MAX TNT Network Configuration Guide

Ascend Communications, Inc.
Part Number: 7820-0547-003
For Software Version 7.0.0 or earlier

Ascend Customer Service

Ascend Customer Service provides a variety of options for obtaining technical assistance, information about Ascend products and services, and software upgrades.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, or modem, or over the Internet. If you need to contact Ascend for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model.
- Software and hardware options.
- Software version.
- Type of computer you are using.
- Description of the problem.

Calling Ascend from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Ascend Advantage Pak service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-ASND (2763) to reach Ascend's Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than three minutes.

Ascend Advantage Pak

Ascend Advantage Pak is a one-year service contract that includes overnight advance replacement of failed products, technical support, software maintenance releases, and software update releases. For more information, call (800) ASCEND-4 (272-3634), or access Ascend's Web site at `www.ascend.com` and select Services and Support, then Advantage Service Family.

Other telephone numbers

For a menu of Ascend's services, call (800) ASCEND-4 (272-3634). Or call (510) 769-6001 for an operator.

Calling Ascend from outside the United States

You can contact Ascend by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Asia Pacific (except Japan)	(+61) 3 9656 7000

Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For the Asia Pacific Region, you can find additional support resources at

`http://apac.ascend.com/contacts.html`

Obtaining assistance through correspondence

Ascend maintains two email addresses for technical support questions. One is for customers in the United States, and the other is for customers in Europe, the Middle East, and Asia. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Ascend's U.S. offices. Following are the ways in which you can reach Ascend Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe or the Middle East—EMEAsupport@ascend.com
- Email from Asia Pacific—apac.support@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302
- Write to Ascend at the following address:

  Attn: Customer Service
  Ascend Communications, Inc.
  One Ascend Plaza
  1701 Harbor Bay Parkway
  Alameda, CA 94502-3002

Finding information and software on the Internet

Visit Ascend's Web site at `http://www.ascend.com` for technical information, product information, and descriptions of available services.

Visit Ascend's FTP site at `ftp.ascend.com` for software upgrades, release notes, and addenda to this manual.

Contents

Ascend Customer Service iii

Chapter 1 Introduction 1-1

What is in this guide 1-1
What's new in this guide 1-2
What you should know 1-3
Related publications 1-3
Related RFCs 1-3
ITU-T recommendations 1-5
Related books 1-5
Documentation conventions 1-6

Chapter 2 WAN Connections 2-1

Introduction to WAN connections 2-1
Types of encapsulation protocols 2-1
How the system answers and authenticates dial-in calls 2-2
How the system initiates dial-out calls 2-2
How the system establishes and monitors sessions 2-3
Spanning cards and shelves for multichannel calls 2-3
System-wide profiles 2-3
Answer-Defaults profile 2-3
Default RADIUS settings 2-4
Requiring authentication for PPP calls 2-4
V.120 settings 2-4
Terminal-Server profile 2-5
External-Auth profile 2-6
Local and external authentication profiles 2-7
Using Connection profiles 2-7
Using RADIUS 2-7
Specifying session time limits 2-8
Settings in a Connection profile 2-8
Settings in a RADIUS profile 2-9
Examples of setting time limits 2-9
Using session accounting 2-10
Configuring switched dial-in connections 2-10
Single-channel PPP connections 2-10
Settings in a Connection profile 2-10
Settings in a RADIUS profile 2-11
Password authentication 2-11
Link compression methods 2-11
Link Quality Monitoring 2-12
Examples of a synchronous PPP connection 2-13

Examples of an asynchronous PPP connection 2-13
Multilink Protocol (MP) connections 2-14
Settings in a Connection profile 2-14
Settings in a RADIUS profile 2-15
Examples of an MP connection 2-15
MP bonding of analog calls 2-16
Multilink Protocol Plus (MP+) connections 2-17
How Ascend units add bandwidth 2-17
Settings in a Connection profile 2-18
Settings in a RADIUS profile 2-19
Examples of an MP+ configuration 2-20
TCP-Clear connections 2-21
Performance enhancements for TCP-Clear calls (local profiles only) 2-21
Settings in a Connection profile 2-21
Settings in a RADIUS profile 2-23
Examples of TCP-Clear connections 2-23
Example of TCP-Clear with packet buffering (local profiles only) 2-24
X.75 connections 2-25
Configuring nailed and nailed/MP+ connections 2-26
Nailed connections 2-26
Settings in a Connection profile 2-26
Settings in a RADIUS profile 2-27
Examples of a nailed connection 2-28
Nailed MP+ connections 2-29
Settings in a Connection profile 2-29
Settings in a RADIUS profile 2-29
Examples of a nailed MP+ connection 2-30
Backup interfaces for nailed connections 2-31
Settings in a Connection profile 2-31
Settings in a RADIUS profile 2-31
Examples of a switched backup interface 2-32
Configuring dial-out connections 2-34
About RADIUS dial-out profiles 2-34
Configurable dial-out timer 2-35
Dial-out PPP and multichannel PPP profiles 2-35
Settings in a Connection profile 2-35
Settings in a RADIUS profile 2-36
Password authentication 2-36
Examples of a dial-out PPP connection 2-37
Modem dial-out connections 2-38
System reset requirement 2-38
Enabling Modem Direct-Access 2-38
Example of Direct-Access using a global password 2-39
Dial-out modem connections that require profiles 2-40

Chapter 3 Frame Relay 3-1

Introduction 3-1
Frame Relay link management 3-2
Using the MAX TNT as a Frame Relay concentrator 3-2
Using the MAX TNT as a Frame Relay switch 3-3
Components of a Frame Relay configuration 3-3

Configuring nailed bandwidth for Frame Relay 3-3
Defining Frame Relay link operations 3-6
Overview of datalink options 3-6
Settings in a Frame-Relay profile 3-6
Settings in a RADIUS frdlink profile 3-8
Examples of a UNI-DTE link interface 3-10
Examples of a UNI-DCE link interface 3-11
Examples of an NNI link interface 3-12
Configuring a DLCI logical interface 3-14
Overview of DLCI interface settings 3-14
Settings in a Connection profile 3-14
Settings in a RADIUS profile 3-14
Examples of a DLCI interface configuration 3-15
Examples of backup interfaces for nailed Frame Relay links 3-16
Concentrating incoming calls onto Frame Relay 3-18
Setting up a Frame Relay gateway 3-18
Routing parameters in the DLCI profile 3-18
Routing parameters in RADIUS 3-19
Examples of a gateway configuration 3-19
Configuring Frame Relay Direct 3-20
Settings in a Connection profile 3-20
Settings in a RADIUS profile 3-21
Examples of FR-Direct connections 3-22
Configuring the MAX TNT as a Frame Relay switch 3-24
Overview of circuit-switching options 3-24
Settings in a Connection profile 3-24
Settings in a RADIUS profile 3-25
Examples of a circuit between UNI interfaces 3-25
Using local profiles 3-26
Using RADIUS profiles 3-27
Examples of a circuit between NNI interfaces 3-27
Using local profiles 3-27
Using RADIUS profiles 3-28
Examples of circuits that use UNI and NNI interfaces 3-29
Using local profiles 3-29
Using RADIUS profiles 3-31
Configuring an ATM-Frame Relay circuit 3-32
Settings in a Connection profile 3-33
Settings in a RADIUS profile 3-34
Examples of configuring an ATM-Frame Relay circuit 3-35
Using local profiles 3-35
Using RADIUS profiles 3-36

Chapter 4 IP Routing 4-1

Routing overview 4-1
Routes and interfaces 4-1
Displaying the routing table 4-2
Displaying the interface table 4-3
Ascend notation for IP addresses 4-4
Configuring LAN IP interfaces 4-6
Overview of LAN interface settings 4-6
Example of configuring a LAN IP interface 4-7

Enabling proxy ARP 4-8
Enabling RIP 4-8
Example of defining virtual LAN interfaces 4-9
Example of defining the interface-independent IP address 4-9
Example of disabling directed broadcasts 4-10
Example of defining a management-only interface 4-11
Configuring WAN IP interfaces 4-11
Overview of WAN interface settings 4-11
Settings in Connection profiles 4-12
Settings in RADIUS profiles 4-14
Examples of a connection to another IP router 4-16
Examples of a host route connection 4-17
Examples of a numbered-interface connection 4-18
Examples of an IP-Direct connection 4-19
Examples of making the route to a connection private 4-20
Examples of client default gateways 4-21
Examples of per-session source address checking 4-21
Examples of setting QoS and TOS policy 4-22
Configuring static IP routes 4-23
Overview of static route settings 4-23
Settings in IP-Route profiles 4-23
Settings in a RADIUS route profiles 4-24
Route settings in a RADIUS user profile 4-25
Connection-specific private static routes (RADIUS only) 4-25
Examples of configuring default routes 4-26
Examples of a LAN-based default route 4-26
Examples of a default route across a WAN link 4-27
Examples of configuring a route to a remote subnet 4-27
Examples of configuring a multipath route 4-28
Examples of private static routes 4-29
Setting TCP/IP routing policies 4-30
Setting a system source IP address 4-30
Setting router security policies 4-31
Requiring acceptance of dynamic address assignment 4-31
Shared profiles 4-32
Restricting Telnet access to the system: 4-32
Setting system-wide routing policies 4-33
Ignoring ICMP packets 4-33
Dropping source-routed packets 4-34
Setting static route preferences 4-34
Setting routing protocol options 4-34
RIP policy for propagating updates back to the originating subnet 4-35
RIP triggering 4-36
Setting the preference value for routes learned from RIP updates 4-36
Poisoning routes to force the use of a redundant Ascend unit 4-36
Limiting the size of UDP packet queues 4-37
Ignoring default routes when updating the routing table 4-37
Suppressing host-route advertisements 4-38
Setting IP route and IP port cache options 4-38
Route caches 4-39
Port caches 4-39
Enabling protocol options 4-39

Enabling Bootstrap Protocol and Reverse-ARP 4-40
Enabling UDP checksums 4-41
Setting a TCP timeout 4-41
Enabling response to Finger queries 4-42
Enabling BOOTP-Relay 4-42
Using SNTP to set and maintain the MAX TNT system time 4-43
Configuring DNS 4-43
Configuring DNS lookups and DNS list 4-44
Specifying domain names for lookups 4-44
Specifying local DNS server addresses 4-45
Supporting DNS list 4-45
Setting up a local DNS table 4-45
Host name matching 4-46
Defining the local table 4-47
Using the Auto-Update feature 4-48
Using client DNS 4-49
Overview of client DNS settings 4-49
Example of configuring client DNS servers at the system level 4-50
Examples of configuring client DNS at the connection level 4-51
Configuring and using address pools 4-51
Overview of settings for defining pools 4-51
Settings in the IP-Global profiles 4-51
Settings in RADIUS pseudo-user profiles 4-52
Global RADIUS pools (RADIPAD) 4-52
Examples of configuring address pools 4-54
Examples of configuring summarized address pools 4-55
Setting the Pool-Summary flag 4-55
Defining network-aligned pools 4-55
Examples of assigning an address from a pool 4-56
Setting up multicast forwarding 4-58
Global settings for enabling multicast forwarding 4-58
Specifying a timeout for group memberships 4-59
Monitoring the multicast traffic heartbeat 4-60
Configuring the MBONE interface 4-61
Overview of MBONE interface settings 4-61
Example of a local MBONE router 4-61
Example of an MBONE router on a WAN interface 4-62
Configuring multicast client interfaces 4-63
Settings in local IP-Interface and Connection profiles 4-63
Settings in RADIUS profiles 4-64
Setting the multicast rate limit 4-64
Specifying a delay for clearing IGMP groups 4-64
Example of configuring a LAN multicast client interface 4-65
Examples of configuring WAN multicast client interfaces 4-65
Configuring virtual routers 4-67
How VRouters affect the routing table 4-67
How VRouters affect network commands 4-67
Current limitations 4-68
Creating a VRouter 4-68
Settings in a VRouter profile 4-69
Example of defining a VRouter 4-69
Viewing the VRouter's routing and interface tables 4-70

Defining address pools for a VRouter 4-72
Assigning interfaces to a VRouter 4-72
Settings in local profiles 4-72
Settings in RADIUS profiles 4-73
Examples of assigning VRouter membership to interfaces 4-73
Viewing assigned interfaces in the VRouter's tables 4-74
Defining VRouter static routes 4-74
Settings in an IP-Route profile 4-75
Settings in RADIUS profiles 4-75
Examples of defining a route on a per-VRouter basis 4-75
Viewing the static route in the VRouter's table 4-75
Specifying an inter-VRouter route 4-76
Viewing the inter-VRouter route in the global table 4-76
Deleting a VRouter 4-77

Chapter 5 OSPF Routing 5-1

Introduction to OSPF 5-1
RIP limitations solved by OSPF 5-1
Distance-vector metrics 5-1
15-hop limitation 5-1
Excessive routing traffic and slow convergence 5-2
Ascend implementation of OSPF 5-2
Limited border router capability 5-2
Authentication 5-2
One active IP interface per port 5-2
OSPF diagnostic commands 5-3
OSPF features 5-3
Security 5-3
Support for variable length subnet masks 5-3
Interior gateway protocol (IGP) 5-4
Exchange of routing information 5-4
Designated and Backup Designated Routers 5-4
Configurable cost metrics 5-5
Hierarchical routing (areas) 5-6
The link-state routing algorithm 5-7
Adding the MAX TNT to an OSPF network 5-9
System reset requirement 5-9
Overview of LAN and WAN OSPF settings 5-9
Example of configuring a LAN OSPF interface 5-11
Examples of configuring WAN OSPF interfaces 5-12
Example of integrating a RIP-v2 interface 5-13
Configuring route options 5-14
Example of importing a summarized pool as an ASE 5-15
Example of setting ASE preferences 5-16
Configuring OSPF static route information 5-16
Example of configuring a Type-7 LSA in an NSSA 5-17
Example of assigning a cost to a static route 5-18
Example of specifying a third-party route 5-18

Chapter 6 Ascend Tunnel Management Protocol 6-1

Introduction to ATMP 6-1
Network settings for ATMP 6-2
System reset requirement 6-2
System IP address recommendation 6-2
Setting the UDP port 6-3
Specifying tunnel retry limits 6-4
Setting an MTU limit 6-4
How link compression affects the MTU 6-4
How ATMP tunneling causes fragmentation 6-5
Pushing the fragmentation task to connection end-points 6-5
Forcing fragmentation for interoperation with outdated clients 6-5
Network isolation and duplicate IP addresses 6-6
Configuring the agent-to-agent connection 6-7
Configuring a Foreign Agent 6-7
Foreign Agent ATMP profile settings 6-7
Mobile client profile settings 6-8
Settings in Connection profiles 6-8
Settings in RADIUS profiles 6-9
Specifying Home Agent addresses and port numbers 6-10
Specifying the home network name 6-11
Example of a Foreign Agent configuration 6-11
Setting the Foreign Agent system address 6-12
Configuring the Foreign Agent ATMP profile 6-12
Configuring a connection to the Gateway Home Agent 6-12
Configuring a connection to the Router Home Agent 6-13
Configuring a mobile-client connection to the Gateway Home Agent 6-14
Configuring a mobile-client connection to the Router Home Agent 6-14
Example of a Foreign Agent that tunnels to a GRF switch 6-15
Configuring Home Agents 6-16
Home Agent ATMP profile settings 6-16
Specifying a Gateway Home Agent 6-17
Specifying a Router Home Agent 6-17
Specifying the tunnel password 6-18
Setting an idle timer for unused tunnels 6-18
Home network gateway profile settings 6-19
Limiting the maximum number of tunnels 6-19
Enabling RIP on the interface to the home router 6-19
Example of a Gateway Home Agent configuration 6-21
Setting the Home Agent's system address 6-22
Configuring the Home Agent ATMP profile 6-22
Configuring a gateway profile for connection to the home network 6-22
Configuring a mobile client connection to the Gateway Home Agent 6-23
Example of a Router Home Agent configuration 6-23
Setting the Home Agent's system address 6-23
Configuring the IP-Interface profile to the home network 6-24
Configuring the Home Agent's ATMP profile 6-24
Configuring a mobile client connection to the Router Home Agent 6-24
Configuring a Home-and-Foreign-Agent 6-25
Configuring the ATMP profile 6-25
Example of a Home-and-Foreign-Agent configuration 6-25
Setting the system address 6-26

Configuring the ATMP profile for Home-and-Foreign Agent 6-26
Configuring a mobile client profile 6-27
Another example of a Home-and-Foreign-Agent configuration 6-28
Setting the system IP address 6-28
Configuring the ATMP profile for Home and Foreign Agent 6-28
Configuring a profile for Mobile-Client-3 6-29
Configuring IPX over ATMP 6-29
Configuring the agents for IPX routing 6-30
Example of IPX ATMP to a Gateway Home Agent 6-30
Configuring a mobile client IPX connection 6-31
Example of a gateway profile IPX connection 6-31
IPX home router requirements 6-32
Example of IPX ATMP to a Router Home Agent 6-33
Configuring a mobile client IPX connection 6-33
Example of an IPX Router Home Agent configuration 6-34

Chapter 7 L2TP, PPTP, and IP-in-IP Tunneling 7-1

Layer 2 Tunneling Protocol (L2TP) 7-1
Components of an L2TP tunnel 7-1
Configuring L2TP operations 7-2
Configuring a connection to the LNS 7-3
Configuring L2TP mobile client profiles 7-3
L2TP settings in Connection profiles 7-4
L2TP settings in RADIUS profiles 7-4
Examples of opening a tunnel after pre-authenticating the call 7-4
Examples of opening a tunnel after password authentication 7-5
Point-to-Point Tunneling Protocol (PPTP) 7-6
Components of a PPTP tunnel 7-6
Configuring PPTP operations 7-7
Configuring a connection to the PNS 7-8
Configuring PPTP mobile client profiles 7-8
PPTP settings in Connection profiles 7-9
PPTP settings in RADIUS profiles 7-9
Examples of opening a tunnel after pre-authenticating the call 7-9
Examples of opening a tunnel after password authentication 7-10
IP-in-IP encapsulation 7-11
Settings in a Connection profile 7-11
Settings in a RADIUS profile 7-12
Examples of an IP-in-IP connection 7-12

Chapter 8 IPX Routing 8-1

IPX routing on the WAN 8-1
How Ascend units use IPX SAP 8-1
How Ascend units use IPX RIP 8-1
How IPX RIP works 8-2
The IPX RIP default route 8-2
Support for IPXWAN negotiation 8-2
Extensions to standard IPX 8-2
Recommendations for NetWare client software 8-3
Configuring the IPX-Global profile 8-4
Defining a virtual IPX network for dial-in clients 8-4

Example of an IPX-Global configuration 8-4
Configuring LAN IPX interfaces 8-5
Overview of LAN IPX settings 8-5
Enabling IPX routing and spoofing on the interface 8-6
Assigning an IPX network number 8-6
Propagating IPX type 20 packets on a LAN interface 8-6
Example of an IPX-Interface configuration 8-6
Configuring WAN IPX interfaces 8-7
Overview of IPX connection settings 8-7
Settings in Connection profiles 8-7
Settings in RADIUS profiles 8-8
Specifying whether the remote device is a router or dial-in client 8-8
Answer-Defaults IPX Peer-Mode setting 8-9
Controlling RIP and SAP updates to and from the remote router 8-9
When to use net-number and net-alias 8-9
Using dial-query 8-9
Home server proxy 8-10
Examples of a connection to a Novell LAN 8-10
Examples of a connection to a dial-in client 8-11
Configuring static IPX routes 8-12
Overview of IPX route settings 8-13
Settings in local IPX-Route profiles 8-13
Settings in RADIUS ipxroute profiles 8-14
Socket numbers in static routes 8-15
Examples of a static IPX route 8-15
Defining and applying IPX SAP filters 8-15
Overview of IPX SAP filter settings 8-16
Example of filtering a file server from the SAP table 8-17
Example of filtering remote NetWare services from the SAP table 8-17
Example of applying a SAP filter to a LAN interface 8-17
Example of applying a SAP filter to a WAN interface 8-17

