode	Pap-PPP-Auth. Other PPP authentication (or None) can be used, depending on the remote side.
PPP-Options > Send-Password	For example, Ascend.
PPP-Options > Recv-Password	For example, Ascend.
PPP-Options > CBCP-Enabled	Not required for Ascend Callback.

External Connection profile configuration for Ascend callback

Following are typical RADIUS configurations for Ascend Callback. The displayed configurations assume the use of external filters.

RADIUS attribute	**Typical setting**
Password (2)	User password. For example, Ascend.
User-Service (6)	Framed-User (2).
Ascend-Callback (246)	Callback-Yes (1).
Framed-Protocol (7)	PPP (1), MP, or MPP (256).

RADIUS attribute	**Typical setting**
Framed-Address (8)	IP address of a caller. RADIUS can authenticate an incoming caller by matching the user's IP address to the one specified in the user profile. For example, 4.5.6.7.
Framed-Netmask (9)	Subnet mask for the caller at Framed-Address. For example, 255.255.255.255.
Ascend-Dial-Number (227)	Telephone number that the TAOS unit dials.
Ascend-Data-Svc (247)	Switched-64K (2). This setting specifies the type of data service that the link uses for outgoing calls.
Ascend-Send-Auth (231)	For example, Send-Auth-PAP (1). This setting is optional.
Ascend-Send-Passwd (232)	For example, Ascend. This optional setting specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. If the value does not match the remote end's value (in the Connection > PPP Options > Recv-Password or in the RADIUS user profile), the remote system rejects the call.
Ascend-Data-Filter (242)	Optional setting that specifies the characteristics of a data filter in a RADIUS user profile. The TAOS unit uses the filter only when it places or receives a call associated with the profile that includes the filter definition. Following are typical settings. For more information about filters, see Chapter 9, "Packet Filters." IP Out Forward. This optional setting specifies an IP filter for filtering packets going out of the TAOS unit and specifies that the unit must forward each packet that matches the filter. Generic Out Forward 12 ffff 0806. This optional setting specifies a generic filter for filtering packets going out of the TAOS unit and specifies that the unit must forward each packet that matches the filter. This setting also specifies the offset, mask, and value. Generic Out Drop 0 0 0. This optional setting specifies a generic filter for filtering packets going out of the TAOS unit and specifies that the unit must drop each packet that matches the filter. This setting also specifies the offset, mask, and value.
Ascend-Route-IP (228)	Route-IP-Yes (1) or Route-IP-No (0). Route-IP-Yes (the default), enables IP routing for the profile. Route-IP-No disables IP routing the profile.

Configuring CBCP callback

Callback Control Protocol (CBCP) is an option negotiated during the Link Control Protocol (LCP) phase of PPP negotiation. Although you configure support for CBCP systemwide on a TAOS unit, not every connection must negotiate CBCP callback. This option is supported by parameters in the Answer-Defaults profile and in each Connection profile. The calling and called sides of a PPP session initiate authentication after acknowledging that CBCP is to be used.

The TAOS unit uses the username and password to link a caller with a specific Connection profile or RADIUS user profile. Configured CBCP parameters in the Connection profile specify variables for the callback. If, at any point, the client and the TAOS unit disagree about any CBCP parameters, the TAOS unit can drop the connection. TAOS units do not support sharing of a Connection profile or CBCP RADIUS profile by more than one Windows client.

Depending on the configuration, either the client or the TAOS unit can supply the callback telephone number.

In CBCP callback, a caller connects to the TAOS unit and LCP negotiations begin. The TAOS unit verifies that CBCP mode is set in the profile. If the caller and TAOS unit successfully negotiate the LCP option for CBCP, CBCP then begins after authentication. The caller authenticates itself to the TAOS unit. If authentication fails, the TAOS unit terminates the connection. During CBCP, the client also supplies to the TAOS unit the number of seconds (a configurable value) it must wait before initiating the callback and, if applicable, the telephone number. The TAOS unit delays the callback on the basis of the previous negotiation. The TAOS unit dials the client by applying the information from the same profile used during negotiation.

Global parameter configuration for CBCP callback

The global parameters are in the Answer-Defaults profile. The CBCP-Enable parameter and two analogous RADIUS attributes, Ascend-CBCP-Enable and Ascend-CBCP-Mode, support CBCP callback. The CBCP-Enable parameter enables the CBCP protocol for incoming PPP calls.