Chapter 9 AppleTalk Routing and Remote Access 9-1

Introduction 9-1
Configuring the Atalk-Global profile 9-1
Configuring LAN AppleTalk interfaces 9-2
Example of configuring a seed router 9-2
Configuring a nonseed router 9-3
Configuring WAN AppleTalk interfaces 9-4
Settings in the Answer-Defaults profile 9-4
Settings in a Connection profile 9-4
Settings in a RADIUS profile 9-5
Examples of configuring an ARA client connection 9-6
Examples of configuring a PPP AppleTalk dial-in 9-6
Examples of configuring a connection to an AppleTalk router 9-7
Examples of an IP over AppleTalk connection 9-8

Chapter 10 Ascend Packet Filters 10-1

Filter overview 10-1
Basic types of filters 10-1
Data and call filters 10-2

How filters work 10-3
Generic filters 10-3
IP filters 10-3
Type of Service filters 10-4
IPX filters 10-4
Route filters 10-5
Specifying a filter's direction 10-5
Specifying a filter's forwarding action 10-6
Defining generic filters 10-6
Settings in a local Filter profile 10-7
Settings in a RADIUS profile 10-8
Specifying the offset to the bytes to be examined 10-8
Specifying the number of bytes to test 10-9
Masking the value before comparison 10-9
Examples of a generic call filter 10-10
Defining IP filters 10-11
Settings in a local Filter profile 10-11
Settings in a RADIUS profile 10-12
Filtering by source or destination address 10-13
Filtering by port numbers 10-14
Examples of an IP filter to prevent local address spoofing 10-14
Examples of an IP filter for more complex security issues 10-15
Defining Type-of-Service filters 10-17
Settings in a local Filter profile 10-17
Settings in a RADIUS profile 10-19
Examples of defining a TOS filter 10-20
Defining IPX filters 10-21
Filtering by source or destination address 10-22
Filtering by socket number 10-23
Example of an outbound IPX filter 10-23
Example of an inbound IPX filter 10-23
Defining route filters 10-24
Example of a filter that excludes a route 10-25
Example of a filter that configures a route's metric 10-25
Applying a filter to an interface 10-26
Settings in local profiles 10-26
Settings in RADIUS profiles 10-27
How the system uses Answer-Defaults profile settings 10-27
Examples of applying a data filter to a WAN interface 10-28
Examples of applying a call filter to a WAN interface 10-29
Examples of applying a TOS filter to a WAN interface 10-29
Examples of applying a route filter to a WAN or LAN IP interface 10-30
Example of applying a filter to a LAN interface 10-30

Appendix A Authentication Methods A-1

Introduction A-1
Password authentication for framed protocol sessions A-1
Authentication of terminal-server logins A-2
Token card password authentication A-2
Pre-authentication using call information A-2
Using callback for added security A-2

RADIUS password handling A-2
Reserved RADIUS passwords A-3
Password expiration A-3
The DEFAULT user profile A-5
Shared secrets and secure exchanges A-5
Authenticating framed protocol sessions A-6
Specifying an authentication protocol required for dial-in calls A-6
How PAP works A-7
How CHAP and MS-CHAP work A-7
Requesting a protocol for use in dial-out calls A-8
Settings in Connection profiles A-8
Settings in RADIUS profiles A-8
Examples of requesting CHAP for a dial-out call A-9
Authenticating user login sessions A-9
Expect-Send login scripts A-10
Terminal-server security mode A-10
Customizing the login sequence A-11
Specifying the banner and prompts A-12
When to use the third prompt A-12
Token card authentication A-13
Enhanced security with token cards A-13
A simple method of authenticating token-card calls A-14
Authenticating token-card connections from Ascend units A-15
Configuring the MAX TNT as the NAS A-16
How the dial-in user displays and responds to challenges A-16
Configuring RADIUS profiles for token-card authentication A-16
Using ACE authentication for network users A-20
Tunnel authentication A-21
Authenticating ATMP tunnels A-21
Authenticating L2TP tunnels A-22
Pre-authentication (CLID or DNIS) A-23
Configuring the MAX TNT to extract and use call information A-23
Specifying the Disconnect Cause Element (RADIUS only) A-24
Configuring profiles for CLID or DNIS authentication A-24
Settings in Connection profiles A-24
Settings in RADIUS profiles A-25
Example of using Caller-ID as a check-item (RADIUS only) A-25
Examples where CLID is preferred A-26
Examples where DNIS is preferred A-27
Examples where CLID is required A-28
Examples where DNIS is required A-28
Callback after authentication A-30
Settings in a Connection profile A-30
Settings in RADIUS A-30
Examples of callback after CLID authentication A-31
Examples of callback after authentication A-31

Appendix B Authorization Options B-1

Introduction B-1
Authorizing immediate mode login service B-2
Using the Terminal-Server profile B-2
Using Connection profiles B-3

Using RADIUS profiles ... B-3
Authorizing menu mode access ... B-4
Terminal-Server profile settings ... B-4
Settings in a RADIUS initial-banner profile ... B-4
Examples of creating a menu of hosts ... B-5
Creating a customized menu of commands (RADIUS only) ... B-6
Extended example of RADIUS and menu mode ... B-7
Authorizing terminal-mode logins ... B-9
TCP, Rlogin, or Telnet connections in terminal mode ... B-9
Authorizing use of the commands ... B-9
Configuring the Rlogin source port range ... B-10
Setting defaults for Telnet sessions ... B-11
PPP and SLIP sessions in terminal mode ... B-12
Authorizing use of the commands ... B-12
Setting defaults for PPP sessions ... B-12
Setting defaults for SLIP sessions ... B-13
Allowing users to dial into the terminal-server interface ... B-14
Authorizing SNMP management access ... B-14
Setting community strings ... B-15
Setting up and enforcing address security ... B-15

Index ... Index-1

Figures

Figure 2-1 A RADIUS server on a LAN interface 2-6
Figure 2-2 Synchronous PPP connection 2-13
Figure 2-3 Asynchronous PPP connection 2-13
Figure 2-4 Multilink Protocol (MP) connection 2-15
Figure 2-5 Weighting line utilization samples 2-17
Figure 2-6 Multilink Protocol Plus (MP+) connection 2-20
Figure 2-7 TCP-Clear connection to a local host 2-24
Figure 2-8 A nailed (permanent) connection 2-28
Figure 2-9 Connection using both nailed and switched bandwidth 2-30
Figure 2-10 Dial-out PPP connection 2-37
Figure 3-1 Frame Relay network 3-2
Figure 3-2 Frame Relay concentrator 3-2
Figure 3-3 Frame Relay switch 3-3
Figure 3-4 Frame Relay DTE interface 3-10
Figure 3-5 Frame Relay DCE interface 3-11
Figure 3-6 Frame Relay NNI interface 3-13
Figure 3-7 Frame Relay PVC 3-15
Figure 3-8 Frame Relay gateway 3-19
Figure 3-9 Frame Relay Direct 3-22
Figure 3-10 Frame Relay circuit with UNI interfaces 3-25
Figure 3-11 Frame Relay circuit with NNI interfaces 3-27
Figure 3-12 Frame Relay circuit with UNI and NNI interface 3-29
Figure 3-13 ATM-Frame Relay circuit 3-35
Figure 4-1 Class C IP address 4-4
Figure 4-2 29-bit subnet mask and the number of supported hosts 4-5
Figure 4-3 Router-to-router IP connection 4-16
Figure 4-4 Dial-in host requiring a static IP address (a host route) 4-17
Figure 4-5 A numbered interface connection 4-18
Figure 4-6 IP Direct connections 4-19
Figure 4-7 Default route to a local IP router 4-26
Figure 4-8 Default route across a Frame Relay DLCI interface 4-27
Figure 4-9 Static route to a remote subnet 4-28
Figure 4-10 Dial-in host requiring assigned IP address 4-57
Figure 4-11 MAX TNT forwarding multicast traffic to LAN and WAN clients 4-58
Figure 4-12 MBONE router on a LAN interface 4-62
Figure 4-13 MBONE router on a WAN interface 4-62
Figure 4-14 LAN multicast client interface 4-65
Figure 4-15 WAN multicast client interfaces 4-65
Figure 4-16 Virtual IP routing 4-67
Figure 5-1 OSPF Autonomous System Boundary Routers (ASBRs) 5-4
Figure 5-2 OSPF Designated Router (DR) and Backup Designated Router (BDR) 5-5
Figure 5-3 OSPF costs for different types of links 5-6
Figure 5-4 Dividing an OSPF Autonomous System (AS) into areas 5-6

Figure 5-5 Sample OSPF topology 5-8
Figure 5-6 OSPF on a LAN interface 5-12
Figure 5-7 OSPF on a WAN interface 5-13
Figure 5-8 Including ASE routes in the OSPF environment 5-14
Figure 6-1 ATMP tunnel from an ISP to a corporate home network 6-1
Figure 6-2 System IP addresses and routes between ATMP agents 6-3
Figure 6-3 Path MTU on an Ethernet segment 6-4
Figure 6-4 Foreign Agent tunneling to two Home Agents 6-12
Figure 6-5 Foreign Agent tunneling to a GRF switch 6-15
Figure 6-6 How a Gateway Home Agent works 6-17
Figure 6-7 How a Router Home Agent works 6-18
Figure 6-8 Resilient ATMP installation 6-21
Figure 6-9 Gateway Home Agent with leased line to home network 6-21
Figure 6-10 Router Home Agent on the home network 6-23
Figure 6-11 MAX TNT acting as both Home Agent and Foreign Agent 6-26
Figure 6-12 Enabling a mobile client to bypass the Foreign Agent connection 6-28
Figure 6-13 IPX routing connections for IPX ATMP 6-30
Figure 6-14 IPX ATMP with a Gateway Home Agent 6-31
Figure 6-15 IPX ATMP with a Router Home Agent 6-33
Figure 7-1 L2TP tunneling 7-1
Figure 7-2 PPTP tunneling 7-6
Figure 7-3 IP-in-IP tunneling 7-12
Figure 8-1 IPX connection with NetWare servers on both sides 8-10
Figure 8-2 Dial-in NetWare client 8-12
Figure 9-1 ARA Client dial-in 9-6
Figure 9-2 AppleTalk connection using a PPP dialer 9-7
Figure 9-3 AppleTalk routing connection 9-7
Figure 9-4 ARA connection that encapsulates IP packets in DDP 9-9
Figure 10-1 Data filters drop or forward certain packets 10-2
Figure 10-2 Call filters prevent certain packets from resetting the timer 10-2
Figure A-1 Shared secret used between the MAX TNT and a RADIUS server A-5
Figure A-2 Token card authentication for dial-in connections A-15
Figure A-3 PAP-TOKEN with an ACE server A-17
Figure A-4 PAP-TOKEN-CHAP with a Safeword server A-18
Figure A-5 CACHE-TOKEN with a SafeWord server A-19
Figure A-6 SACE authentication for remote router users A-20
Figure B-1 Terminal-server access modes B-1
Figure B-2 Terminal-server menu mode B-6
Figure B-3 Customized login screen for RADIUS user B-7
Figure B-4 A customize login screen with match patterns B-7
Figure B-5 An extended terminal-server example B-8
Figure B-6 Menu displayed when DEFAULT profile is used B-8

Tables

Table 1-1	Documentation conventions	1-6
Table 4-1	IP address classes	4-4
Table 4-2	Standard subnet masks and Ascend notation	4-5
Table 5-1	Link state databases for OSPF topology in Figure 5-5	5-8
Table 5-2	Shortest-path tree and resulting routing table for Router-1	5-8
Table 5-3	Shortest-path tree and resulting routing table for Router-2	5-9
Table 5-4	Shortest-path tree and resulting routing table for Router-3	5-9
Table 6-1	Foreign Agent supporting duplicate IP addresses	6-6
Table 8-1	Ascend extensions to IPX	8-3
Table 9-1	Macintosh TCP/IP settings for PPP connections	9-8
Table 9-2	Macintosh TCP/IP settings for ARA connections	9-8

Introduction

1

What is in this guide 1-1

What's new in this guide 1-2

What you should know 1-3

Related publications 1-3

Documentation conventions 1-6

What is in this guide

This guide describes how to configure the MAX TNT for network connectivity. It assumes that you have already set up the MAX TNT system (standalone or multishelf), installed the slot cards, and provisioned and tested the lines. If you have not already finished those tasks, please see the *MAX TNT Hardware Installation Guide.*

Each chapter in the guide focuses on a particular aspect of network configuration. To get the full network connectivity you need, you might need information from only a few chapters, or from many chapters. For example, many dial-in connections require packet routing, either onto a local network or to a next-hop router. In that case, you have to configure both the routing parameters and the encapsulation protocol settings (such as PPP or Frame Relay) that enable the MAX TNT to negotiate a WAN link. So you have to refer to multiple chapters in this guide.

This guide includes information about hash-code protected features, which may be visible in the command-line interface but are not supported in the system unless the appropriate software option has been purchased from Ascend. To determine whether a feature is disabled in the system software, check the Base profile. For example:

```
admin> get base
[in BASE]
shelf-number = 1
software-version = 7
software-revision = 0
software-level = b
d-channel-enabled = yes
switched-enabled = yes
multi-rate-enabled = no
frame-relay-enabled = yes
data-call-enabled = yes
r2-signaling-enabled = no
serial-number = 1234567
modem-dialout-enabled = no
network-management-enabled = no
```

```
phs-support = no
routing-protocols-disabled = no
tnt-adsl-restricted = no
tnt-sdsl-restricted = no
tnt-idsl-restricted = no
ss7asg = disabled
atmp-enabled = enabled
l2tp-enabled = disabled
pptp-enabled = disabled
ipinip-enabled = disabled
```

For information about the settings of the Base profile, see the *MAX TNT Reference Guide*.

What's new in this guide

In this release, the *MAX TNT Network Configuration Guide* includes information about using RADIUS authentication as well as the command-line interface configurations shown in previous releases. In addition, the following new features are described in this release (see the Index for page references):

- MP bonding of analog calls
- Backup interfaces for nailed connections
- Multiple destination support for TCP-Clear
- LQM magic number support
- X.75 support
- Configurable dial-out timer
- Configurable Rlogin source port range
- Link management on DLCI 1023
- ATM-FR circuit support
- Ways to reload RADIUS nailed profiles
- RADIPAD support for centralized pool management
- Private static routes in RADIUS
- Management-only Ethernet interface
- Proxy-QoS and TOS support
- Per-session source address checking
- Routing Information Protocol (RIP) triggering
- Suppress host route advertisements
- Changes in setting an interface-independent IP address
- BOOTP-Relay Agent
- Virtual Routers
- MD5 authentication for OSPF (RFC 2178)
- ATMP resiliency in Primary and Secondary Home Agents
- IP-in-IP Encapsulation
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

- IPX over ATMP
- Answer-Defaults IPX Peer-Mode setting
- AppleTalk routing and remote access
- RADIUS Filter-ID support
- Type-of-Service filters

What you should know

While this guide attempts to provide enough conceptual framework to enable an administrator who is not an expert in a particular network technology to configure the 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

Related publications

Additional information is available in the other guides in the MAX TNT documentation set. If you need more background information than these guides provide, many external references are readily available on the Web or in technical bookstores. You'll find a partial list of such references below.

Related RFCs

RFCs are available on the Web.

Information about PPP connections

For information about PPP connections and authentication, you might want to download one or more of the following:

- RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 1990: *The PPP Multilink Protocol (MP)*
- RFC 1989: *PPP Link Quality Monitoring*
- RFC 1974: *PPP Stac LZS Compression Protocol*

- RFC 1962: *The PPP Compression Control Protocol (CCP)*
- RFC 1934: *Ascend's Multilink Protocol Plus (MP+)*
- RFC 1662: *PPP in HDLC-like Framing*
- RFC 1661: *The Point-to-Point Protocol (PPP)*
- RFC 1618: *PPP over ISDN*
- RFC 1332: *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*

Information about IP routing

RFCs that describe the operation of IP routers include:

- RFC 2030: *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*
- RFC 2002: *IP Mobility Support*
- RFC 1812: *Requirements for IP Version 4 Routers*
- RFC 1787: *Routing in a Multi-provider Internet*
- RFC 1582: *Extensions to RIP to Support Demand Circuits*
- RFC 1519: *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 1433: *Directed ARP*
- RFC 1393: *Traceroute Using an IP Option*
- RFC 1256: *ICMP Router Discovery Messages*

Information about OSPF routing

For information about OSPF routing, see:

- RFC 1850: *OSPF Version 2 Management Information Base*
- RFC 1587: *The OSPF NSSA Option*
- RFC 1586: *Guidelines for Running OSPF Over Frame Relay Networks*
- RFC 1583: *OSPF Version 2*
- RFC 1246: *Experience with the OSPF protocol*

Information about multicast

For information about multicast, see:

- RFC 1458: *Requirements for Multicast Protocols*
- RFC 1112: *Host Extensions for IP Multicasting*

Information about virtual private networks

For details about tunneling, see:

- RFC 1701: *Generic Routing Encapsulation (GRE)*
- RFC 2107: *Ascend Tunnel Management Protocol - ATMP*
- RFC 2003: *IP Encapsulation Within IP*

Information about IPX routing

RFCs that describe the operation of IPX routing across the WAN include:

- RFC 1634: *Novell IPX Over Various WAN Media (IPXWAN)*
- RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*
- RFC 1132: *A Standard for the Transmission of 802.2 Packets over IPX Networks*

Information about packet filtering

RFCs that describe firewalls and packet filters include:

- RFC 1858: *Security Considerations for IP Fragment Filtering*
- RFC 1579: *Firewall-Friendly FTP*
- RFC 1700: *Assigned Numbers*

Information about general network security

RFCs pertinent to network security include:

- RFC 1704: *On Internet Authentication*
- RFC 1636: *Report of IAB Workshop on Security in the Internet Architecture*
- RFC 1281: *Guidelines for the Secure Operation of the Internet*
- RFC 1244: *Site Security Handbook*

Information about external authentication

For information about RADIUS and TACACS authentication, see:

- RFC 2138: *Remote Authentication Dial In User Service (RADIUS)*
- RFC 1492: *An Access Control Protocol, Sometimes Called TACACS*

ITU-T recommendations

ITU-T (formerly CCITT) recommendations are available commercially. You can order them at http://www.itu.ch/publications/.

Related books

The following books are available in technical bookstores.

- *Interconnections*, by Radia Perlman. Addison-Wesley, 1992. Recommended for information about packet bridging.
- *Routing in the Internet*, by Christian Huitema. Prentice Hall PTR, 1995. Recommended for information about IP, OSPF, CIDR, IP multicast, and mobile IP.
- *Building Internet Firewalls*, by Brent Chapman and Elizabeth Zwicky. O'Reilly & Associates, Inc., 1995. Recommended for packet filtering information.
- *SNMP, SNMPV2 and RMON: Practical Network Management*, by William Stallings. Addison-Wesley, 1996. Recommended for network management information.

- *Enterprise Networking: Fractional T1 to Sonet Frame Relay to Bisdn*, by Daniel Minoli. Artech House, 1993. Recommended as a WAN reference.
- *TCP/IP Illustrated*, volumes 1&2, by W. Richard Stevens. Addison-Wesley, 1994.

Documentation conventions

Table 1-1 shows the conventions used in this guide.

Table 1-1. Documentation conventions

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface mono-space 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 bold type.
|	Separates command choices that are mutually exclusive.
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.

WAN Connections

2

Introduction to WAN connections 2-1
System-wide profiles 2-3
Local and external authentication profiles 2-7
Configuring switched dial-in connections 2-10
Configuring nailed and nailed/MP+ connections. 2-26
Configuring dial-out connections. 2-34

Introduction to WAN connections

WAN connections can be dialed into or dialed out of the MAX TNT. Dial-in connections are initiated by a remote user or access router, and dial-out is initiated by the MAX TNT itself (typically on the basis of packet routing) or by a user dialing out 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 an Ascend Pipeline uses a synchronous link, while an analog modem requires asynchronous.

A synchronous link uses HDLC encoding and connects to an access router for a network-to-network link. The call is initially routed as a digital call to an HDLC channel in the MAX TNT, 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 async call initiated by a modem is typically routed as a voice call to a digital modem in the MAX TNT, and then to the terminal-server software. Other kinds of async 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. Support in the MAX TNT includes 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

V.120 encapsulation is handled transparently and requires minimal configuration (for details, see "Answer-Defaults profile" on page 2-3).

AppleTalk routing and ARA connections are described in Chapter 9, "AppleTalk Routing and Remote Access."

Frame Relay, Frame Relay circuits, and ATM-to-Frame Relay circuits are described in Chapter 3, "Frame Relay." For a description of an ATM connection, see the ATM section of the *MAX TNT Hardware Installation Guide*.

Note: PPP calls use a single channel. MP calls use a static number of multiple channels, and can be used to communicate with any MP-compliant device. MP+ calls can add channels dynamically as needed, and can be used only between Ascend units. If you configure MP+ and the remote device does not support it, the MAX TNT attempts an MP connection. If the remote device does not support MP, the MAX TNT falls back to single-channel PPP.

How the system answers and authenticates dial-in calls

When the MAX TNT 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 MAX TNT 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 MAX TNT begins authentication. If it does not find a matching profile and the Answer-Defaults profile requires a profile for all callers (the default), the MAX TNT drops the call.

How the system initiates dial-out calls

When the MAX TNT 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 MAX TNT 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 2-34.

In addition, the MAX TNT can allow users to access its 56K modems to initiate dial-out sessions. This configuration is described in "Modem dial-out connections" on page 2-38.

How the system establishes and monitors sessions

After it authenticates a call, the MAX TNT builds and maintains a session with the caller. The call's data can be forwarded to the MAX TNT 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 MAX TNT uses settings in the caller's profile to monitor and, if appropriate, to 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 2-8.)

Spanning cards and shelves for multichannel calls

The MAX TNT can bundle channels for an MP or MP+ connection across multiple HDLC cards, which may reside in different shelves of a multishelf system. The behavior of the Call-Routing-Sort-Method parameter in the System profile has been modified to enable bundling channels across HDLC cards transparently. For details, see the *MAX TNT Reference Guide*.

System-wide profiles

In addition to a connection-specific profile, which specifies the name and password to be used in the authentication sequence as well as configuration settings, the Answer-Defaults, Terminal-Server, and External-Auth profiles also set parameters system-wide that affect WAN connections.

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 MAX TNT 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 MAX TNT uses the connection-specific value rather than the Answer-Defaults value to build the session.

The following command displays the contents of the Answer-Defaults profile:

```
admin> get answer
[in ANSWER-DEFAULTS]
use-answer-for-all-defaults = yes
force-56kbps = no
profiles-required = yes
clid-auth-mode = ignore
ppp-answer = { yes no-ppp-auth yes 0 none 1524 no 600 600 }
mp-answer = { yes 1 2 }
mpp-answer = { yes quadratic transmit 1 1 15 5 10 70 }
fr-answer = { yes }
tcp-clear-answer = { yes }
ara-answer = { no }
v120-answer = { yes 256 }
ip-answer = { yes yes no 1 }
```

```
ipx-answer = { no router-peer }
session-info = { "" "" no 120 no-idle 120 0 }
x75-answer = { yes 7 10 1000 1024 }
framed-only = no
```

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 value from the Answer-Defaults settings.

If Use-Answer-For-All-Defaults is set to No and a RADIUS profile does not return certain values, the MAX TNT uses factory default values for RADIUS attributes instead. For more details, see the *MAX TNT RADIUS Guide*.

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 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 MAX TNT accepts incoming PPP calls that support any of the authentication methods, but it drops connections that do not offer any authentication protocols during 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 the MAX TNT, 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 MAX TNT 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 MAX TNT 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 MAX TNT 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 async PPP call, the terminal server forwards the call to the router software as soon as it detects a PPP packet. For information about configuring async PPP calls, see "Examples of an asynchronous PPP connection" on page 2-13.

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 following authentication. For information about both of these issues, see Appendix A, "Authentication Methods."

You must enable the terminal-server software to allow the MAX TNT 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

The MAX TNT supports RADIUS as well as TACACS and TACACS+ for external authentication and accounting. In Figure 2-1, the MAX TNT answers incoming calls and forwards authentication requests to a RAIUD server on a LAN interface:

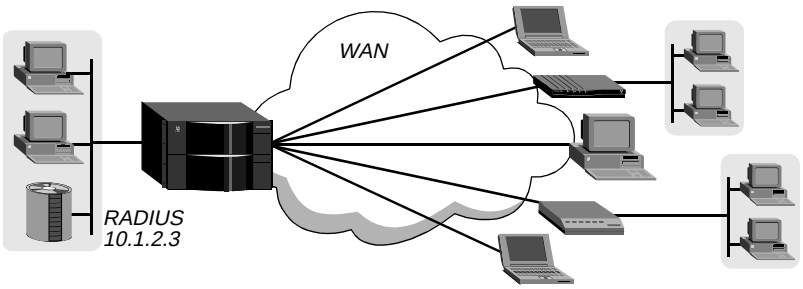


Figure 2-1. A RADIUS server on a LAN interface

The following commands configure the MAX TNT to access the RADIUS server at 10.1.2.3 on UDP port 5000, using the password `tntpw`:

```
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 = tntpw
admin> write
EXTERNAL-AUTH written
```

For details about installing the daemon and for more information about configuring the MAX TNT as a RADIUS client, see the *MAX TNT RADIUS Guide*.

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. The two commands in the following example create a new Connection profile and list its contents:

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

admin> list
[in CONNECTION/newyork]
station* = ""
active = no
encapsulation-protocol = mpp
called-number-type = national
dial-number = ""
clid = ""
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no no 0 0.0.0.0 ro+
ipx-options = { no router-peer both both no 00:00:00:00 00:00:00:00 ""+
bridging-options = { 0 no }
session-options = { "" "" no 120 no-idle 120 "" 0 }
telco-options = { ans-and-orig no off 1 no no 56k-clear 0 "" "" no no 0 }
ppp-options = { no-ppp-auth "" "" stac 1524 no 600 600 no }
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
fr-options = { "" 16 "" no "" 16 }
tcp-clear-options = { "" 0 no "" 256 20 }
ara-options = { "" 0 }
appletalk-options = { no "" 0 0 router-peer }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
framed-only = no
tunnel-options = { disabled 0 "" "" 5150 "" "" }
```

Using RADIUS

You can use RADIUS to externally authenticate connections answered by the MAX TNT. 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. For details about obtaining and installing the Ascend RADIUS daemon and dictionary, and for a sample users file, see the *MAX TNT RADIUS Guide*.

RADIUS profiles 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 may also be a phone number (for CLID or DNIS authentication), a special string

indicating a pseudo-user profile, or the string DEFAULT (for the default user profile). For details about pseudo-user profiles, see the *MAX TNT RADIUS Guide*.

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 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.

Specifying session time limits

Once the MAX TNT has answered a call and established a WAN session, it uses settings 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.

Settings in a Connection profile

Following are the relevant parameters in a Connection profile, shown with default settings:

```
[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 Data-Filter	Name of a filter or firewall to apply to the connection. For details, see Chapter 10, "Ascend Packet Filters."
Filter-Persistence	Enables/disables filter persistence across connection state changes.
Idle-Timer	Number of seconds a packetized network session can remain idle before it is terminated (120 by default).
TS-Idle-Mode	In which direction 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 (120 by default).
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.)

Settings in a RADIUS profile

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

Attribute	Value
Filter-ID (11)	Name of a local Filter profile that defines a data filter. The next time the MAX TNT accesses the RADIUS user profile in which this attribute appears, the referenced data filter is applied to the connection. For details, see Chapter 10, "Ascend Packet Filters."
Idle-Timeout (28)	Maximum number of consecutive seconds of idle time allowed to 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 Ascend now supports and recommends 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 Ascend now supports and recommends 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)	In which direction 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.)

Examples 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 maximum 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"
    User-Service =Login-User,
    Login-Service = Telnet,
    Login-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 see the *MAX TNT RADIUS Guide*.

Configuring switched dial-in connections

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

Note: For details about dial-ins that use Frame Relay, see Chapter 3, “Frame Relay.”

Single-channel PPP connections

A single-channel PPP dial-in can be initiated by an async device, such as an analog modem, or by a synchronous network device, such as an Ascend Pipeline. For connections requiring more then 56K bandwidth, see “Multilink Protocol (MP) connections” on page 2-14 or “Multilink Protocol Plus (MP+) connections” on page 2-17.

Settings in a Connection profile

Following are the PPP parameters, shown with their 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 2-11.
MRU	Maximum number of bytes the MAX TNT can receive in a single packet (from 1 to 1524, default 1524).
LQM	Enables/disables 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:

Attribute	Value
Password (2)	Password expected from the caller for a dial-in connection.
User-Service (6)	Type of services the link can use. Set to Framed-User (2) for dial-in PPP connections that do not use a terminal-server login, or Login-User (1) for async 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 MAX TNT 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” (below).

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 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. The MAX TNT supports the following types of PPP link compression:

- Stac compression uses an Ascend-modified version of draft 0 of the CCP Protocol, which predates RFC 1974. Older Ascend equipment supports this compression method. It 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, including recent Ascend 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

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 MAX TNT 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.

The MAX TNT inspects the magic-number field in received packets. If it is equal to zero or the peer's unique magic number, the packet is processed normally. If the magic-number field is equal to the local magic number, indicating a loopback link, the MAX TNT brings down the link.

Examples of a synchronous PPP connection

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

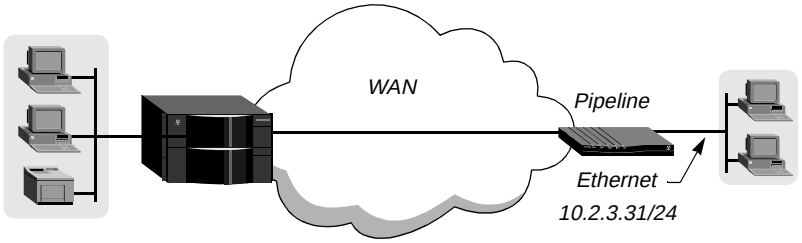


Figure 2-2. Synchronous PPP connection

The 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 are is a comparable RADIUS profile:

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

For details about enabling the MAX TNT to dial out to the Pipeline to route packets to that destination, see "Configuring dial-out connections" on page 2-34.

Examples 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 2-5. For information about terminal-server authentication, see Appendix A, "Authentication Methods."

In Figure 2-3, the calling device is a modem, so the call is asynchronous.

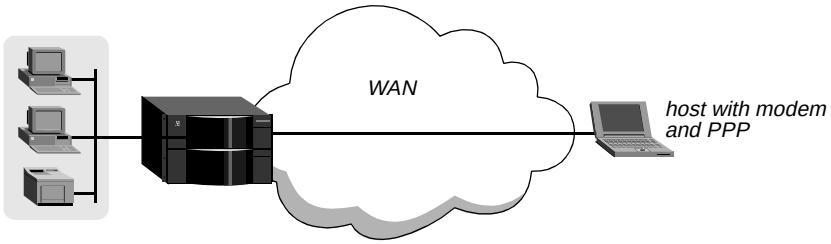


Figure 2-3. Asynchronous PPP connection

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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.2.3.78,
    Framed-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 MAX TNT cannot successfully negotiate the connection, it falls back to single-channel PPP (see "Configuring dial-out connections" on page 2-34).

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

Settings in a Connection profile

Following are the parameters related to MP connections, shown with default settings.

```
[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 MAX TNT 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 this release, MP does not make use this value. However, it's value can apply to MP+ connections.
Maximum-Channels	Maximum number of channels available to a multilink PPP connection. In this release, MP does not make use this value. However, it's value can apply to MP+ connections.

Settings in a RADIUS profile

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

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 MAX TNT 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 this release, MP does not make use this value. However, it's value can apply to MP+ connections.
Ascend-Maximum-Channels (235)	Maximum number of channels available to a multilink PPP connection. In this release, MP does not make use this value. However, it's value does apply to 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 2-4 is allocated two channels.

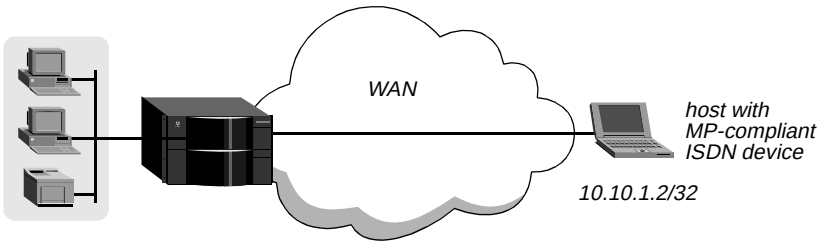


Figure 2-4. Multilink Protocol (MP) connection

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

MP bonding of analog calls

MP also operates on MAX TNT modem cards to bond multiple channels for analog calls. This enables a client with two modems to dial into the MAX TNT at a connect speed that is the aggregate speed of both connections.

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

For example, a Windows NT 4.0 system with two 56K modems, and Dial Up Networking (DUN) configured to use multiple lines, can set both modems to dial into the MAX TNT. The administrator specifies 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", User-Service = Framed-User
    Framed-Protocol = MP,
    Framed-Address = 10.10.1.2
    Framed-Netmask = 255.255.255.248,
    Ascend-Base-Channel-Count = 2
```

The first 56K modem call negotiates the MP connection, and the second modem call is bundled with the first. The MAX TNT reports a single MP user with a 128K connect speed.

Multilink Protocol Plus (MP+) connections

Multilink Protocol Plus (MP+) uses PPP encapsulation with Ascend extensions, as described in RFC 1934. MP+ enables the MAX TNT to monitor traffic on a connection with another Ascend unit, and add or subtract bandwidth on demand. The criteria for adding or dropping bandwidth are part of the Ascend extensions, and are supported only by Ascend 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 MAX TNT initiates the first call, all calls to add channels are also 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 2-14).

How Ascend units add bandwidth

Dynamic Bandwidth Allocation (DBA) enables the MAX TNT to add bandwidth on demand by establishing additional connections and inverse multiplexing them into the call. It 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. The three algorithms are represented in Figure 2-5:

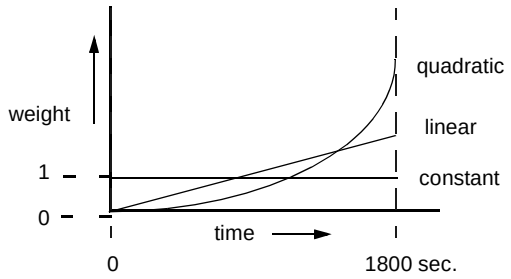


Figure 2-5. Weighting line utilization samples

For information about configuring per-channel add-on numbers that enable the MAX TNT to add bandwidth on demand, see the *MAX TNT Hardware Installation Guide*. You can add channels one at a time or, if the MAX TNT 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
```

The MAX TNT 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 restriction prevents both ends from continually trying to add new channels unsuccessfully. The MAX TNT and the Ascend unit at the other end 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 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 MAX TNT 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 MAX TNT 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 MP+, shown with default settings:

```
[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) indicates Multilink Protocol Plus. The far end must be an Ascend unit.
Aux-Send-Password	Password the MAX TNT sends when it adds channels to an MP+ call that uses PAP-Token-CHAP authentication. For details, see "Token card authentication" on page A-13
Dynamic-Algorithm	Algorithm for calculating average line utilization (ALU) over a certain number of seconds (Seconds-History). For details, see "How Ascend units add bandwidth" on page 2-17.

Parameter	Specifies
Bandwidth-Monitor-Direction	Criteria for adding or subtracting bandwidth from the connection. Bandwidth-Monitor-Direction specifies 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 MAX TNT 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 MAX TNT 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 MAX TNT 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 the connection's PPP options, in addition to the PPP attributes described in "Single-channel PPP connections" on page 2-10 and the MP parameters described in "Multilink Protocol (MP) connections" on page 2-14:

Attribute	Value
Framed-Protocol (7)	Encapsulation protocol. MPP (256) indicates an MP+ connection with another Ascend unit.
Ascend-History-Weigh-Type (239)	Algorithm for calculating average line utilization (ALU) over a certain number of seconds. For details, see "How Ascend units add bandwidth" on page 2-17.
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 MAX TNT 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 MAX TNT 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 MAX TNT adds bandwidth.

Attribute	Value
Ascend-Remove-Seconds (241)	Number of seconds for which the ALU must persist below the Target-Utilization threshold before the unit subtracts bandwidth.
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 this release, MP does not make use this value. However, it's value does apply to 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+ configuration

In Figure 2-6, both Ascend units specify MP+ encapsulation.

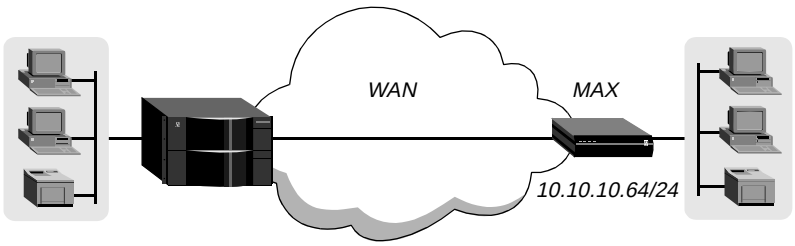


Figure 2-6. Multilink Protocol Plus (MP+) connection

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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.10.10.64,
    Framed-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.

TCP-Clear connections

The MAX TNT does 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 MAX TNT 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 TCP-Clear, shown with their default values:

```
[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. While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the MAX TNT 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	Enables/disables packet buffering of incoming data. If set to Yes, the MAX TNT begins buffering incoming data as soon as the dialup 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 MAX TNT matches 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. See
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 msecs has elapsed without matching the End-of-Packet-Pattern, 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 special 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

RADIUS profiles can specify up to four Login-Host and Login-TCP-Port attributes. The MAX TNT validates the number of these attributes in an Access-Accept packet returned by RADIUS. If it finds more than four, the MAX TNT logs an error in RADIF debug output and processes only the first four specifications.

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

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

Attribute	Value
Login-Service (15)	Type of login service allowed to the caller. Set to TCP-Clear (2).
Login-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.
User-Service (6)	Specifies whether the link can use framed or unframed services. Valid values are Login-User (1), Framed-User (2), and Dialout-Framed-User (5).

Examples of TCP-Clear connections

The following set of commands specifies a TCP-clear connection to a host named 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 = 10.10.10.1
admin> set tcp port = 23
admin> set tcp host1 = 10.10.10.2
admin> set tcp port1 = 125
admin> write
CONNECTION/tcpapp1 written
```

Following is a comparable RADIUS profile:

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

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

In Figure 2-7, a caller dialing into the MAX TNT is running an application that uses an encapsulation method that must be decoded by a local host. The MAX TNT sends the data stream from the incoming call directly to the host.