Following are typical global configuration settings for CBCP callback:

Answer-Defaults parameter	**Typical setting**
CLID-Auth-Mode	CLID-Require or DNIS-Require are not mandatory settings.
PPP-Answer > Enable	Yes.
PPP-Answer > Receive-Auth-Mode	Any-PPP-Auth.
PPP-Answer > CBCP-Enable	Yes is mandatory.

Local Connection profile configuration for CBCP callback

You specify local configuration within the Connection profile. Following are examples of typical Connection profile settings for CBCP callback, for a particular user:

Connection profile parameter	**Setting**
Active	Yes.
Encapsulation-Protocol	PPP. Encapsulation-Protocol can also be set to MP or MPP.
Dial-Number	If CBCP mode is set to CBCP-User-Number or CBCP-All, the callback telephone number can be given during callback negotiation. This setting can be left empty.
Telco-Options > Callback	No.
Telco-Options > Data-Service	For example, Modem.

Connection profile parameter	Setting
Telco-Options > Dialout-Allowed	Yes.
PPP-Options > Send-Auth-Mode	Not required. Used with Windows 95, Windows 98, Windows NT.
PPP-Options > Recv-Password	For example, Ascend.
PPP-Options > CBCP-Enabled	Yes.
PPP-Options > Trunk-Group-Callback-Control	For example, 9. If the caller supplies the telephone number, set this parameter to the value that the TAOS unit prepends to the number supplied by the user when calling back.
PPP-Options > Mode-Callback-Control	CBCP-User-Number. This parameter has the following possible values: CBCP-No-Callback, CBCP-User-Number, CBCP-Profile-Num, and CBCP-All.

External Connection profile configuration for CBCP callback

Following are typical RADIUS configurations for CBCP callback:

RADIUS attribute	Typical setting
Password (2)	Password for the CBCP user. For example, Ascend.
User-Service (6)	Framed-User (2)
Framed-Protocol (7)	PPP (1), MP (2) or MPP (256).
Ascend-Dial-Number (227)	Telephone number that the TAOS unit uses to call back when CBCP mode is set to CBCP-Profile-Num or CBCP-All.
Ascend-Data-Svc (247)	Usually Switched-Modem (42), for CBCP. This setting specifies the type of data service the link uses for outgoing calls.
Ascend-Send-Auth (231)	For example, Send-Auth-None (0). This setting is optional.
Ascend-CBCP-Enable (112)	CBCP-Enabled (1).
Ascend-CBCP-Mode (113)	CBCP-Profile-Callback (3).
Ascend-Assign-IP-Pool (218)	1 (the default). An integer that corresponds to an address pool. With a setting of 0, RADIUS chooses an address from any pool that has one available.
Ascend-Route-IP (228)	Route-IP-Yes (1) or Route-IP-No (0). Route-IP-Yes (the default) enables IP routing for the profile. Route-IP-No disables IP routing for the profile.

The Ascend-CBCP-Trunk-Group setting is not mandatory. The setting is useful when the caller enters the callback number and trunk groups are used.

Example of configuring callback after CLID authentication

The following commands define a Connection profile that uses CLID preauthentication and then calls back the far end:

```
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
```

Following is a comparable RADIUS profile:

```
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
```

Example of configuring callback after authentication

The following commands define a Connection profile that performs PPP authentication and then calls back the far end:

```
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
```

Following is a comparable RADIUS profile:

```
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
```

Authorization Options

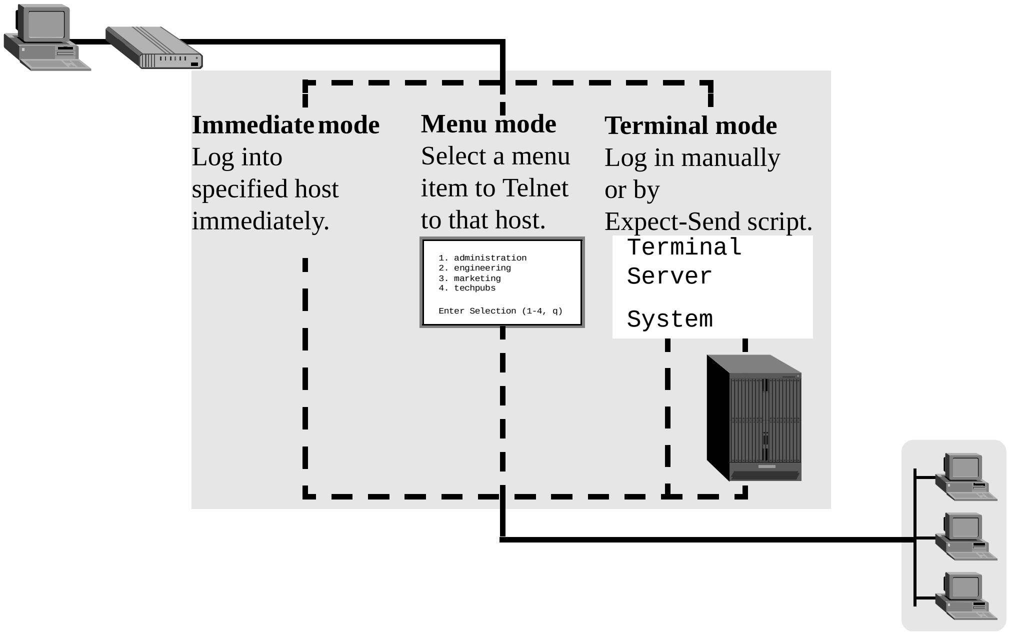
B

Authorization overview

Authorization procedures define what a user can do once he or she has access to your network. Authorization occurs *after* authentication has been completed. Dial-in users access the network through the terminal-server software or by using SNMP software. (For details about SNMP access, see “Authorizing SNMP management access” on page B-14.)

In most cases, the terminal server is used as a stepping stone toward logging in to a network host, rather than as an interface in its own right. It supports three dial-in access modes, each of which authorizes specific actions, as shown in Figure B-1.

Figure B-1. Terminal-server access modes



Immediate mode redirects the incoming data stream to a specified login host. Depending on the specified service, it can use a Telnet, TCP, or BSD-style Rlogin session to do so.

Menu mode displays a menu of authorized actions. If the call is RADIUS-authenticated, an administrator can set up a customized menu of authorized commands. For locally authenticated calls, the menu is limited to a number of login hosts.

Terminal mode accesses the terminal-server command line. Many sites do not authorize dial-in access to the prompt, because of the possible security risk. However, you can include a terminal-server command, such as SLIP or PPP, in the modem Expect-Send script, causing it to automatically execute the authorized command and invoke a packet-mode session as part of the login sequence. (For other commands, such as Telnet, TCP, or BSD-style Rlogin, immediate mode provides a more secure way of redirecting the incoming data stream.)

Authorizing immediate-mode login service

In immediate mode, the terminal server uses TCP, Rlogin, or Telnet to send the data stream of incoming calls directly to a host for a login session.

Using the Terminal-Server profile

Following are the parameters (shown with sample settings) required for setting up immediate mode:

```
[in TERMINAL-SERVER:immediate-mode-options]
service = telnet
telnet-host-auth = no
host = 10.2.3.4
port = 56
```

Parameter	Specifies
Service	Enable/disable immediate mode. Also specifies the service to use for logging in to the specified host. The default setting of None disables immediate mode. Other values are Telnet, Raw-TCP, and Rlogin.
Telnet-Host-Auth	Enable/disable handling of asynchronous PPP calls in immediate mode. With the No setting, asynchronous PPP calls fail. With the Yes setting, the terminal server directs asynchronous PPP calls to the specified host rather than to the router software.
Host	Hostname or IP address to which users will be connected in terminal-server immediate mode.
Port	TCP port number to use for the connections.

For example, the following commands enable immediate Telnet connections to the host address 10.2.3.4 for terminal-server connections, including asynchronous PPP connections:

```
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
```

If the incoming call is TCP-Clear (unencapsulated) or V.120, the call is authenticated in the terminal server as usual and then directed to the Telnet host, where the user logs in according to the login sequence used on that host.

If the incoming call uses PPP encapsulation, the normal course of events for the TAOS unit is to authenticate the call by means of PAP or CHAP and then use the router software to establish an asynchronous PPP session. To avoid redirection of the call to the router, so the user can log into the Telnet host instead, you must set the Telnet-Host-Auth parameter to Yes.