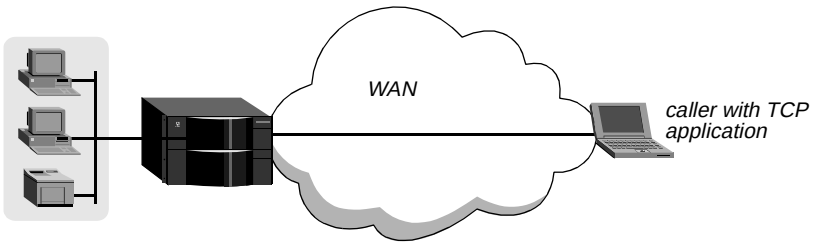


Figure 2-7. TCP-Clear connection to a local host

The following commands configure a TCP-Clear connection to a host named Sparky on TCP port 23, with the MAX TNT 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
```

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	Enables/disables X.75 system-wide 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 MAX TNT 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. The HDLC card (or the new HDLC-2 card) can support the maximum frame size of 1532 bytes.

Full technical specifications for X.75 can be found in the CCITT Blue Book Recommendation X series 1988. The following commands configure a Connection profile for X.75 when an HDLC-2 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 MAX TNT attempts to restore the link at ten-second intervals. If the MAX TNT 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 MAX TNT or the far-end device resets, the nailed connection must be re-established, which typically involves negotiations similar to a switched connection. The next sections describe only the parameters that are unique to nailed connections.

Settings in a Connection profile

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 2-31.
Answer-Originate	Enables/disables origination of the call to establish the nailed connection.
Call-Type	Type of nailed call. Set to FT1 for nailed.

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:

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 2-31.
Ascend-Call-Type (177)	Type of nailed call. Set to Nailed (1) for nailed connections.
Ascend-Group (178)	Group numbers of the dedicated channels for 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 this release, the administrator can specify how nailed connections are handled following a Refresh –n. Following is the relevant parameter, which is 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 following a Refresh, or reestablish only changed permanent connections. If set to All (the default), the system behaves as in previous releases: All existing permanent connections are brought down and then brought up again (along with any new connections) following the update. This causes service interruption every time any nailed profile is updated or added. If set to Changed, only new connections are created, and only those with modified attribute values are reestablished.

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

```
admin> read system
SYSTEM read
```

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

admin> write
SYSTEM written
```

Examples of a nailed connection

In Figure 2-8, the two MAX TNT units communicate via a leased T1 line with all of its channels assigned to group 11.

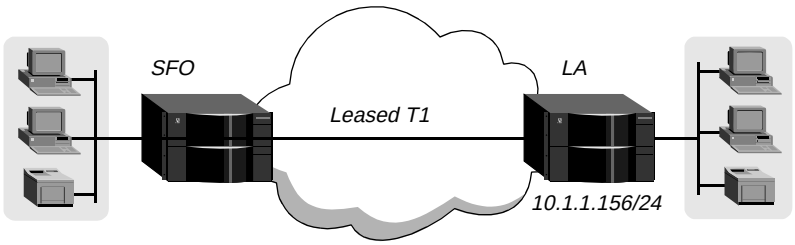


Figure 2-8. A nailed (permanent) connection

The following set of commands on the MAX TNT named SFO configures a local profile for the nailed connection to LA:

```
admin> new connection LA
CONNECTION/LA 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/LA written
```

Following is a comparable RADIUS profile:

```
permconn-SFO-1 Password = "ascend", User-Service =Dialout-Framed-User
    User-Name = "LA",
    Framed-Protocol = PPP,
    Framed-Address = 10.1.2.156,
    Framed-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 DBA algorithms. (For details about DBA, see “Multilink Protocol Plus (MP+) connections” on page 2-17.)

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 MAX TNT 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 2-17, 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	Enables/disables origination of the call to establish the nailed connection. Together, the Answer-Originate and FT1-Caller parameters specify that the MAX TNT is the designated caller for the switched part of the connection.
Call-Type	Type of nailed call. Set to FT1-MPP for nailed MP+.
Nailed-Groups	Group numbers of the dedicated channels for the nailed part of the connection.
FT1-Caller	Enables/disables 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 (described in “Multilink Protocol Plus (MP+) connections” on page 2-17), RADUS uses the following attribute-value pairs for nailed/MPP connections:

Attribute	Value
Ascend-Call-Type (177)	Type of nailed call. Set to Nailed/Mpp (2) for nailed MP+.

Attribute	Value
Ascend-Group (178)	Group numbers of the dedicated channels for the nailed part of the connection.
Ascend-FT1-Caller (175)	Enables/disables origination of the switched part of the connection. FT1-No (0) to wait for the remote end to initiate the call, FT1-Yes (1) for the MAX TNT to dial out to add channels. Only one end of the connection can be the FT1-caller.

Examples of a nailed MP+ connection

In Figure 2-9, the MAX TNT establishes a Nailed/MPP connection with a Pipeline 25 across the WAN.

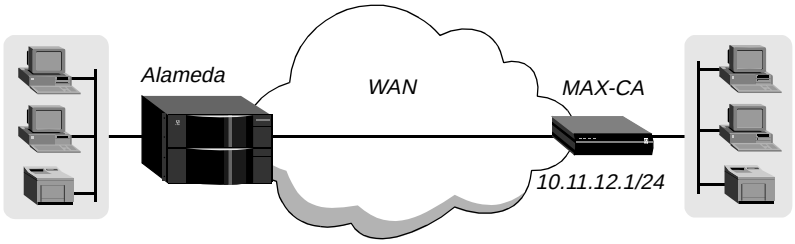


Figure 2-9. Connection using both nailed and switched bandwidth

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-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 and write the modified profile, the additional channels become available immediately.

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

```
permconn-Alameda-1 Password = "ascend", User-Service =Dialout-Framed-User
    User-Name = "MAX-CA",
    Framed-Protocol = MPP,
    Framed-Address = 10.11.12.1,
    Framed-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, alternate 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 system 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. It then diverts traffic from the primary to the backup interface. When the system 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 MAX TNT then brings it down.

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

Administrators 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

Following is the relevant parameter in a Connection profile, shown here with its default value:

```
[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 this format:

```
permconn-name-N Password="ascend", User-Service=Dialout-Framed-User
```

The *name* argument is the MAX TNT 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 MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

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

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

Examples of a switched backup interface

In the sample profiles that follow, the primary interface is a nailed MPP 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 uses different IP addresses for the primary and backup connections, both of which are nailed, see "Examples of backup interfaces for nailed Frame Relay links" on page 3-16)

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-tnt1-1 Password = "ascend", User-Service =Dialout-Framed-User
    User-Name = "nailed",
    Framed-Address = 10.168.7.9,
    Framed-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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.168.7.0/24 10.168.7.9 7 n p7"

p7 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "p7",
    Framed-Protocol = MPP,
    Ascend-Dial-Number = "55050",
    Framed-Address = 10.168.7.9
    Framed-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 MAX TNT brings up the nailed connection, the routing table includes entries such as this:

```
...
10.168.7.0/24    10.168.7.9    wan44      rGT    60   1      0       543
10.168.7.0/24    10.168.7.9    wan44      *SG   120   7      0       681
10.168.7.9/32    10.168.7.9    wan44      rT     60   1      0       543
10.168.7.9/32    10.168.7.9    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         10.168.7.9/32   11.168.6.234/32
044 1:17 000 +   p wan44     nailed    10.168.7.9/32    11.168.6.234/32
```

Notice that `nailed` is shown with plus-sign (+) to show 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         10.168.7.9/32    11.168.6.234/32
044 1:03 002 *   p wan44    nailed      10.168.7.9/32    11.168.6.234/32
```

Configuring dial-out connections

Typically, the MAX TNT initiates dial-out connections on the basis of packet routing. When it receives a packet to be forwarded across a WAN interfaces and the WAN connection is not up, it searches for a route, and dials the connection on the basis of the routing entry. For profiles that are located external to the 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 MAX TNT digital modems to dial out. For details about modem dialout, see “Modem dial-out connections” on page 2-38.

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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.2.3.31,
    Framed-Netmask = 255.255.255.0,
    Ascend-Link-Compression = Link-Comp-Stac

route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.2.3.0/24 10.2.3.31 1 n joel-out"

joel-out Password = "localpw", User-Service = Dialout-Framed-User
    User-Name = "joel",
    Framed-Protocol = PPP,
    Framed-Address = 10.2.3.31,
    Framed-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 user name and password. When the MAX TNT wants to dial out, it uses the name and a well-known password to retrieve the 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 specify User-Service set to Dialout-Framed-User. This attribute-value pair prevents anyone from using the profile for incoming authentication.

The User-Name attribute within the 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 MAX TNT uses a 20-second timer to establish a dialout call. If the remote side is not connected within that time, the dialout attempt fails. However, you can set the dialout 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 from the remote side when dialing out. Valid values are from 0 to 255. The default is 20 seconds. If set to zero, the MAX TNT uses its internal default of 20 seconds. In the following example, the dialout 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 dialout 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 may not require dial-out capability in a PPP, MP, or MP+ profile. The main reason to provide dial-out capability it to enable the MAX TNT 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.

Parameter	Specifies
Send-Auth-Mode	Authentication protocol to request when the MAX TNT initiates the connection. See “Password authentication” on page 2-11.
Send-Password	Password sent to the remote device when the MAX TNT initiates the connection.
Remote-Address	IP address of the remote device. The MAX TNT 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 2-34. A RADIUS user profile can specify the following attribute-value pairs for configuring a dialout PPP connection:

Attribute	Value
User-Service (6)	Type of service. Set to Dialout-Framed-User for dial-out profiles to avoid possible security issues.
User-Name (1)	Name of the remove 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 MAX TNT 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 MAX TNT 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 MAX TNT does not request the use of a particular protocol). This is the default: in a local profile the setting is No-PPP-Auth. In a RADIUS profile it is Send-Auth-None (0).
- Password Authentication Protocol (PAP). The MAX TNT 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 MAX TNT 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 2-10, the far-end device is a Pipeline unit with the IP address 10.2.3.31/29:

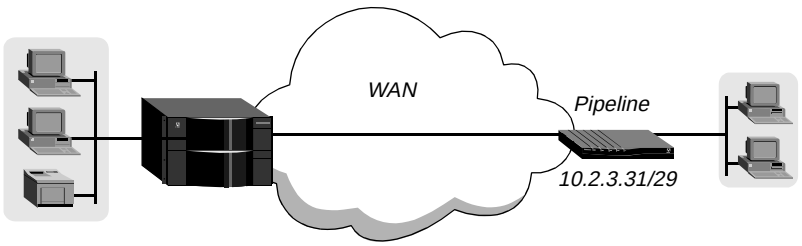


Figure 2-10. Dial-out PPP connection

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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.2.3.31,
    Framed-Netmask = 255.255.255.248
route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.2.3.0/29 10.2.3.31 1 n phani-out"
phani-out Password = "localpw", User-Service = Dialout-Framed-User
    User-Name = "phani",
    Ascend-Dial-Number = "1212",
```

```
Framed-Protocol = PPP,
Framed-Address = 10.2.3.31
Framed-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 using the MAX TNT 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 dialout 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 56K modems by setting the following parameters, which are 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	Enables/disables modem dial-out of any kind. If set to No, none of the other parameters in the Dialout-Configuration subprofile apply.
Direct-Access	Enables/disables the Direct-Access dial-out feature. If set to Yes, users can Telnet to a particular port on the MAX TNT to get immediate dial-out service. The port number configured as the Port-for-Direct-Access tells the MAX TNT that all Telnet sessions to that port want direct-access to a modem. If set to No, the remaining parameters in the Dialout-Configuration subprofile do not apply.
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.

Parameter	Specifies
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 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 set to User, a user must have a dial-out profile that specifically allows modem dialout. In that case, the PPP Recv-Password in the user's profile is required to access 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:

```
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 MAX TNT modem as follows:

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

   ```
   telnet tnt01 5028
   ```

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

   ```
   Password: pizza
   ```

3. Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a 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 dialout. In that case, the Send-Password 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 user name and matches the user's input to a Connection profile (or RADIUS profile). It then password-authenticates the dialout session using the profile's password.

Connection profile settings

Following are the relevant Connection profile parameters, shown with their default settings:

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

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

Parameter	Specifies
Recv-Password	The user's password. The system prompts for this password before allowing the user access to its modems.
Dialout-Allowed	If the user-name 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 relevant RADIUS profile attributes:

Attribute	Usage for a Direct-Access dial-out
Password (2)	The user's password. The system prompts for this password before allowing the user access to its modems.
Ascend-Dialout-Allowed (131)	If the user-name 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.

Examples of Direct-Access with user security

The following commands set up Direct-Access dial-out on TCP port 5000 with User security:

```
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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-Dialout-Allowed = Dialout-Allowed
```

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

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

   telnet tnt01 5000

2. Enter your user name 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.

Frame Relay

3

Introduction 3-1
Configuring nailed bandwidth for Frame Relay 3-3
Defining Frame Relay link operations 3-6
Configuring a DLCI logical interface 3-14
Concentrating incoming calls onto Frame Relay 3-18
Configuring the MAX TNT as a Frame Relay switch 3-24
Configuring an ATM-Frame Relay circuit 3-32

Introduction

In the Frame Relay network, every access point connects directly to a switch. Frame Relay virtual circuits (VCs) are bidirectional data paths between two endpoints. An established permanent virtual circuit (PVC) is a connection between two endpoints, which can include a number of hops in between.

Depending on how a device such as the MAX TNT is integrated into a Frame Relay network, it can operate as a Frame Relay terminating unit (Customer Premise Equipment or CPE) or as a Frame Relay switch.

A CPE is the source or destination of data traversing the Frame Relay service. For example, the MAX TNT labeled TNT-02 in Figure 3-1 terminates the data stream to its PPP callers. When it is configured with a User-to-Network (UNI) interface to Frame Relay, the MAX TNT acts as the user side (UNI-DTE) communicating with the network side (UNI-DCE) of a switch.

The network-side device connects the CPE device to a Frame Relay network. For example, the MAX TNT labeled TNT-01 in Figure 3-1 receives Frame Relay encapsulated frames from a CPE and forwards them on to another Frame Relay switch. When it is configured with a UNI-DCE interface to Frame Relay, the MAX TNT acts as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device.

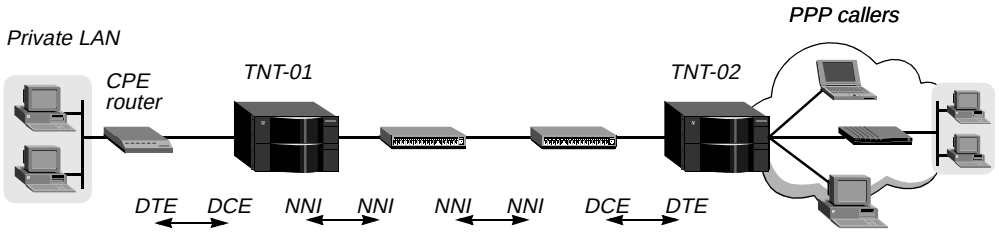


Figure 3-1. Frame Relay network

A Frame Relay switch is another kind of network-side device, which switches frames from one interface to another and exchanges status information with its peer switch. For example, the MAX TNT labeled TNT-01 in Figure 3-1 receives frames from its peer switch and switches them to its other Frame Relay interface. When it is configured with a Network-to-Network (NNI) interface to Frame Relay, the MAX TNT acts as a Frame Relay switch. Switch-to-switch communication includes both user side (NNI-DTE) and network side (NNI-DCE) functions.

Frame Relay link management

Frame Relay link management enables administrators to retrieve information about the status of the Frame Relay interface via special management frames with a unique Data Link Connection Identifier (DLCI) address. (DLCI 0 is the default for link management frames.) Link management frames are used to monitor the interface and provide information about DLCI status.

On a UNI interface to Frame Relay, link management procedures occur in one direction. The UNI-DTE device requests information and the UNI-DCE device provides it.

On an NNI interface, link management procedures are bidirectional. Switches perform both the NNI-DTE and NNI-DCE link management functions, since both sides of the connection request information from their peer switches.

Using the MAX TNT as a Frame Relay concentrator

As a Frame Relay concentrator, the MAX TNT forwards many lower-speed PPP connections onto one or more high-speed Frame Relay interfaces, as shown in Figure 3-2:

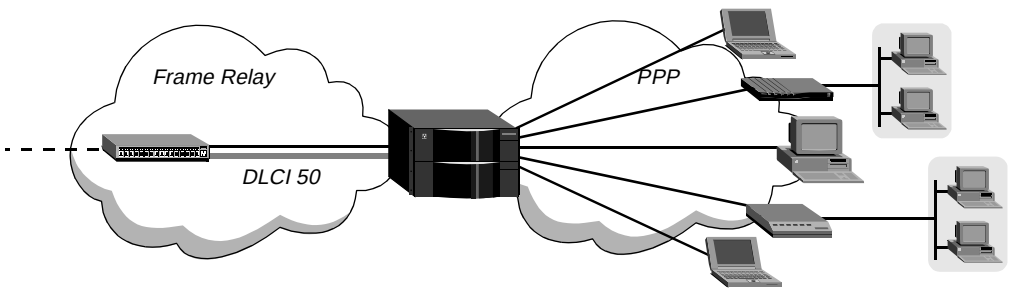


Figure 3-2. Frame Relay concentrator

In this kind of configuration, the decision to forward frames onto the Frame Relay interface can be made through OSI layer 3 (routing), or by Frame Relay Direct.

Using the MAX TNT as a Frame Relay switch

As a Frame Relay switch, the MAX TNT receives frames on one interface and transmits them on another interface. The decision to forward frames onto the Frame Relay interface is made through the assignment of circuit names. The MAX TNT router software is not involved.

To use the MAX TNT as a switch, you must configure a circuit that pairs two Frame Relay DLCI interfaces. Instead of going to the layer 3 router for a decision on which interface to forward the frames, it relies on the circuit configuration to relay the frames received on one interface to its paired interface. A circuit is defined in two Connection or RADIUS user profiles.

Figure 3-3 shows the MAX TNT operating as a Frame Relay switch:

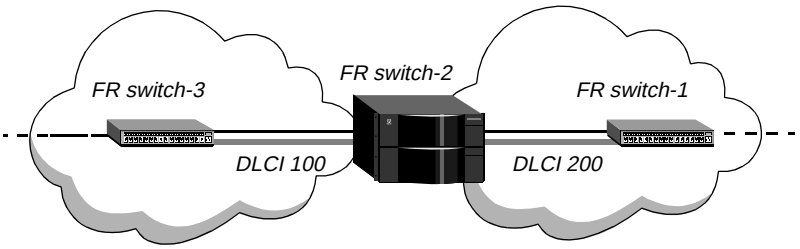


Figure 3-3. Frame Relay switch

Components of a Frame Relay configuration

The physical link to another Frame Relay device must be nailed (similar to a dedicated leased line). The administrator allocates nailed bandwidth in a line profile (the profile of a T1, E1, SWAN, or other network line).

The link interface to the Frame Relay device, which is also called a datalink, references specific nailed bandwidth in the MAX TNT and defines the operations and link management functions the MAX TNT performs on the interface. The administrator specifies these settings in a Frame-Relay profile or RADIUS frdlink pseudo-user profile.

The logical interface is a PVC endpoint, which requires a DLCI. DLCIs uniquely identify the logical endpoints of a virtual circuit (a specific end device). Administrators obtain DLCIs from Frame Relay providers and assign them in Connection profiles or RADIUS user profiles.

Configuring nailed bandwidth for Frame Relay

Each Frame Relay interface in the MAX TNT requires its own nailed bandwidth, which is similar to a dedicated leased line.

Note: If you configure the bandwidth on nailed T1, make sure that the number of channels the MAX TNT uses for the link matches the number of channels used by the device at the other end of the link, and that only one line profile specifies the Nailed-Group number to be used by the Frame Relay datalink.

Following are some examples of relevant parameters, shown with sample settings:

```
[in T1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]]
channel-usage = nailed-64-channel
nailed-group = 1

[in E1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]]
channel-usage = nailed-64-channel
nailed-group = 1

[in SWAN/{ any-shelf any-slot 0 }:line-config]
nailed-group = 1
```

Parameter	Specifies
Channel-Usage	Switched or Nailed channel usage. To configure nailed bandwidth on a channelized T1 or E1 card, set to Nailed-64-Channel (a clear-channel 64K circuit). On unchannelized cards, this parameter does not apply.
Nailed-Group	A number from 1 to 1024, used to identify nailed bandwidth. Frame-Relay profiles or RADIUS frdlink pseudo-user profiles specify this number to use the associated bandwidth.

Following is an example that shows how to configure the 24 channels of a T1 line for nailed usage. The example assigns the Nailed-Group number 11:

admin> **read t1 { 1 13 6 }**
T1/{ shelf-1 slot-13 6 } read

```
admin> set line channel 1 channel-usage = nailed-64-channel
admin> set line channel 1 nailed-group = 11
admin> set line channel 2 channel-usage = nailed-64-channel
admin> set line channel 2 nailed-group = 11
admin> set line channel 3 channel-usage = nailed-64-channel
admin> set line channel 3 nailed-group = 11
admin> set line channel 4 channel-usage = nailed-64-channel
admin> set line channel 4 nailed-group = 11
admin> set line channel 5 channel-usage = nailed-64-channel
admin> set line channel 5 nailed-group = 11
admin> set line channel 6 channel-usage = nailed-64-channel
admin> set line channel 6 nailed-group = 11
admin> set line channel 7 channel-usage = nailed-64-channel
admin> set line channel 7 nailed-group = 11
admin> set line channel 8 channel-usage = nailed-64-channel
admin> set line channel 8 nailed-group = 11
admin> set line channel 9 channel-usage = nailed-64-channel
admin> set line channel 9 nailed-group = 11
admin> set line channel 10 channel-usage = nailed-64-channel
```

```
admin> set line channel 10 nailed-group = 11
admin> set line channel 11 channel-usage = nailed-64-channel
admin> set line channel 11 nailed-group = 11
admin> set line channel 12 channel-usage = nailed-64-channel
admin> set line channel 12 nailed-group = 11
admin> set line channel 13 channel-usage = nailed-64-channel
admin> set line channel 13 nailed-group = 11
admin> set line channel 14 channel-usage = nailed-64-channel
admin> set line channel 14 nailed-group = 11
admin> set line channel 15 channel-usage = nailed-64-channel
admin> set line channel 15 nailed-group = 11
admin> set line channel 16 channel-usage = nailed-64-channel
admin> set line channel 16 nailed-group = 11
admin> set line channel 17 channel-usage = nailed-64-channel
admin> set line channel 17 nailed-group = 11
admin> set line channel 18 channel-usage = nailed-64-channel
admin> set line channel 18 nailed-group = 11
admin> set line channel 19 channel-usage = nailed-64-channel
admin> set line channel 19 nailed-group = 11
admin> set line channel 20 channel-usage = nailed-64-channel
admin> set line channel 20 nailed-group = 11
admin> set line channel 21 channel-usage = nailed-64-channel
admin> set line channel 21 nailed-group = 11
admin> set line channel 22 channel-usage = nailed-64-channel
admin> set line channel 22 nailed-group = 11
admin> set line channel 23 channel-usage = nailed-64-channel
admin> set line channel 23 nailed-group = 11
admin> set line channel 24 channel-usage = nailed-64-channel
admin> set line channel 24 nailed-group = 11
admin> write
T1/{ shelf-1 slot-13 6 } written
```

For details about configuring nailed bandwidth on other types of slot cards, and for more details about configuring T1, see the *MAX TNT Hardware Installation Guide*.

Note: If several Series56 II cards are installed before an HDLC card (if they are installed in lower-numbered slots), and the system has a Frame Relay datalink that uses a single nailed channel, the system attempts to allocate the call to each available channel of the Series56 II cards before it reaches the HDLC card. Series56 II cards do not support Frame Relay. The result is up to 48 call rejects for each Series56 II card before a successful call is established on the HDLC card. No system messages are reported during the interval.

Defining Frame Relay link operations

A Frame-Relay profile defines datalink operations, including link management functions. The same settings can be specified in a RADIUS frdlink pseudo-user profile.

Overview of datalink options

In this release, all Frame Relay link interfaces require nailed bandwidth.

Note: Link management settings are optional. It is possible to set up a Frame Relay interface and pass data across it without setting these parameters. However, they do provide a mechanism for retrieving information about the status of the interface and its DLCIs.

Settings in a Frame-Relay profile

Following are the relevant Frame-Relay parameters, shown with their default settings:

```
[in FRAME-RELAY/"" ]
fr-name* = ""
active = no
nailed-up-group = 1
nailed-mode = ft1
called-number-type = 0
switched-call-type = 56k-restricted
phone-number = ""
billing-number = ""
transit-number = ""
link-mgmt = none
call-by-call-id = 0
link-type = dte
n391-val = 6
n392-val = 3
n393-val = 4
t391-val = 10
t392-val = 15
MRU = 1532
dceN392-val = 3
dceN393-val = 4
link-mgmt-dlci = dlci0
```

Parameter	Specifies
FR-Name	Frame-Relay profile name, which must be unique, lowercase, and no longer than 15 characters.
Active	Availability of this profile for use. The default is No.
Nailed-Up-Group	Group number assigned to nailed channels in a line profile, such as a T1 or E1 profile. The default is 1. If the channels are on nailed T1, make sure that the number of channels the MAX TNT uses for the link matches the number of channels used by the device at the other end of the link, and that only one T1 profile specifies the Nailed-Group number to be used by the Frame Relay datalink.

Parameter	Specifies
Nailed-Mode	Type of nailed connection. FT1 (the default) indicates all nailed channels. The FT1-MPP or FT1-BO settings do not apply in this release.
Called-Number-Type	Type of number in the Phone-Number field. Does not apply when the call type is nailed.
Switched-Call-Type	Type of bearer channel capability. If a T1 line is set for ESF/B8ZS signaling, the remote switch or router typically requires that you set this parameter to 64k-clear. A setting of 56k-clear (the default) is required if the line is set to D4/AMI. E1 lines typically use 64k-clear.
Phone-Number	Phone number to dial. Does not apply when the call type is nailed.
Billing-Number	Number to use for billing purposes. Does not apply when the call type is nailed.
Transit-Number	String for use in the transit network. Does not apply when the call type is nailed.
Call-by-Call-ID	ID for call-by-call PRI signaling.Does not apply when the call type is nailed.
Link-Mgmt	Link management protocol. Settings are None (the default, which disables link management), ANSI-T1.617 (Annex D), and CCITT-Q.933a (CCITT Q.933 Annex A). To ensure interoperability with equipment from different vendors, the same version of management protocol must be used at each end of the Frame Relay link.
Link-Type	Type of operations performed by the MAX TNT on the link interface. Settings are DTE (the default), DCE, and NNI. (For more information, see “Examples of a UNI-DTE link interface” on page 3-10, “Examples of a UNI-DCE link interface” on page 3-11, and “Examples of an NNI link interface” on page 3-12.)
N391-Val	Number of T391 polling cycles between full Status Enquiry messages. The default is 6, which indicates that after 6 status requests spaced T391-Val seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Link-Type is DCE.
N392-Val	Number of errors which, if occurring in the number of DTE monitored events specified by N393-Val, causes the user-side to declare the network-side procedures inactive. The value should be less than that of N393-Val (which can be from 1 to 10). The default value is 3. Does not apply when Link-Type is DCE.
N393-Val	DTE monitored event count (from 1 to 10). The default is 4. Does not apply when Link-Type is DCE.
T391-Val	Link Integrity Verification polling timer. The value should be less than that of T392-Val. The default is 10, which indicates that after N391-Val status requests spaced 10 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Link-Type is DCE.

Parameter	Specifies
T392-Val	Interval (in seconds) at which Status Enquiry messages should be received (default 15). If the network does not receive a status inquiry message within the specified number of seconds, the network receives an error. Does not apply when Link-Type is DTE.
MRU	Maximum number of bytes the MAX TNT can receive in a single packet across the link interface. Usually the default of 1532 is the right setting. However, the far-end device might require a lower number.
DCEN392-Val	Number of errors which, if occurring in the number of DCE monitored events (DCEN393-Val), causes the network-side to declare the user-side procedures inactive. The value should be less than that of DCEN393-Val (which can be set from 1 to 10). The default value is 3. Does not apply when Link-Type is DTE.
DCEN393-Val	DCE monitored event count (from 1 to 10). The default is 4. Does not apply when Link-Type is DTE.
Link-Mgmt-DLCI	DLCI to use for LMI link management on the Frame Relay datalink. Valid values are DLCI0 (the default) and DLCI1023.

Settings in a RADIUS frdlink profile

An frdlink profile is a pseudo-user profile in which the first line has this format:

```
frdlink-name-N Password="ascend", User-Service = Dialout-Framed-User
```

The *name* argument is the MAX TNT system name (specified by the Name parameter in the System profile). It cannot include embedded spaces. *N* is a number in a sequential series, starting with 1, that applies to this type of pseudo-user profile (frdlink-*name*-1, frdlink-*name*-2, and so forth). Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

The following attribute-value pairs can be used to define a frdlink pseudo-user profile:

Attribute	Value
Ascend-FR-Profile-Name (180)	A Frame-Relay profile name (up to 15 characters), to be referenced in profiles that use this datalink. If the name is referenced by local Connection profiles, it must be lowercase. The name cannot duplicate the name of a local Frame-Relay profile.
Ascend-FR-Nailed-Grp (158)	Group number assigned to nailed channels in a line profile, such as a T1 or E1 profile. The default is 1. If the channels are on nailed T1, make sure that the number of channels the MAX TNT uses for the link matches the number of channels used by the device at the other end of the link, and that only one T1 profile specifies the Nailed-Group number to be used by the Frame Relay datalink.
Ascend-Call-Type (177)	Type of nailed connection: Nailed (1), Nailed/Mpp (2), or Perm/Switched (3). Nailed is the default.

Attribute	Value
Ascend-Data-Svc (247)	Type of data service on the nailed link.Typically set to Nailed-64K for a Frame Relay datalink.
Ascend-FR-Link-Mgt (160)	The link management protocol. Settings are Ascend-FR-No-Link-Mgt (0) (link management protocol is disabled), Ascend-FR-T1-617D (1) (Annex D), and Ascend-FR-Q-933A (2)(CCITT Q.933 Annex A). Ascend-FR-No-Link-Mgt is the default. To ensure interoperability with equipment from different vendors, the same version of management protocol must be used at each end of the Frame Relay link.
Ascend-FR-Type (159)	Type of operations performed by the MAX TNT on this interface. Settings are Ascend-FR-DTE (0), Ascend-FR-DCE (1), or Ascend-FR-NNI (2). Ascend-FR-DTE is the default. (For more information, see “Examples of a UNI-DTE link interface” on page 3-10, “Examples of a UNI-DCE link interface” on page 3-11, and “Examples of an NNI link interface” on page 3-12.)
Ascend-FR-N391 (161)	Number of T391 polling cycles between full Status Enquiry messages. The default is 6, which indicates that after 6 status requests spaced Ascend-FR-T391 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N392 (163)	Number of errors which, if occurring in the number of DTE monitored events specified by Ascend-FR-DTE-N393, causes the user-side to declare the network-side procedures inactive. The value should be less than that of Ascend-FR-DTE-N393l (which can be from 1 to 10). The default value is 3. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N393 (165)	DTE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-T391 (166)	Link Integrity Verification polling timer. The value should be less than that of Ascend-FR-T392. The default is 10, which indicates that after Ascend-FR-N391 status requests spaced 10 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-T392 (167)	Interval in which Status Enquiry messages should be received (from 5 to 30 seconds). The default T392 value is 15. An error is recorded if no Status Enquiry is received within the specified number seconds. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Framed-MTU (12)	Maximum number of bytes the MAX TNT can transmit in a single packet across the link interface. Usually the default of 1532 is the right setting. However, the far-end device might require a lower number.

Attribute	Value
Ascend-FR-DCE-N392 (162)	Number of errors which, if occurring in the number of DCE monitored events specified by Ascend-FR-DCE-N393, causes the network-side to declare the user-side procedures inactive. The value should be less than that of Ascend-FR-DCE-N393 (which can be from 1 to 10). Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Ascend-FR-DCE-N393 (164)	DCE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Ascend-FR-Link-Status-Dlci (106)	DLCI to use for LMI link management on the Frame Relay datalink. Valid values are DLCI0 (the default) and DLCI1023.

Examples of a UNI-DTE link interface

On a UNI-DTE interface, the MAX TNT acts as the user side communicating with the network side DCE switch. It initiates link management functions by sending a Status Enquiry to the UNI-DCE device. Status Enquiries may include queries about the status of PVC segments the DTE knows about, as well as the integrity of the datalink between the UNI-DTE and UNI-DCE interfaces.

The UNI-DTE uses the values of N391-Val, N392-Val, N393-Val, and T391-Val in the Frame-Relay profile to define the timing of its Status Enquiries to the DCE and its link integrity parameters. (These correspond to the Ascend-FR-N391, Ascend-FR-DTE-N392, Ascend-FR-DTE-N393, and Ascend-FR-T391 attributes in a RADIUS profile.)

Figure 3-4 shows a MAX TNT with a UNI-DTE interface.

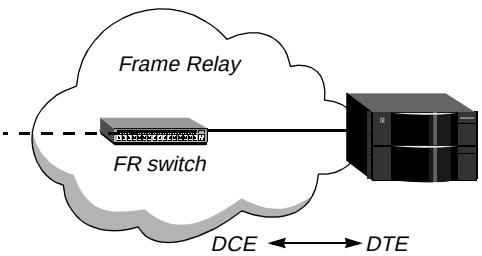


Figure 3-4. Frame Relay DTE interface

The following commands specify Nailed-Group 11 as the bandwidth for the sample DTE interface. *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
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
```

With these link management settings, the MAX TNT uses the CCITT Q.933 Annex A link management protocol to communicate with the Frame Relay DCE. It initiates link management functions by sending a Status Enquiry to the DCE every 10 seconds.

On a UNI-DTE interface, the state of a DLCI is determined by the Full status report from the DCE or by an async PVC update. The Full status report from the DCE specifies active and inactive and new DLCIs. If the DCE does not specify a DLCI as active or inactive, the DTE considers it inactive.

Following is a comparable RADIUS profile:

```
frdlink-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dte",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DTE,
    Ascend-FR-Nailed-Grp = 11,
    Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
    Ascend-Data-Svc = Nailed-64K
```

Examples of a UNI-DCE link interface

On a UNI-DCE interface, the MAX TNT acts as the network side communicating with the user side (UNI-DTE) of a Frame Relay terminating unit.

The UNI-DCE uses the values of T392-Val, DCEN392-Val, and DCEN393-Val in the Frame-Relay profile to define the parameters of the Status Enquiries it expects from the DTE. (These correspond to the Ascend-FR-T392, Ascend-FR-DCE-N392, and Ascend-FR-DCE-N393 attributes in a RADIUS profile.)

For example, it expects a Status Enquiry from the DTE every T392 seconds. If it does not receive a Status Enquiry at the configured interval, it records an error.

Figure 3-5 shows a MAX TNT with a UNI-DCE interface.

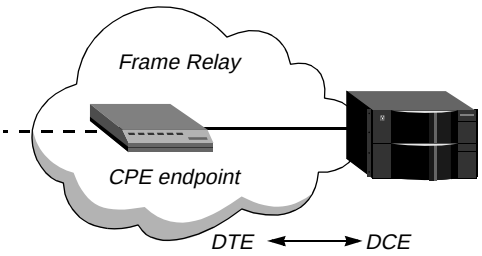


Figure 3-5. Frame Relay DCE interface

The following commands specify Nailed-Group 36 as the bandwidth for the sample DCE interface. *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
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> set t392 = 15
admin> write
FRAME-RELAY/fr-dce written
```

With these link management settings, the MAX TNT uses the CCITT Q.933 Annex A link management protocol to communicate with the CPE endpoint. It expects a Status Enquiry at intervals less than 15 seconds.

On a UNI-DCE interface, if the datalink is up, the DLCI is considered to be up as well. In the DCE Full status response to the DTE, if a PVC segment terminates within the DCE, it is reported as active. If the PVC segment is not terminated, the DCE has to request further information on the Frame Relay network. In that case, it requests information about the DLCI from the next hop switch, and reports back to the DTE when the segment is confirmed to be active or inactive.

Following is a comparable RADIUS profile:

```
frdlink-tnt-2 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dce",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 36,
    Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-T392 = 15
```

Examples of an NNI link interface

An NNI interface implements procedures used by Frame Relay switches to communicate status between them. The MAX TNT uses these procedures to inform its peer switch about the status of PVC segments from its side of the Frame Relay network, as well as the integrity of the datalink between them. The procedure is bidirectional. The switches act as both the user side (DTE) and network side(DCE) in that they both send Status Enquiries and respond to them.

Because NNI is bidirectional, all of the link management values defined in the Frame-Relay profile are used. The values of N391-Val, N392-Val, N393-Val, and T391-Val are used to define the user side of the NNI. These values define the timing of the status enquiries the MAX TNT sends to its peer switch and the boundary conditions that define link integrity. The values of T392-Val, DCEN392-Val, and DCEN393-Val are used by the network side of the NNI to define the parameters of the Status Enquiries it expects from the its peer switch.

Figure 3-6 shows a MAX TNT with an NNI interface:

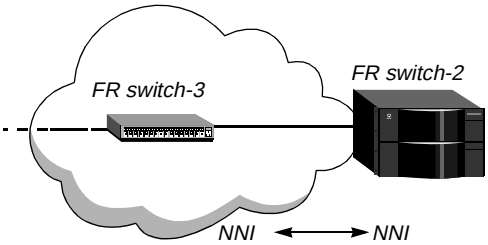


Figure 3-6. Frame Relay NNI interface

To operate as a switch, the MAX TNT requires a hard-coded circuit configuration in two Connection profiles. It relies on the circuit configuration to relay the frames received on one of the circuit endpoints to the other circuit endpoint. For details about circuit configuration, see "Configuring the MAX TNT as a Frame Relay switch" on page 3-24.

Note: The two Frame Relay endpoints that make up the circuit do not require NNI interfaces.

The following commands specify channels in group 52 for the NNI interface to Switch-3 (Figure 3-6). *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
admin> new frame-relay switch-3
FRAME-RELAY/switch-3 read
admin> set active = yes
admin> set link-type = nni
admin> set nailed-up-group = 52
admin> set link-mgmt = ansi-t1.617d
admin> set n391 = 6
admin> set t391 = 10
admin> set t392 = 15
admin> write
FRAME-RELAY/switch-3 written
```

With these link management settings, the MAX TNT uses the ANSI Annex D link management protocol to communicate with Switch-3. It sends a Status Enquiry for Link Integrity Verification to Switch-3 every 10 seconds, and requests a Full status report every sixth enquiry (every 60 seconds). It also sends a Full Status report in response to requests from the other switch. If it does not receive a Status Enquiry within a 15-second interval (T392), it records an error. Following is a comparable RADIUS profile:

```
frdlink-tnt-3 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "switch-3",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 52,
    Ascend-FR-Link-Mgt = Ascend-FR-T1-617D,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-N391 = 6,
    Ascend-FR-T391 = 10,
    Ascend-FR-T392 = 15
```

Configuring a DLCI logical interface

A Connection profile defines a DLCI interface. The same settings can be specified in a RADIUS permconn pseudo-user profile.