Using Connection profiles

You can enable immediate TCP connections globally in the Terminal-Server profile by using TCP service in immediate mode, as described in this section. Or, you can configure TCP-Clear for a specific connection, as described in “TCP-Clear connections” on page 1-23.

Using RADIUS profiles

RADIUS uses the following attribute-value pairs to specify an immediate-mode login:

RADIUS Attribute	Value
Login-Service (15)	Type of login service allowed to the caller. Valid values are Telnet (0), Rlogin (1), and TCP-Clear (2).
Login-Host (14)	IP address of the login host.
Login-TCP-Port (16)	Destination TCP port on the specified login host (an integer from 1 to 65535). The default is 23.
Service-Type (6)	Specifies whether the link can use framed or unframed services. Valid values are Login-User (1), Framed-User (2), and Outbound-User (5).

If you set the Login-Service attribute to Telnet or TCP-Clear, and you do not specify a value for the Login-Host attribute, the TAOS unit’s response depends on the value of the Auth-TS-Secure parameter in the Rad-Auth-Client subprofile of the External-Auth profile. If Auth-TS-Secure is set to Yes (the default), the TAOS unit drops the call. If Auth-TS-Secure is set to No, the TAOS unit allows the caller access to the terminal-server interface. For detailed information about the Auth-TS-Secure parameter, see the *APX 8000/MAX TNT Reference*.

Following is a RADIUS profile that specifies an immediate Telnet session for the user:

```
joel Password = "localpw"
   Service-Type = Login-User,
   Login-Service = Telnet
   Login-Host = 10.2.3.4,
   Login-TCP-Port = 56
```

Authorizing menu-mode access

In menu mode, the terminal server displays a menu of authorized hosts or, if the call is RADIUS-authenticated, a menu of authorized commands or other items. Users initiate a Telnet session by selecting a host from the menu.

Terminal-Server profile settings

Following are the parameters that enable you to describe up to four hosts that will be accessible to users in menu mode. (The settings shown are the defaults.)

```
[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 = ""
```

Parameter	**Specifies**
Start-With-Menus	Enable/disable menu mode after authentication. The Menu command in terminal mode can invoke menu mode regardless of this setting.
Toggle-Screen	Enable/disable toggling from menu mode to terminal mode. With a setting of Yes, users can press 0 (the zero key) in the menu to toggle to the terminal-server command line. See “Authorizing SNMP management access” on page B-14 for related issues.
Remote-Configuration	Enable/disable retrieval of the menu definition from RADIUS.
Text-*N*	Text description related to a host (typically a hostname or a description of the host).
Host-*N*	IP addresses for up to four hosts. The terminal server assigns each entry a number. When the user selects the number, the terminal server initiates a Telnet session to the host at the specified IP address.

Settings in a RADIUS initial-banner profile

An `initial-banner` profile is a pseudo-user profile in which the first line has the following format:

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

The optional *name* argument is the TAOS unit’s system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1.

Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the TAOS unit stops retrieving the profiles when it encounters the gap.

The following attribute-value pair can be used to define an `initial-banner` pseudo-user profile:

RADIUS Attribute	Value
Reply-Message (18)	Text description related to a host. The text can be a hostname, or can contain instructions or other helpful information.

Note: The Remote-Configuration parameter in Terminal-Server Menu-Mode-Options must be set to Yes for the terminal server to use the remote menu definition.

Examples of creating a menu of hosts

The following commands configure the menu shown in Figure B-2, and specify that the menu is displayed upon initial login:

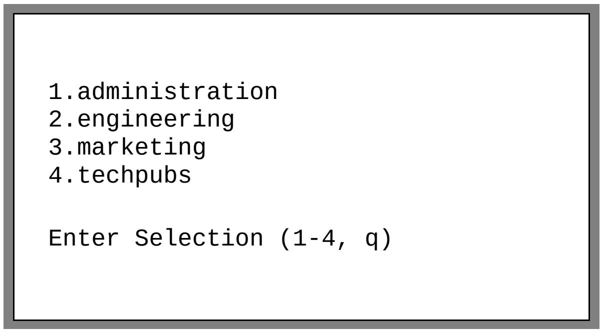
```
admin> read terminal
TERMINAL-SERVER read

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
```

Following is a comparable RADIUS `initial-banner` pseudo-user profile:

```
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"
```

With one of these configurations, the TAOS unit displays the menu as soon as it has authenticated the user’s login name and password.

Figure B-2. Terminal-server menu mode



```
1.administration
2.engineering
3.marketing
4.techpubs

Enter Selection (1-4, q)
```

Users can Telnet to the specified host by pressing 1, 2, 3, or 4, or can quit the menu by pressing Q. Quitting the menu terminates the connection. If the Toggle-Screen parameter were set to Yes, users could press 0 to exit menu mode and enter the terminal-server command line.

Creating a customized menu of commands (RADIUS only)

In RADIUS profiles, you can configure a custom menu of items from which the user can choose, and you can specify an input prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile. The menu items are displayed in the order in which they appear in the RADIUS profile.

When you specify a custom menu in a RADIUS profile, the user does not have access to the regular menu mode or to the terminal-server command line.

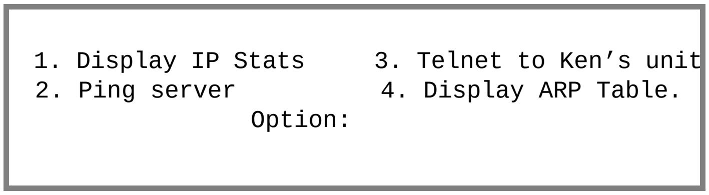
RADIUS uses the following attribute-value pairs to create a custom login menu:

RADIUS Attribute	**Value**
Ascend-Menu-Item (206)	Menu item that appears in lieu of the terminal-server prompt. Each item can include a command, a text string, and a pattern the user must type to select the menu item, separated by semicolons. The format is as follows: `"command;text;[match]"` The *command* is a string sent to the terminal server when the item is selected. It must be a valid terminal-server command. The *text* is a string that appears on the user's screen (up to 31 characters). The optional *match* is a pattern of up to 10 characters that the user must type to select the item. The TAOS unit considers blanks part of the matching pattern.
Ascend-Menu-Selector (205)	Prompt for user input in the custom menu interface. The default string is: `Enter Selection (1-`*`n`*`, q)` where *n* is the number of instances of Ascend-Menu-Item attributes in the profile.

For example, the following RADIUS profile defines the custom login screen shown in Figure 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:"
```

Figure B-3. Customized login screen for RADIUS user



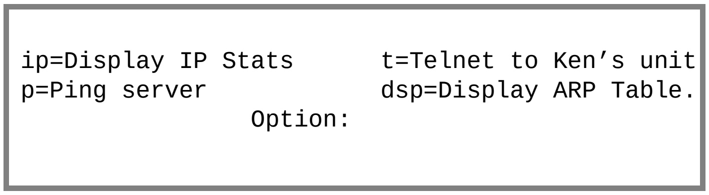
```
 1. Display IP Stats     3. Telnet to Ken’s unit
 2. Ping server          4. Display ARP Table.
                Option:
```

With the login screen shown in Figure B-3, the user has only four options. By selecting option 3, for example, the user Telnets to a local host. By selecting option 2, the user pings a server.

To modify the screen to display a unique string (a match pattern) instead of a number for each option, add the Ascend-Menu-Item definitions for the match patterns. For example, the following profile defines the custom login screen shown in Figure 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:"
```

Figure B-4. A customized login screen with match patterns



```
ip=Display IP Stats      t=Telnet to Ken’s unit
p=Ping server            dsp=Display ARP Table.
                Option:
```

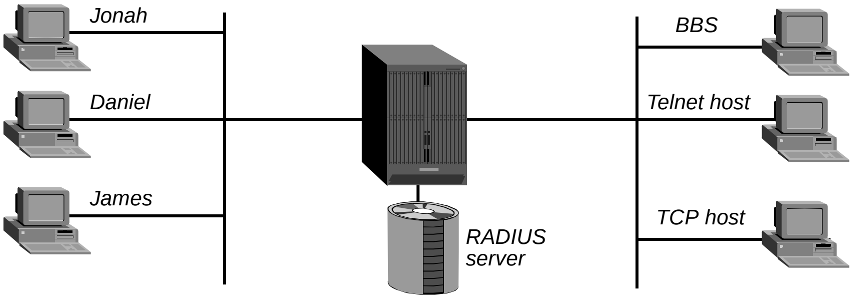
Note: Do not combine numeric menu selections with pattern matching. The first Ascend-Menu-Item attribute setting determines whether the screen displays numbered selections or patterns.