Overview of DLCI interface settings

Administrators configure a Connection or RADIUS permconn profile that specifies a connection to a far-end device across Frame Relay. The first hop of the connection is known by the DLCI assigned in the profile.

A DLCI is an integer between 16 and 991 that uniquely identifies a specific endpoint in the Frame Relay network. The Frame Relay administrator must provide a valid DLCI for each logical interface to a Frame Relay network.

Settings in a Connection profile

Following are the relevant Connection parameters, shown here with sample settings:

```
[in CONNECTION/""]
encapsulation-protocol = frame-relay

[in CONNECTION/"":fr-options]
frame-relay-profile = fr-dce
dlci = 55

[in CONNECTION/"":telco-options]
call-type = ft1

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

Parameter	Specifies
Encapsulation-Protocol	The encapsulation protocol. Must be set to Frame-Relay.
Frame-Relay-Profile	Name of the Frame-Relay profile that defines the datalink.
DLCI	A DLCI for this PVC endpoint.The DLCI must be obtained from a Frame Relay provider. The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Call-Type	Type of nailed call. Set to FT1 for nailed.
Backup	Name of a backup Connection profile to the next hop (optional). See “Examples of backup interfaces for nailed Frame Relay links” on page 3-16.

Settings in a RADIUS profile

A permconn profile is a pseudo-user profile in which the first line has this format:

`permconn-`*`name`*`-`*`N`* `Password="ascend", User-Service = Dialout-Framed-User`

The *name* argument is the MAX TNT system name (specified by the Name parameter in the System profile). It cannot include embedded spaces. *N* is a number in a sequential series,

starting with 1, that applies to this type of pseudo-user profile (permconn-*name*-1, permconn-*name*-2, and so forth). Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

The following attribute-value pairs can be used to define a permconn pseudo-user profile that uses Frame Relay:

Attribute	Value
User-Name (1)	Name of the far-end Frame Relay device.
Framed-Protocol (7)	The encapsulation protocol. Must be set to FR (261).
Ascend-FR-Profile-Name (180)	Name of the Frame-Relay profile that defines the data link.
Ascend-FR-DLCI (179)	A DLCI for this PVC endpoint.The DLCI must be obtained from a Frame Relay provider. The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Framed-Address (8)	Destination IP address, which lies at the end of a PVC whose first hop is known by the specified DLCI.
Framed-Netmask (9)	A subnet mask for Framed-Address.
Ascend-Backup (176)	Name of a backup Connection profile to the next hop (optional). See “Examples of backup interfaces for nailed Frame Relay links” on page 3-16.

Examples of a DLCI interface configuration

In Figure 3-8, the MAX TNT has a connection to a Frame Relay switch that also supports IP routing:

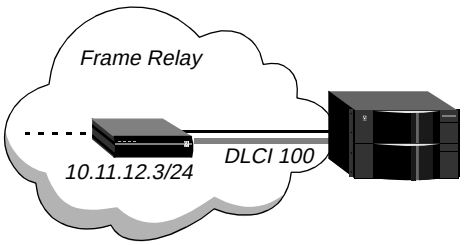


Figure 3-7. Frame Relay PVC

The following set of commands configures the Connection profile, assigning DLCI 100:

```
admin> new conn max-switch
CONNECTION/max-switch read

admin> set active = yes

admin> set encaps = frame-relay

admin> set ip remote-address = 10.11.12.3/24

admin> set telco call-type = ft1
```

```
admin> set fr frame-relay-profile = fr-dce

admin> set fr dlci = 100

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

Following is a comparable RADIUS profile:

```
permconn-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "max-switch",
    Framed-Protocol = FR,
    Framed-Address = 10.11.12.3,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-dce"
```

Note: When IP routing is enabled, the MAX TNT creates a route for this destination . Administrators can choose to add static routes to other subnets or to enable RIP updates to or from the router across Frame Relay. The usual considerations for IP routing connections apply (see Chapter 4, “IP Routing”).

Examples of backup interfaces for nailed Frame Relay links

On UNI-DTE and NNI interfaces, the MAX TNT issues Status Enquiries that check the state of the other end of PVC segments on the interface. If a DLCI becomes inactive, and the profile configuring its nailed interface specifies a backup connection, the MAX TNT uses the backup connection to provide an alternate route to the other end. For an introduction to backup interfaces, see “Backup interfaces for nailed connections” on page 2-31.

In the sample profiles that follow, the primary interface is a Frame Relay DLCI interface defined in a profile named `fp7`, and the backup interface is another DLCI interface defined in a profile named `pvc`. In this example, the remote IP address of the primary and the backup connection are different.

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

```
admin> new conn fp7
CONNECTION/fp7 read

admin> set active = yes

admin> set encaps = frame-relay

admin> set fr frame-relay-profile = frt2-7

admin> set fr dlci = 18

admin> set ip remote-address = 10.168.7.9/24

admin> set telco call-type = ft1

admin> set session backup = pvc

admin> write
CONNECTION/fp7 written

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

```
admin> set active = yes
admin> set encaps = frame-relay
admin> set fr frame-relay-profile = frt1-7
admin> set fr dlci = 16
admin> set telco call-type = ft1
admin> set ip remote-address = 10.168.7.11/24
admin> write
CONNECTION/pvc written
```

Following are comparable RADIUS profiles:

```
permconn-tnt1-1 Password = "ascend", User-Service = Dialout-Framed-User
   User-Name = "fp7",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.9,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Backup = "pvc",
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 18,
   Ascend-FR-Profile-Name = "radius-frt2-7",
   Framed-MTU = 1524

permconn-tnt1-2 Password = "ascend", User-Service = Dialout-Framed-User
   User-Name = "pvc",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.11,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 16,
   Ascend-FR-Profile-Name = "radius-frt1-7",
   Framed-MTU = 1524
```

When the MAX TNT brings up the two Frame Relay PVC, the routing table includes entries such as this:

```
...
10.168.7.0/24    10.168.7.9     wan33     rGT     60    1     0    89
10.168.7.0/24    10.168.7.9     wan33     *SG    120    7     0   198
10.168.7.9/32    10.168.7.9     wan33     rT      60    1     0    89
10.168.7.9/32    10.168.7.9     wan33     *      120    7         198
10.168.7.11/32   10.168.7.11    wan32     rT      60    1     0    51
10.168.7.11/32   10.168.7.11    wan33     *S     120    1          89
...
```

At this point, both nailed connections are up, and the output of the Ifmgr command contains entries such as the following:

```
bif slot sif u m p ifname   host-name remote-addr      local-addr
------------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:03 002 *   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

If the primary PVC becomes unavailable, the routing table does not change, but the entries in the output of the Ifmgr command look like the following output:

```
bif slot sif u m p ifname  host-name  remote-addr      local-addr
------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:17 000 +   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

Notice that `fp7` is shown with a plus-sign (+) to show that it is in the Backup Active state (that it is backed up by another connection). When the primary PVC comes up again, the data flow is directed to that interface again. At that point, the Ifmgr command output again shows both interfaces as up.

Concentrating incoming calls onto Frame Relay

A common way to concentrate incoming connections onto a Frame Relay link is by making use of OSI layer 3 (IP routing). For this purpose, the MAX TNT requires ordinary profiles for the callers, and a DLCI logical interface that specifies a destination IP router. When clients dial in to reach the destination router, the MAX TNT consults its routing table to forward the packets onto Frame Relay. In this type of configuration, the MAX TNT acts as a Frame Relay gateway.

For incoming PPP connections, Frame Relay Direct is another way to concentrate the calls onto a Frame Relay link. Frame Relay Direct aggregates multiple PPP connections and forwards them as a combined data stream solely on the basis of the FR-Direct specifications. The assumption is that an upstream device will examine the packets and route them appropriately.

Note: A Frame Relay Direct connection is not a full-duplex tunnel between a PPP dial-in and a far-end device. Although the MAX TNT does not use the router to forward packets onto the Frame Relay link, it must use the router to send packets received across Frame Relay back to the appropriate PPP caller. For this reason, Frame Relay Direct connections must enable IP routing.

Setting up a Frame Relay gateway

To act as a Frame Relay gateway, the Frame Relay DLCI profile must specify a destination router. Incoming connections are routed in the usual way, and all of the usual options apply. Administrators can choose to create static routes, enable or disable RIP, and so forth. For details, see Chapter 4, “IP Routing.”

For background information about specifying a DLCI interface, see “Configuring a DLCI logical interface” on page 3-14.

Routing parameters in the DLCI profile

In addition to the Frame Relay settings described in “Overview of DLCI interface settings” on page 3-14, the following Connection parameters are relevant to a gateway DLCI profile:

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

Parameter	Specifies
IP-Routing-Enabled	Enables/disables IP routing for this connection. It is enabled by default, and must be enabled for a Frame Relay gateway.
Remote-Address	Destination IP address, which lies at the end of a PVC whose first hop is known by the specified DLCI.

Routing parameters in RADIUS

In addition to the attributes described in "Overview of DLCI interface settings" on page 3-14, the following attribute-value pairs must be specified in the permconn profile of a Frame Relay gateway:

Attribute	Value
Ascend-Route-IP (228)	Enables/disables IP routing for this connection. (IP is enabled by default. If this attribute is present, it must be set to Route-IP-Yes for Frame Relay gateway connections.)
Framed-Address (8)	Destination IP address, which lies at the end of a PVC whose first hop is known by the specified DLCI.
Framed-Netmask (9)	A subnet mask for Framed-Address.

Examples of a gateway configuration

In the following example, the MAX TNT acts as a gateway between a client that dials in with the address 10.1.2.3/29, and a remote router that is reachable across Frame Relay, as shown in Figure 3-8:

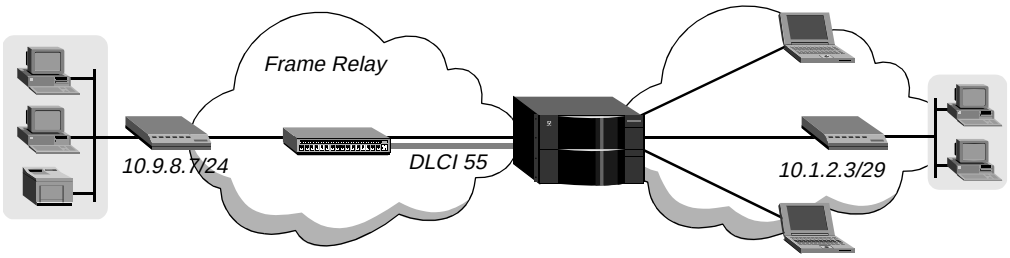


Figure 3-8. Frame Relay gateway

The following set of commands configures an MP+ Connection profile for the dial-in client in Figure 3-8:

```
admin> new connection mpp-client
CONNECTION/mpp-client read

admin> set active = yes

admin> set ppp recv-password = clientpw

admin> set ip remote-address = 10.1.2.3/29

admin> write
CONNECTION/mpp-client written
```

Following is a comparable RADIUS profile:

```
mpp-client Password = "clientpw"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.1.2.3,
    Framed-Netmask = 255.255.255.248
```

The next set of commands configures a DLCI Connection profile to the CPE router:

```
admin> new conn cpe-router
CONNECTION/cpe-router read

admin> set active = yes

admin> set encaps = frame-relay

admin> set ip remote-address = 10.9.8.7/24

admin> set telco call-type = ft1

admin> set fr frame-relay-profile = fr-dte

admin> set fr dlci = 55

admin> write
CONNECTION/cpe-router written
```

Following is a comparable RADIUS profile:

```
permconn-tnt-2 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "cpe-router",
    Framed-Protocol = FR,
    Framed-Address = 10.9.8.7,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 55,
    Ascend-FR-Profile-Name = "fr-dte"
```

Note: The MAX TNT creates a route for this destination and uses it to forward packets from PPP clients. Administrators can choose to add static routes to other subnets or to enable dynamic routing updates to or from the router across Frame Relay. The usual considerations for IP routing connections apply (see Chapter 4, “IP Routing”).

Configuring Frame Relay Direct

When a PPP Connection profile specifies FR-Direct, the MAX TNT simply forwards the data stream out on a specified DLCI interface. It leaves the task of routing the packets to an upstream device.

For background information about specifying a DLCI interface, see “Configuring a DLCI logical interface” on page 3-14.

Settings in a Connection profile

Following are the relevant FR-Direct parameters, shown with sample settings:

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

```
[in CONNECTION/"":fr-options]
fr-direct-enabled = no
fr-profile = ""
fr-dlci = 16

[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 10.111.112.113/24
```

Parameter	Specifies
Encapsulation-Protocol	The encapsulation protocol. Must be set to PPP, MP, or MPP for Frame Relay Direct connections.
FR-Direct-Enabled	Enables/disables FR-Direct mode for this connection.
FR-Profile	Name of the Frame-Relay profile that defines the datalink.
FR-DLCI	DLCI assigned in a Connection profile to a next hop on the specified interface. Multiple FR-Direct Connection profiles can refer to the same DLCI in this setting.
IP-Routing-Enabled	Enables/disables IP routing for this connection. Must be enabled for the MAX TNT to send data back to the appropriate PPP caller.
Remote-Address	PPP caller's IP address. As the MAX TNT receives return packets for many Frame Relay Direct connections on the same DLCI, it uses this address to determine which PPP caller should receive the return packets.

Settings in a RADIUS profile

RADIUS uses the following attribute-value pairs for FR-Direct connections:

Attribute	Value
Framed-Protocol (7)	The encapsulation protocol. Must be set to PPP (1), MP (262), or MPP (256) for FR-Direct connections.
Ascend-FR-Direct (219)	Enables/disables FR-Direct mode for this connection. FR-Direct-No (0) is the default. Set to FR-Direct-Yes (1) for FR-Direct connections.
Ascend-FR-Direct-Profile (220)	Name of the Frame-Relay profile that defines the datalink.
Ascend-FR-Direct-DLCI (221)	DLCI assigned in a Connection profile to a next hop on the specified interface. Multiple FR-Direct Connection profiles can refer to the same DLCI in this setting.
Ascend-Route-IP (228)	Enables/disables IP routing for this connection. (IP is enabled by default.) If this attribute is present, it must be set to Route-IP-Yes to enable the MAX TNT to send data back to the appropriate PPP caller.

Attribute	Value
Framed-Address (8)	PPP caller's IP address. As the MAX TNT receives return packets for many Frame Relay Direct connections on the same DLCI, it uses this address to determine which PPP caller should receive the return packets.
Framed-Netmask (9)	A subnet mask for Framed-Address.

Examples of FR-Direct connections

In Figure 3-9, the MAX TNT forwards the data stream from two PPP dial-in hosts across Frame Relay on the same DLCI interface:

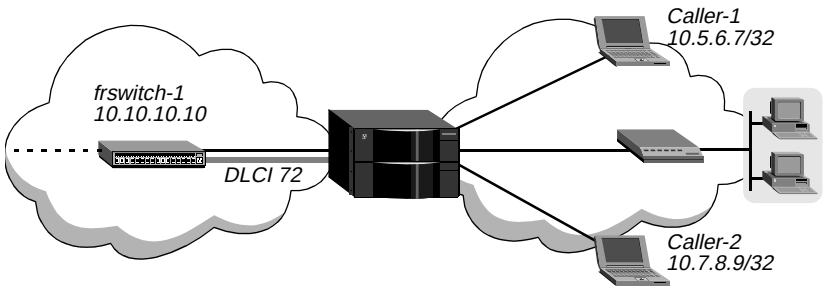


Figure 3-9. Frame Relay Direct

The following commands specify the DLCI interface to frswitch-1 in Figure 3-9:

```
admin> new conn frswitch-1
CONNECTION/frswitch-1 read

admin> set active = yes

admin> set encaps = frame-relay

admin> set ip remote-address = 10.10.10.10/24

admin> set telco call-type = ft1

admin> set fr frame-relay-profile = fr-dte

admin> set fr dlci = 72

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

Following is a comparable RADIUS profile:

```
permconn-tnt-3 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "frswitch-1",
    Framed-Protocol = FR,
    Framed-Address = 10.10.10.10,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 72,
    Ascend-FR-Profile-Name = "fr-dte"
```

The following set of commands configures FR-Direct Connection profiles for the incoming calls:

```
admin> new conn caller-1
CONNECTION/caller-1 read

admin> set active = yes

admin> set encaps = ppp

admin> set ppp recv-password = caller1*3

admin> set ip remote-address = 10.5.6.7/32

admin> set fr fr-direct-enabled = yes

admin> set fr fr-profile = fr-dte

admin> set fr fr-dlci = 72

admin> write
CONNECTION/caller-1 written

admin> new conn caller-2
CONNECTION/caller-2 read

admin> set active = yes

admin> set encaps = ppp

admin> set ppp recv-password = caller2!!8

admin> set ip ip-routing-enabled = yes

admin> set ip remote-address = 10.7.8.9/32

admin> set fr fr-direct-enabled = yes

admin> set fr fr-profile = fr-dte

admin> set fr fr-dlci = 72

admin> write
CONNECTION/caller-2 written
```

Following are comparable RADIUS profiles:

```
caller-1 Password = "caller1*3"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.5.6.7,
    Framed-Netmask = 255.255.255.255
    Ascend-FR-Direct = FR-Direct-Yes,
    Ascend-FR-Direct-Profile = "fr-dte",
    Ascend-FR-Direct-DLCI = 72

caller-2 Password = "caller2!!8"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.7.8.9,
    Framed-Netmask = 255.255.255.255
    Ascend-FR-Direct = FR-Direct-Yes,
    Ascend-FR-Direct-Profile = "fr-dte",
    Ascend-FR-Direct-DLCI = 72
```

Configuring the MAX TNT as a Frame Relay switch

As a Frame Relay switch, the MAX TNT receives frames on one DLCI interface and transmits them on another one. The decision to forward frames is made on the basis of circuit name assignments.

To use the MAX TNT as a switch, you must configure a circuit that pairs two DLCI interfaces. Instead of going to the layer 3 router for a decision on which interface to forward the frames, it relies on the circuit name to relay the frames to the paired interface. A circuit is defined in two Connection profiles, one for each endpoint of the circuit.

Note: When it is operating as a switch, the MAX TNT relays all frames received on one endpoint of the circuit to the other endpoint of the circuit. It does not examine the packets at OSI layer 3.

Overview of circuit-switching options

With a Frame Relay circuit configuration, the MAX TNT can operate as a switch on UNI-DCE interfaces, NNI interfaces, or a combination of the two. NNI is not required.

Routing parameters or attributes should be disabled for switched connections.

Note: Make sure that the Enabled parameter is set to Yes in the Answer-Defaults FR-Answer subprofile.

Settings in a Connection profile

Following are the relevant circuit parameters, shown with sample settings:

```
[in CONNECTION/endpoint-1]
encapsulation-protocol = frame-relay-circuit

[in CONNECTION/"":telco-options]
call-type = ft1

[in CONNECTION/endpoint-1:fr-options]
frame-relay-profile = max
dlci = 100
circuit-name = frcir1

[in CONNECTION/endpoint-2]
encapsulation-protocol = frame-relay-circuit

[in CONNECTION/"":telco-options]
call-type = ft1

[in CONNECTION/endpoint-2:fr-options]
frame-relay-profile = p130-east
dlci = 200
circuit-name = frcir1
```

Parameter	Specifies
Encapsulation-Protocol	Encapsulation protocol. Both endpoints of the circuit must specify Frame-Relay-Circuit encapsulation.
Call-Type	Type of nailed call. Set to FT1 for nailed.

Parameter	Specifies
Frame-Relay-Profile	Name of the Frame-Relay profile that defines the datalink.
DLCI	A DLCI for this PVC endpoint.The DLCI must be obtained from a Frame Relay provider. The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Circuit-Name	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.

Settings in a RADIUS profile

Following are the RADIUS attributes for configuring a Frame Relay circuit:

Attribute	Value
Framed-Protocol (7)	Encapsulation protocol. Both endpoints of a circuit must specify FR-CIR (263) encapsulation.
Ascend-Call-Type (177)	Type of nailed connection: Nailed (1) is the default.
Ascend-FR-Profile-Name (180)	Name of the Frame-Relay profile that defines the datalink.
Ascend-FR-DLCI (179)	A DLCI for this PVC endpoint. The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Ascend-FR-Circuit-Name (156)	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.

Examples of a circuit between UNI interfaces

Figure 3-10 shows a circuit configuration using UNI-DCE interfaces in the MAX TNT:

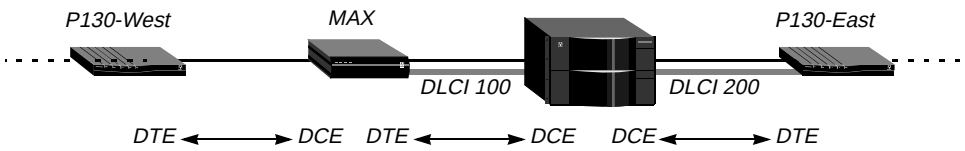


Figure 3-10. Frame Relay circuit with UNI interfaces

Using local profiles

The following commands on the MAX TNT define the datalinks to the MAX and to the Pipeline 130 (P130-East):

```
admin> new frame max
FRAME-RELAY/max read

admin> set active = yes

admin> set nailed-up-group = 111

admin> set link-type = dce

admin> write
FRAME-RELAY/max written

admin> new frame p130east
FRAME-RELAY/p130east read

admin> set active = yes

admin> set nailed-up-group = 222

admin> set link-type = dce

admin> write
FRAME-RELAY/p130east written
```

The next set of commands specifies the circuit between the two Frame Relay interfaces:

```
admin> read conn max6
CONNECTION/max6 read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = max

admin> set fr-options dlci = 100

admin> set fr-options circuit-name = fr-cir1

admin> write
CONNECTION/max6 written

admin> read conn p130
CONNECTION/p130 read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = p130east

admin> set fr-options dlci = 200

admin> set fr-options circuit-name = fr-cir1

admin> write
CONNECTION/p130 written
```

Using RADIUS profiles

The following RADIUS frdlink pseudo-user profiles define the datalinks to the MAX and to the Pipeline 130 (P130-East):

```
frdlink-tnt-21 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 111

frdlink-tnt-22 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "p130east",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 222
```

The next set of profiles specifies the circuit between the two Frame Relay interfaces:

```
permconn-tnt-10 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "max6",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "max",
    Ascend-FR-Circuit-Name = "fr-cir1"

permconn-tnt-11 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "p130east",
    Ascend-FR-Circuit-Name = "fr-cir1"
```

Examples of a circuit between NNI interfaces

Figure 3-11 shows a circuit configuration that uses NNI interfaces:

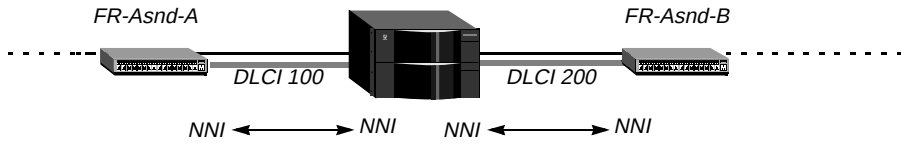


Figure 3-11. Frame Relay circuit with NNI interfaces

Using local profiles

The following commands on the MAX TNT define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
admin> new frame fr-asnd-a
FRAME-RELAY/fr-asnd-a read

admin> set active = yes
```

```
admin> set nailed-up-group = 333

admin> set link-type = nni

admin> write
FRAME-RELAY/fr-asnd-a written

admin> new frame fr-asnd-b
FRAME-RELAY/fr-asnd-b read

admin> set active = yes

admin> set nailed-up-group = 444

admin> set link-type = nni

admin> write
FRAME-RELAY/fr-asnd-b written
```

The next set of commands specifies the circuit between the two Frame Relay interfaces:

```
admin> new conn asnd-a
CONNECTION/asnd-a read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = fr-asnd-a

admin> set fr-options dlci = 100

admin> set fr-options circuit-name = pvc-pipe

admin> write
CONNECTION/asnd-a written

admin> new conn asnd-b
CONNECTION/asnd-b read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = fr-asnd-b

admin> set fr-options dlci = 200

admin> set fr-options circuit-name = pvc-pipe

admin> write
CONNECTION/asnd-b written
```

Using RADIUS profiles

The following frdlink pseudo-user profiles define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
frdlink-tnt-23 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-Call-Type = Nailed,
```

```
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 333

frdlink-tnt-24 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 444
```

The next set of profiles specifies the circuit between the two Frame Relay interfaces:

```
permconn-tnt-12 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "asnd-a",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-FR-Circuit-Name = "pvc-pipe"

permconn-tnt-13 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "asnd-b",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-FR-Circuit-Name = "pvc-pipe"
```

Examples of circuits that use UNI and NNI interfaces

Figure 3-12 shows circuit configurations that use one UNI-DCE and one NNI interface:

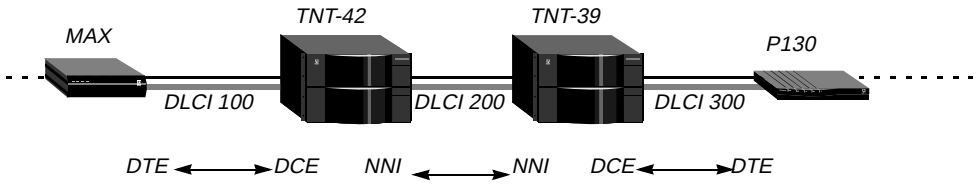


Figure 3-12. Frame Relay circuit with UNI and NNI interface

Using local profiles

The following commands on TNT-42 define the datalinks to the MAX and TNT-39:

```
admin> new frame dce-max
FRAME-RELAY/dce-max read

admin> set active = yes

admin> set nailed-up-group = 555

admin> set link-type = dce

admin> write
FRAME-RELAY/dce-max written

admin> new frame nni-39
FRAME-RELAY/nni-39 read

admin> set active = yes
```

```
admin> set nailed-up-group = 666

admin> set link-type = nni

admin> write
FRAME-RELAY/nni-39 written
```

The next set of commands on TNT-42 specifies the circuit between its two Frame Relay interfaces:

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

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = dce-max

admin> set fr-options dlci = 100

admin> set fr-options circuit-name = cir-42

admin> write
CONNECTION/max written

admin> new conn tnt39
CONNECTION/tnt39 read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = nni-39

admin> set fr-options dlci = 200

admin> set fr-options circuit-name = cir-42

admin> write
CONNECTION/tnt39 written
```

The following commands on TNT-39 define the datalinks to TNT-42 and to the Pipeline 130:

```
admin> new frame nni-42
FRAME-RELAY/nni-42 read

admin> set active = yes

admin> set nailed-up-group = 777

admin> set link-type = nni

admin> write
FRAME-RELAY/nni-42 written

admin> new frame dce-p130
FRAME-RELAY/dce-p130 read

admin> set active = yes

admin> set nailed-up-group = 888

admin> set link-type = dce
```

```
admin> write
FRAME-RELAY/dce-p130 written
```

The next set of commands on TNT-39 specifies the circuit between its two Frame Relay interfaces:

```
admin> new conn tnt42
CONNECTION/tnt42 read
admin> set active = yes
admin> set encaps = frame-relay-circuit
admin> set ip-options ip-routing-enabled = no
admin> set telco call-type = ft1
admin> set fr-options frame-relay-profile = nni-42
admin> set fr-options dlci = 200
admin> set fr-options circuit-name = cir-39
admin> write
CONNECTION/tnt42 written
admin> new conn p130
CONNECTION/p130 read
admin> set active = yes
admin> set encaps = frame-relay-circuit
admin> set ip-options ip-routing-enabled = no
admin> set telco call-type = ft1
admin> set fr-options frame-relay-profile = dce-p130
admin> set fr-options dlci = 300
admin> set fr-options circuit-name = cir-39
admin> write
CONNECTION/p130 written
```

Using RADIUS profiles

The following profiles define the datalinks from TNT-42 to the MAX and TNT-39:

```
frdlink-tnt-25 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 555
frdlink-tnt-26 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 666
```

The next set of profiles specifies the circuit on TNT-42:

```
permconn-tnt-14 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "max"
    Framed-Protocol = FR-CIR,
```

```
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-FR-Circuit-Name = "cir-42"

permconn-tnt-15 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "tnt39",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-FR-Circuit-Name = "cir-42"
```

The following profiles define the datalinks from TNT-39 to TNT-42 and the Pipeline 130:

```
frdlink-tnt-27 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 777

frdlink-tnt-28 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 888
```

The next set of profiles specifies the circuit on TNT-39:

```
permconn-tnt-16 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "tnt42"
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-FR-Circuit-Name = "cir-39"

permconn-tnt-17 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 300,
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-FR-Circuit-Name = "cir-39"
```

Configuring an ATM-Frame Relay circuit

The MAX TNT can receive frames on a Frame Relay DLCI interface and transmit them on an Asynchronous Transfer Mode (ATM) PVC, or vice versa. The decision to forward frames is made on the basis of circuit name assignments. When the MAX TNT receives frames on an ATM-Frame Relay circuit endpoint, it removes the frame's encapsulation and adds the encapsulation required by the other endpoint.

The operations of an ATM-Frame Relay circuit are similar to a regular Frame Relay circuit. The MAX TNT relies on the circuit name to relay the frames to the paired interface. A circuit is defined in two Connection profiles, one for each endpoint of the circuit.

Note: For information about configuring the ATM DS3 slot card, see the *MAX TNT Hardware Installation Guide*.

Settings in a Connection profile

Following are the relevant parameters for an ATM-Frame Relay circuit, shown with sample settings:

```
[in CONNECTION/fr-endpoint]
encapsulation-protocol = frame-relay-circuit

[in CONNECTION/fr-endpoint:fr-options]
frame-relay-profile = fr7
dlci = 100
circuit-name = atmfr-1

[in CONNECTION/fr-endpoint:telco-options]
call-type = ft1

[in CONNECTION/atm-endpoint]
encapsulation-protocol = atm-frame-relay-circuit

[in CONNECTION/atm-endpoint:fr-options]
circuit-name = atmfr-1

[in CONNECTION/atm-endpoint:atm-options]
vpi = 0
vci = 32
atm-enabled = yes

[in CONNECTION/atm-endpoint:telco-options]
call-type = ft1
nailed-groups = 111
```

Parameter	Specifies
Encapsulation-Protocol	Encapsulation protocol. For an ATM-Frame Relay circuit, one endpoint specifies ATM-Frame-Relay-Circuit and the other specifies Frame-Relay-Circuit.
Frame-Relay-Profile	The Frame Relay endpoint specifies the name of the Frame-Relay profile that defines the datalink.
DLCI	A DLCI for the Frame Relay PVC endpoint.The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Circuit-Name	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.

Parameter	Specifies
Call-Type	Type of nailed call. Set to FT1 for nailed.
Nailed-Groups	Group number assigned in the DS3-ATM profile.
VPI	Virtual Path Identifier (VPI) for the ATM PVC. A VPI identifiers the unidirectional transport of ATM cells belonging to a bundle of virtual channels. The VPI/VCI must be assigned by an ATM administrator.
VCI	Virtual Channel Identifier (VCI) for the ATM PVC.

Settings in a RADIUS profile

Following are the RADIUS attributes for configuring an ATM-Frame Relay circuit:

Attribute	Value
Framed-Protocol (7)	Encapsulation protocol. Both endpoints of a circuit must specify FR-CIR (263) or ATM-FR-CIR (265) encapsulation.
Ascend-FR-Profile-Name (180)	The Frame Relay endpoint specifies the name of the Frame-Relay profile that defines the datalink.
Ascend-FR-DLCI (179)	A DLCI for the Frame Relay PVC endpoint. The MAX TNT does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Ascend-FR-Circuit-Name (156)	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.
Ascend-Group (178)	Group number assigned in the DS3-ATM profile.
Ascend-ATM-Vpi (94)	Virtual Path Identifier (VPI) for the ATM PVC. A VPI identifiers the unidirectional transport of ATM cells belonging to a bundle of virtual channels. The VPI/VCI must be assigned by an ATM administrator.
Ascend-ATM-Vci (95)	Virtual Channel Identifier (VCI) for the ATM PVC.

Examples of configuring an ATM-Frame Relay circuit

Figure 3-12 shows circuit configurations that use one UNI-DCE and one NNI interface:

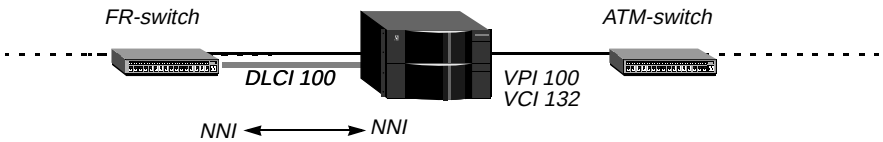


Figure 3-13. ATM-Frame Relay circuit

Using local profiles

The following commands define the datalink to the Frame Relay switch:

```
admin> new frame fr-switch
FRAME-RELAY/fr-switch read

admin> set active = yes

admin> set nailed-up-group = 999

admin> set link-type = nni

admin> write
FRAME-RELAY/fr-switch written
```

The next commands configure the DS3-ATM card:

```
admin> read ds3-atm {1 3 1}
DS3-ATM/{ shelf-1 slot-3 1 } read

admin> set name = atm-switch

admin> set enabled = yes

admin> set line nailed-group = 111

admin> set line high-tx-output = yes

admin> write
ATM-DS3/{ shelf-1 slot-3 1 } written
```

For details about configuring ATM physical links, see the *MAX TNT Hardware Installation Guide*. The next commands specify the circuit between the Frame-Relay and ATM interfaces:

```
admin> new conn fr-endpoint
CONNECTION/fr-endpoint read

admin> set active = yes

admin> set encaps = frame-relay-circuit

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

admin> set telco call-type = ft1

admin> set fr-options frame-relay-profile = fr-switch

admin> set fr-options dlci = 100

admin> set fr-options circuit-name = atmfr-1

admin> write
CONNECTION/fr-endpoint written
```

```
admin> new conn atm-endpoint
CONNECTION/atm-endpoint read
admin> set active = yes
admin> set encaps = atm-frame-relay-circuit
admin> set ip-options ip-routing-enabled = no
admin> set fr-options circuit-name = atmfr-1
admin> set telco call-type = ft1
admin> set telco nailed-groups = 111
admin> set atm vpi = 100
admin> set atm vci = 132
admin> write
CONNECTION/atm-endpoint written
```

Using RADIUS profiles

The following frdlink pseudo-user profile defines the datalink to the Frame Relay switch:

```
frdlink-tnt-33 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-switch",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 999
```

The DS3-ATM card is configured in a local profile, as shown in the preceding section. The next set of profiles specifies the circuit between the Frame Relay and ATM interfaces:

```
permconn-tnt-22 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "fr-endpoint",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-switch",
    Ascend-FR-Circuit-Name = "atmfr-1"

permconn-tnt-13 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "atm-endpoint",
    Framed-Protocol = ATM-FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-Group = "111",
    Ascend-ATM-Vpi = 100,
    Ascend-ATM-Vci = 132,
    Ascend-FR-Circuit-Name = "atmfr-1"
```

IP Routing

4

Routing overview 4-1
Configuring LAN IP interfaces 4-6
Configuring WAN IP interfaces 4-11
Configuring static IP routes 4-23
Setting TCP/IP routing policies 4-30
Configuring DNS 4-43
Configuring and using address pools 4-51
Setting up multicast forwarding 4-58
Configuring virtual routers 4-67

Routing overview

When you power on or reset the MAX TNT, 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 MAX TNT 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 MAX TNT removes the route from its routing table.

Routes and interfaces

An IP route specifies a destination address, a router (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

MAX TNT, 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 or egress to 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

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 router will use 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 MAX TNT 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 4-58.)

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 multicasted 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 an 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, an IP-Interface profile with the following index:

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

has the following interface name:

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

The other names in the interface table, and their significance, are:

- 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 dialout 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 4-58.
- The `tunnel` interface is a pseudo-interface that is used only when the MAX TNT is configured as an ATMP Router Home Agent. In that configuration, the MAX TNT creates a route for each registered mobile client. Regardless of how many tunnels the Home Agent may terminate, there is always a single tunnel interface. (The number terminating the tunnel interface name is an internal number which may change from one software version to the next.)
- The `vr0_main` interface represents the router itself. For details, see “Configuring virtual routers” on page 4-67.
- The `sip0` interface is a soft IP interface. For details, see “Setting a system source IP address” on page 4-30.
- The numbered WAN (`wan`*N*) interfaces are WAN connections, which are entered in the interface table as they become active.

Ascend notation for IP addresses

In the MAX TNT, IP addresses use dotted decimal format (not hexadecimal). If no subnet mask is specified, the MAX TNT assumes a default mask based on the address class. Table 4-1 shows address classes and the number of network bits in the default mask for each class.

Table 4-1. IP address classes

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 MAX TNT assumes the default mask of 24 bits, as shown in Figure 4-1:

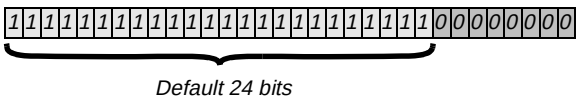


Figure 4-1. Class C IP address

To specify a subnet mask, the MAX TNT appends to the IP address a modifier that specifies the total number of network bits in the address. For example:

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

In this example, the /29 specification indicates that 29 bits of the address are used to specify the network. This is commonly referred to as a 29-bit subnet. The three remaining bits specify unique hosts.

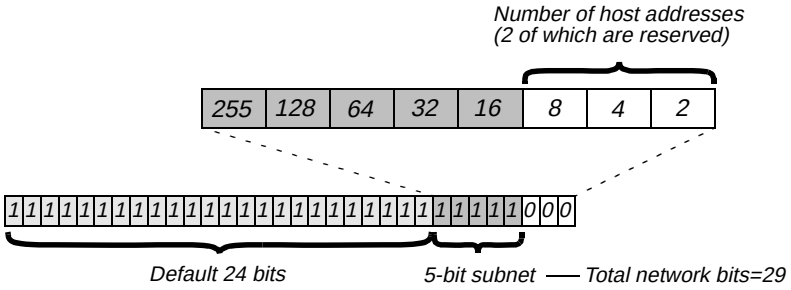


Figure 4-2. 29-bit subnet mask and the number of supported hosts

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: Early implementations of TCP/IP did not allow zero subnets. That is, subnets could not have the same base address that a class A, B, or C network would have. 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 192.32.8.4/30 was legal (192.32.8.0/30 is called a zero subnet, because like a class C base address, its last octet is zero). Modern implementations of TCP/IP allow subnets to have base addresses that might be identical to the class A, B, or C base addresses. Ascend's implementations of RIP-v2 and OSPF treat these so-called zero 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 4-2 shows standard and Ascend subnet formats for a class C network number.

Table 4-2. Standard subnet masks and Ascend notation

Subnet mask	Number of host addresses	Ascend notation
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, if the MAX TNT configuration assigns the following address to a remote router:

```
198.5.248.120/29
```

The Ethernet 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 subnet mask of /32. For example:

```
198.5.248.40/32
```

Host routes are required for dial-in hosts. The route is 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. The MAX TNT 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
    66  09/14/1998  10:13:24  { { shelf-1 controller 1 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 2 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 3 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 4 } 0 }
    64  09/14/1998  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 consist 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 4-9.

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.
Proxy-Mode	Enables/disables proxy ARP responses for dial-in devices that are assigned local addresses.
RIP-Mode	Enables/disables RIP updates on the interface. RIP is disabled by default on LAN interfaces.
Route-Filter	Filter for RIP update packets. For details, see Chapter 10, "Ascend Packet Filters."
RIP2-Use-Multicast	Enables/disables 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 the MAX TNT to an OSPF network" on page 5-9.
Multicast-Allowed	Multicast forwarding option. See "Setting up multicast forwarding" on page 4-58.
Multicast-Rate-Limit	Multicast forwarding option. See "Setting up multicast forwarding" on page 4-58.
Multicast-Group-Leave-Delay	Multicast forwarding option. See "Setting up multicast forwarding" on page 4-58.
Directed-Broadcast-Allowed	Enables/disables 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 4-72.
Management-Only-Interface	Enables/disables management-only on the IP interface.

Example of configuring a LAN IP interface

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

```
admin> dir ip-interface
    66  09/14/1998  10:13:24  { { shelf-1 controller 1 } 0 }

admin> read ip-interface { { 1 c 1 } 0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> set ip-address = 10.1.2.65/24

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

In this example, the MAX TNT 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 4-26.