For detailed information about RADIUS, see the *TAOS RADIUS Guide and Reference*.

Extended example of RADIUS and menu mode

In the example illustrated in Figure B-5, a network administrator needs to set up a terminal-server menu that gives each user the choice of logging into a BBS or starting PPP, SLIP, or CSLIP. RADIUS is running on a UNIX server.

Figure B-5. An extended terminal-server example



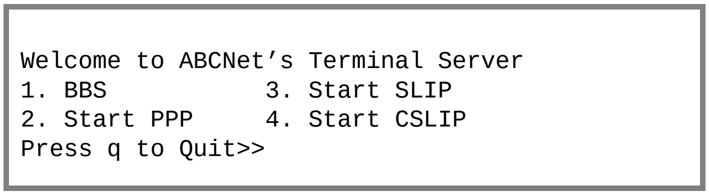
The RADIUS server uses the `DEFAULT` profile to determine the kind of access it grants to users who do not appear in the `users` file. You can configure only one `DEFAULT` profile in the `users` file. Make sure that the `DEFAULT` profile is last in the file. RADIUS ignores any profiles that follow the `DEFAULT` profile.

The first line of the user profile enables a terminal-server user to log in with his or her UNIX account name or password. The Reply-Message attribute provides introductory message text. The Ascend-Menu-Selector and Ascend-Menu-Item attributes provide the lines of menu text. In this example, you would configure the user profile as follows:

```
DEFAULT Password = "UNIX"
   Ascend-Idle-Limit = 1800,
   Framed-Routing = None,
   Framed-Compression = Van-Jacobsen-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",
   Ascend-Menu-Item = "slip;Start SLIP",
   Ascend-Menu-Item = "cslip;Start CSLIP"
```

Figure B-6 shows the text that appears on the terminal-server screen.

Figure B-6. Menu displayed when DEFAULT profile is used



```
Welcome to ABCNet’s Terminal Server
1. BBS            3. Start SLIP
2. Start PPP      4. Start CSLIP
Press q to Quit>>
```

Instead of using the `DEFAULT` profile, you can configure individual profiles to restrict users access to certain services. For example, if you want the user Emma to immediately establish an Rlogin session with `bbs.net` upon authentication, you might configure the following user profile:

```
Jonah Password = "UNIX"
   Service-Type = Login-User,
   Login-Host = bbs.net,
   Login-Service = Rlogin
```

To let new users sign up, you might configure a profile like the following:

```
Guest Password = "UNIX"
   Service-Type = Login-User,
   Login-Host = unix.bbs.net,
   Login-Service = Rlogin
```

When a user dials in as Guest, he or she immediately logs into the UNIX machine. The UNIX machine has a shell script in `/usr/local/bin/guest`, such as the following:

```
#!/bin/sh
echo Welcome to BBS.NET.
signup
```

The `signup` line refers to an interactive shell script you can write in order to gather introductory information, set up a temporary account for verification, and perform any other relevant tasks.

Authorizing terminal-mode logins

Typically, administrators set up terminal mode to negotiate a user-to-host session as part of the dial-in Expect-Send script. Instead of providing only the login and password needed to authenticate a Connection profile, the script also includes the terminal-server prompt and a command, such as PPP, SLIP, Telnet, or Rlogin. In this way, the session to a host is invoked as part of the login process, so the user never actually sees the command-line prompt.

TCP, Rlogin, or Telnet connections in terminal mode

By default, the Terminal-Server profile disables the use of the TCP, Rlogin, and Telnet commands, because immediate mode provides those commands in a more secure fashion. However, you can enable them in terminal mode to allow users to log in and initiate a login from the command line or to initiate the login as part of an Expect-Send script, such as the following:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend%" send "telnet 10.1.2.3"
```

For information about using immediate mode instead of terminal mode, see “Authorizing immediate-mode login service” on page B-2.

Authorizing use of the commands

The following Terminal-Server parameters (shown with default settings) disable initiation of TCP, Rlogin, and Telnet connections in terminal mode:

```
[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
```

Parameter	Specifies
TCP	Enable/disable the TCP command, which initiates a TCP session to a specified host. The command is disabled by default.
Rlogin	Enable/disable the Rlogin command, which initiates a remote login session to a specified host. The command is disabled by default.
Telnet	Enable/disable the Telnet command, which initiates a Telnet session to a specified host. The command is disabled by default.

The following commands enable the use of the Telnet and Rlogin commands from the terminal-server prompt:

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

admin> set terminal telnet telnet = yes

admin> set terminal rlogin rlogin = yes

admin> write
TERMINAL-SERVER written
```

Configuring the Rlogin source port range

Administrators can configure the Rlogin port range by using the following parameters (shown with their default settings):

```
[in TERMINAL-SERVER:terminal-mode-configuration:rlogin-options]
max-source-port = 1023
min-source-port = 128
```

Parameter	Specifies
Max-Source-Port	Highest Rlogin source port. Its value must be from 128 to 1023, and should be greater than or equal to the value of Min-Source-Port. The default value is 1023.
Min-Source-Port	Lowest Rlogin source port. Its value must be from 128 to 1023, and should be less than or equal to the value of Max-Source-Port. The default value is 128. To use with BSD Rlogin, set this value to 512.

For example, the following commands configure a valid source port range from 512 to 1023:

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

admin> set terminal rlogin min-source-port = 512

admin> write
TERMINAL-SERVER written
```

The Slot command reports unavailability of ports or an incorrectly configured range. The following message indicates that all ports in the configured range are in use:

```
"no connection: no port available, connection was refused."
```

The following messages indicate that the source port range is configured incorrectly:

```
"error: max-source-port should be greater than or equal to min-source-
port"
"error: Value (1024) out of range [128 - 1023]"
```

Setting defaults for Telnet sessions

In addition to the Telnet parameter, which enables Telnet sessions in terminal mode, the following parameters set default values for Telnet sessions. The settings do not override selections a user might make on a per-session basis when executing the Telnet command.

```
[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
```

Parameter	Specifies
Terminal-Type	Terminal type, such as the VT100, for the Telnet session.
Clear-Call	Enable/disable termination of the connection when a user terminates a Telnet session.
Buffer-Chars	Enable/disable the holding of input characters in a buffer for 100 milliseconds before forwarding them to the host. The alternative is to send input characters as they are received.
Telnet-Mode	Binary, ASCII, or Transparent mode.
Auto-Telnet	Enable/disable initiation of a Telnet session when a user enters a hostname at the command-line prompt. As a side-effect, when Auto-Telnet is set to Yes the system interprets an unknown command string as the name of a host for a Telnet session.
Local-Echo	Enable/disable echoing of characters locally. Users can change the echo setting within an individual Telnet session.

Following is an example in which an administrator configures some of the session parameters:

```
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
```

PPP and SLIP sessions in terminal mode

By default, the Terminal-Server profile disables the use of the PPP command, because callers typically use PPP dial-in software for a framed-protocol session. However, you can enable callers who do not have PPP software to start a PPP session as part of an Expect-Send script. For example:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend% " send "PPP"
```

Some applications require SLIP rather than PPP. The TAOS unit does not support a direct SLIP dial-in, because SLIP does not support authentication. However, if SLIP is enabled in the terminal server, users can initiate a SLIP session and then run an application such as FTP in that session. To initiate SLIP, the user must invoke a session in terminal mode. For example:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend% " send "SLIP"
```

Authorizing use of the commands

The following parameters (shown with default settings) authorize PPP and SLIP sessions in terminal mode:

```
[TERMINAL-SERVER:ppp-mode-configuration]
ppp = no
```

```
[in TERMINAL-SERVER:slip-mode-configuration]
slip = no
```

Parameter	**Specifies**
PPP	Enable/disable the PPP command, which initiates a PPP session. The command is disabled by default.
SLIP	Enable/disable the SLIP command, which initiates a SLIP session. The command is disabled by default.

For example, the following commands enable PPP and SLIP sessions:

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

admin> set ppp ppp = yes

admin> set slip slip = yes

admin> write
TERMINAL-SERVER written
```

Setting defaults for PPP sessions

In addition to the PPP parameter, which enables PPP sessions in terminal mode, the following parameters set default values for PPP sessions:

```
[TERMINAL-SERVER:ppp-mode-configuration]
delay = 5
```

```
direct = no
info = session-ppp
```

Parameter	Specifies
Delay	Number of seconds to delay before transitioning from login to packet-mode processing.
Direct	Enable/disable direct PPP negotiation after using the PPP command. By default, the terminal server waits to receive a PPP packet before beginning PPP negotiation.
Info	Enable/disable display of an informational message when the user enters PPP mode. With a setting of Session-PPP, the system displays `PPP Session`. With a setting of Mode-PPP, it displays `PPP Mode`.

The following commands set the system to start PPP negotiation immediately after the PPP command is executed:

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

admin> set ppp ppp = yes

admin> set ppp direct = yes

admin> write
TERMINAL-SERVER written
```

Setting defaults for SLIP sessions

In addition to the SLIP parameter, which enables SLIP sessions in terminal mode, the following parameters set default values for SLIP sessions:

```
[in TERMINAL-SERVER:slip-mode-configuration]
slip-bootp = no
info = basic-slip
```

Parameter	Specifies
SLIP-BOOTP	Enable/disable response to BOOTP within SLIP sessions. With a Yes setting, a user who initiates a SLIP session can get an IP address from the designated IP address pool by means of BOOTP. With a No setting, the terminal server does not run BOOTP. Instead, the system prompts the user to accept an IP address at the start of the SLIP session.
Info	Enable/disable display of an informational message when the user enters SLIP mode. With a Basic-SLIP setting, a default startup message is displayed. With an Advanced-SLIP slip, the message includes the caller’s subnet mask and IP gateway address.

The following commands enable the terminal server to respond to BOOTP in SLIP sessions:

```
admin> read term
TERMINAL-SERVER read

admin> set slip slip-bootp = yes
admin> write
TERMINAL-SERVER written
```

Allowing users to dial in to the terminal-server interface

Some sites provide callers access to the terminal-server command line and restrict which commands are accessible. If you decide to allow access to the terminal-server command line, you might want to assign the terminal server its own password, to protect the command line from unauthorized access.

Note: For details about logging into the terminal-server command line, see “Authenticating user login sessions” on page A-21.

Authorizing SNMP management access

SNMP management software that uses the Ascend Enterprise MIB and has IP connectivity with the TAOS unit can perform administrative tasks, including reconfiguring the TAOS unit. It is important to restrict this type of access to trusted management stations. Following are the relevant SNMP parameters (shown with their default settings):

```
[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 = ""
```

Parameter	Specifies
Enabled	Enable/disable SNMP access. The default of No prevents SNMP managers from accessing the unit.
Read-Community	Password (up to 32 characters) to be required for Read access by an SNMP manager. Read access enables the use of the SNMP GET command. The default password is the well-known string `public`.
Read-Write-Community	Password (up to 32 characters) to be required for Read-Write access by an SNMP manager. Read-Write access enables the use of the SNMP Get and Set commands. The default is the well-known string `write`.
Enforce-Address-Security	Enable/disable address security, which excludes SNMP management unless it is initiated from a specified IP address.
Read-Access-Hosts	Array of up to five IP addresses from which SNMP managers can access the unit with Read (Get) permission.
Write-Access-Hosts	Array of up to five IP addresses from which SNMP managers can access the unit with Read-Write (Get or Set) permission.
Contact	Name of a person to contact about the TAOS unit (SNMP readable and settable).
Location	Where the unit is located (SNMP readable and settable).

For example, the following commands enable access by SNMP management utilities:

```
admin> read SNMP
SNMP read

admin> set enabled = yes

admin> write
SNMP written
```

Setting community strings

Once you have enabled access by SNMP managers, you must set a secret Read-Write community string or limit access by using address security. *Otherwise, unauthorized management stations will be able to reconfigure the unit.*

The following commands assign a confidential Read-Write-Community string:

```
admin> read snmp
SNMP read

admin> set read-write-community = secret

admin> write
SNMP written
```

Setting up and enforcing address security

If the Enforce-Address-Security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If it is set to Yes, the TAOS unit checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the Read-Access-Host and Write-Access-Host arrays.

The following commands enforce address security and specify trusted addresses for both Read and Write access:

```
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

admin> set write-access-hosts 4 = 10.1.1.4

admin> set write-access-hosts 5 = 10.1.1.5

admin> write
SNMP written
```

Index