After you assign an IP address, you can verify that the MAX TNT 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 MAX TNT 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 MAX TNT is set to respond to ARP requests for inactive connections, it brings up the required WAN connection.

The following commands enable the MAX TNT to respond as proxy for ARP requests for active WAN connections:

```
admin> read ip-interface { { 1 c 1 } 0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> set proxy-mode = active

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

Enabling RIP

RIP is off by default, so the MAX TNT does not send out its routing table or receive routing information from other routers on the interface. This means that 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 MAX TNT routing table. It can access more networks, but route searches are not as fast. Sending updates propagates information about remote networks to local routers.

Note: Ascend does not recommend running RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other’s advertisements. 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 the MAX TNT to receive RIP-v2 updates on the multicast address:

```
admin> read ip-interface { { 1 c 1 } 0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> set rip-mode = routing-recv-v2

admin> write
IP-INTERFACE/{ { shelf-1 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 interface-independent IP address

The interface-independent IP address is a soft destination address for the MAX TNT. It is *soft* because it is not associated with a physical port, which means that it is always accessible to inbound traffic. The interface-independent address must be unique.

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

You define the interface-independent address in the IP-Interface profile with the default index ({ { any-shelf any-slot 0 } 0 }), which is reserved for that purpose. For example, the following commands set the soft interface address to 11.168.7.100:

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

admin> set ip-addr = 11.168.7.100

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 MAX TNT 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 "Configuring virtual routers" on page 4-67.

If routing updates (RIP or OSPF) are enabled, the MAX TNT 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 MAX TNT must have a static route to the soft address. To verify that other hosts in your network have a route to the soft address, use 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 the direction of packets to IP broadcast addresses. These attacks are intended to cause degraded network performance, possibly to the point that the network becomes unusable.

To prevent the MAX TNT router from being used as an intermediary in this type of denial-of-service attack launched from another network, you should disable the MAX TNT from forwarding directed broadcasts it receives from another network. The following example shows how to disable directed broadcasts that are not generated locally on all IP interfaces of a MAX TNT with a four-port Ethernet card in shelf 1, slot 12:

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

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 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. It 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. The MAX TNT creates a routed 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 MAX TNT 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, the 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, as shown in the next sections.

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	Enables/disables IP routing for the interface. IP routing is enabled by default.
VJ-Header-Prediction	Enables/disables Van Jacobsen prediction for TCP packets on incoming calls using encapsulation protocols that support this feature. The default setting is Yes.
Remote-Address	IP address of the calling device, which can include a subnet specification. If it 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 “Examples of a numbered-interface connection” on page 4-18.)
Routing-Metric	RIP metric for the specified route (a number between 1 to 15, default 1). If preference values are equal, the higher the metric, the less likely that the MAX TNT 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 4-34.
Down-Preference	Preference value for the route when the interface is down.

Parameter	Specifies
Private-Route	Enables/disables advertisement of the route when the router sends RIP or OSPF updates. If set to Yes, the route is excluded from update packets.
Multicast-Allowed	See "Setting up multicast forwarding" on page 4-58.
Address-Pool	Number of the address pool from which to acquire an address (see "Configuring and using address pools" on page 4-51).
IP-Direct	IP address of a host to which all IP packets received across the link will be directed (see "Examples of an IP-Direct connection" on page 4-19).
RIP	Enables/disables RIP updates on the interface. RIP is disabled by default.
Route-Filter	Filter for RIP update packets. For details, see Chapter 10, "Ascend Packet Filters."
Source-IP-Check	Enables/disables anti-spoofing for the session. When set to Yes, the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet.
OSPF-Options	OSPF routing options (see Chapter 5, "OSPF Routing").
Multicast-Rate-Limit	Multicast forwarding option (see "Setting up multicast forwarding" on page 4-58).
Multicast-Group-Leave-Delay	Multicast forwarding option (see "Setting up multicast forwarding" on page 4-58).
Client-DNS-Primary-Addr	Client DNS option (see "Using client DNS" on page 4-49.)
Client-DNS-Secondary-Addr	Client DNS option (see "Using client DNS" on page 4-49.)
Client-DNS-Addr-Assign	Client DNS option (see "Using client DNS" on page 4-49.)
Client-Default-Gateway	Default route for traffic from this connection. For details, see "Examples of client default gateways" on page 4-21.
TOS-Options:Active	Enables/disables proxy-QoS and TOS for this connection (see "Examples of setting QoS and TOS policy" on page 4-22).
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, those 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).

Parameter	Specifies
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 based on 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	In which direction TOS is enabled. If set to Input (the default), bits are set in packets received on the interface. If set to Output, bits are set in outbound packets only. If set to Both, both incoming and outgoing packets are tagged.

Settings in RADIUS profiles

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

Attribute	Value
Ascend-Route-IP (228)	Enables/disables IP routing for the interface. IP routing is enabled by default.
Framed-Compression (13)	Enables/disables Van Jacobsen prediction. You can specify Van-Jacobson-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-Address (8)	IP address of the calling device.
Framed-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 "Examples of a numbered-interface connection" on page 4-18.)
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 between 1 to 15, default 7). If preference values are equal, the higher the metric, the less likely that the MAX TNT will use the route.
Ascend-Route-Preference (126)	A 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 4-34.
Framed-Route (22)	A static route definition, which can be used to make a user profile a private route. See "Configuring static IP routes" on page 4-23.
Ascend-Assign-IP-Pool (218)	Number of the address pool number from which to acquire an address (see "Configuring and using address pools" on page 4-51).
Ascend-Assign-IP-Global-Pool (146)	Name of a global address pool (see "Global RADIUS pools (RADIPAD)" on page 4-52).

Attribute	Value
Ascend-IP-Direct (209)	IP address of a host to which all IP packets received across the link will be directed (see “Examples of an IP-Direct connection” on page 4-19).
Framed-Routing (10)	Enables/disables 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)	Enables/disables anti-spoofing for the session. The default is Source-IP-Check-No (0). When set to Source-IP-Check-Yes (1), the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet.
Ascend-Multicast-Client (155)	Multicast forwarding option (see “Setting up multicast forwarding” on page 4-58).
Ascend-Multicast-Rate-Limit (152)	Multicast forwarding option (see “Setting up multicast forwarding” on page 4-58).
Ascend-Multicast-GLeave-Delay (111)	Multicast forwarding option (see “Setting up multicast forwarding” on page 4-58).
Ascend-Client-Primary-DNS (135)	Client DNS option (see “Using client DNS” on page 4-49.)
Ascend-Client-Secondary-DNS (136)	Client DNS option (see “Using client DNS” on page 4-49.)
Ascend-Client-Assign-DNS (137)	Client DNS option (see “Using client DNS” on page 4-49.)
Ascend-Client-Gateway (132)	Default route for traffic from this connection (see “Examples of client default gateways” on page 4-21).
Ascend-IP-TOS (88)	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. which are used to choose a link based on the type of service. One of the following values can be specified: Ascend-IP-TOS IP-TOS-Normal (0): Normal service. Ascend-IP-TOS IP-TOS-Disabled (1): Disables 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.

Attribute	Value
Ascend-IP-TOS-Precedence (89)	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, those bits can be set 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 (90)	In which direction TOS is enabled. If set to IP-TOS-Apply-To-Incoming (1024), which is the default, bits are set in packets received on the interface. If set to IP-TOS-Apply-To-Outgoing (2048), bits are set in outbound packets only. If set to IP-TOS-Apply-To-Both (3072), both incoming and outgoing packets are tagged.

Examples of a connection to another IP router

Figure 4-3 shows the MAX TNT connecting to a far-end router, such as an Ascend Pipeline. This could be a telecommuting configuration, for example, where the Pipeline is located at a branch or home office.

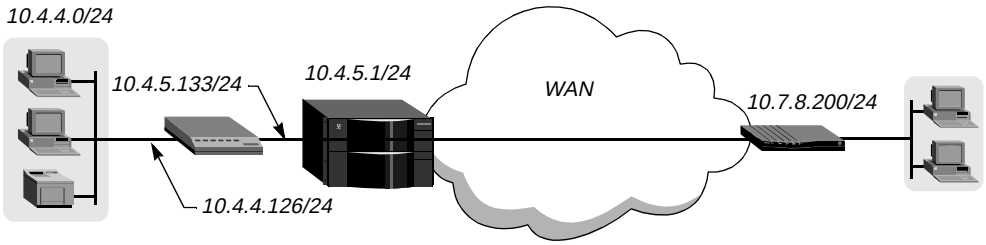


Figure 4-3. Router-to-router IP connection

The default settings for the IP-Options subprofile enable IP routing and Van Jacobsen header compression and turn RIP off. Those are the appropriate settings for the following example, which configures a Connection profile for the Pipeline in Figure 4-3:

```
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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.7.8.200,
    Framed-Netmask = 255.255.255.0

route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.7.8.0/24 10.7.8.200 1 n pipeline1-out"

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

Examples 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 4-4 shows a sample connection in which a dial-in host with an ISDN modem card calls into the MAX TNT.

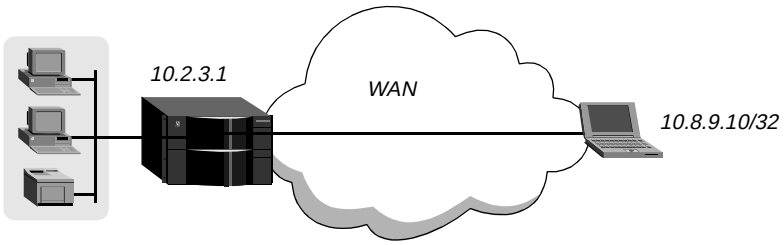


Figure 4-4. Dial-in host requiring a static IP address (a host route)

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 configures the Connection profile for the host in Figure 4-4:

```
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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.8.9.10,
    Framed-Netmask = 255.255.255.255
```

Examples 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 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. The MAX TNT accepts IP packets destined for the specified address and treats them as destined for the system itself. (The packets may 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 MAX TNT unit's real, physical LAN interfaces. Assigning one of the MAX TNT IP addresses will cause routing problems.

Figure 4-5 shows a numbered-interface connection. The real, physical MAX TNT 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.

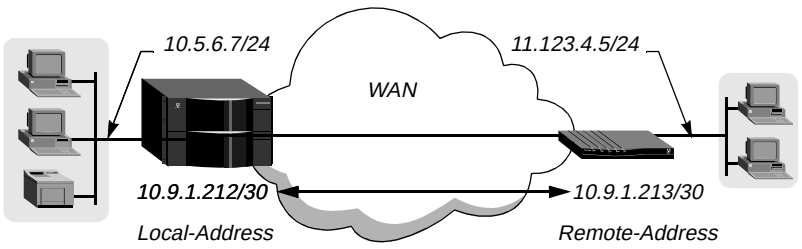


Figure 4-5. A numbered interface connection

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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Route-IP = Route-IP-Yes,
    Framed-Address = 10.9.1.213,
    Framed-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 those 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 4-38.

Examples 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. At this time, the feature is implemented only for data calls. Figure 4-6 shows an example of the IP-Direct traffic flow.

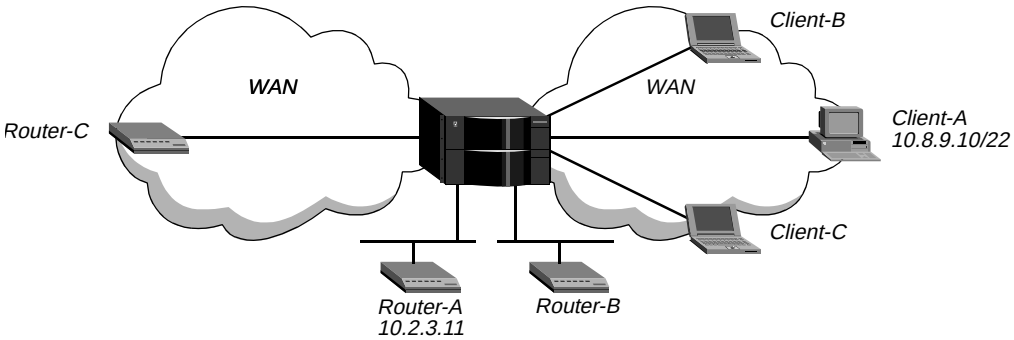


Figure 4-6. IP Direct connections

In Figure 4-6, 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 MAX TNT, 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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.8.9.10,
    Framed-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 MAX TNT can correctly forward packets *destined* for the client.
- ARP requests received from the incoming connection are ignored.
- The caller cannot Telnet to the MAX TNT, because the connection is passed through to the IP-Direct host.

Examples 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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.8.9.10,
    Framed-Netmask = 255.255.255.0,
    Framed-Route = "10.8.9.10/24 0.0.0.0 3 y"
```

Examples of client default gateways

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

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

Packets from other users or from the Ethernet 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". User-Service = Framed-User
    Ascend-Client-Gateway = 17.1.1.1
```

Examples of per-session source address checking

Administrators can configure WAN IP interfaces so 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 MAX TNT 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 anti-spoofing:

```
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"
    User-Service = Framed-User,
    Ascend-Source-IP-Check = Source-IP-Check-Yes
```

Examples of setting QoS and TOS policy

You can configure the MAX TNT to set Quality of Service (QoS) priority bits and Type of Service (TOS) classes of service on behalf of customer applications. The MAX TNT 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 MAX TNT 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 administrators 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 10, “Ascend 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. This 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. This means that the priority-queuing router will choose a high bandwidth connection if one is available, even if it is of higher cost, higher latency, or 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"
    User-Service = 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 MAX TNT cannot find a route. If the administrator defines a default route (with the zero destination address), the MAX TNT routes all packets with unknown destinations to the specified gateway. If no default route is defined, the MAX TNT 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 MAX TNT 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 MAX TNT.

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.

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 settings 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.

Parameter	Specifies
Metric	RIP metric for the specified route (a number between 1 to 15, default 8). If preference values are equal, the higher the metric, the less likely that the MAX TNT will use the route.
Cost	OSPF option (see "Configuring OSPF static route information" on page 5-16).
Preference	Preference value of the route. For details, see "Setting static route preferences" on page 4-34.
Third-Party	OSPF option (see "Configuring OSPF static route information" on page 5-16).
ASE-Type	OSPF option (see "Configuring OSPF static route information" on page 5-16).
ASE-Tag	OSPF option (see "Configuring OSPF static route information" on page 5-16).
Private-Route	Enables/disables advertisement of the route when the router sends RIP or OSPF updates. If set to Yes, the route is excluded from update packets.
Active-Route	Enables/disables entering the route in the routing table. (Setting this to No is a useful way to make a route temporarily inactive, so you can reinstate the route later.)
ASE7-Adv	OSPF option (see "Configuring OSPF static route information" on page 5-16).
VRouter	Virtual router option (see "Defining VRouter static routes" on page 4-74).
Inter-VRouter	Virtual router option (see "Defining VRouter static routes" on page 4-74).

Settings in a RADIUS route profiles

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

`route-`*`name`*`-N Password = "ascend", User-Service = Dialout-Framed-User`

The *name* argument is the MAX TNT 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 MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

Note: To specify routes that may 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 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.

Syntax element	Specifies
gateway-addr	IP address of the next-hop router to reach the specified destination.
metric	RIP metric for the specified route (a number between 1 to 15, default 8). If preference values are equal, the higher the metric, the less likely that the MAX TNT will use the route.
private	Enables/disables advertisement of the route when the router sends RIP or OSPF updates. If set to Yes, the route is excluded from update packets. Set to Y to make the route private.
profile	Name of the dialout 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 4-34.
VRouter	Virtual router option (see “Defining VRouter static routes” on page 4-74).

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. See “Settings in a RADIUS route profiles” on page 4-24 for details about Framed-Route usage.

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 MAX TNT replaces with the caller’s IP address.When RADIUS authenticates the caller and sends the MAX TNT an Access-Accept message with a value of 0.0.0.0 for the router address, the MAX TNT updates its routing tables with the Framed-Route value, but substitutes the caller’s IP address for the router. This setting is useful when the MAX TNT assigns an IP address from an address pool and RADIUS cannot know the IP address of the caller.

If a Framed-Route definition in a user profile duplicates a route defined in a route 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 in RADIUS 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 MAX TNT 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 pairs configure IP options in a RADIUS profile:

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 4-29.

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, it forwards the packet to a default route rather than dropping the packet. If there is no default route in the routing table, the MAX TNT drops packets for which it cannot find a route.

The MAX TNT 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 the zero destination and a valid gateway address.

Examples of a LAN-based default route

Figure 4-7 shows a router that resides on the same subnet as one of the MAX TNT unit's local IP interfaces:

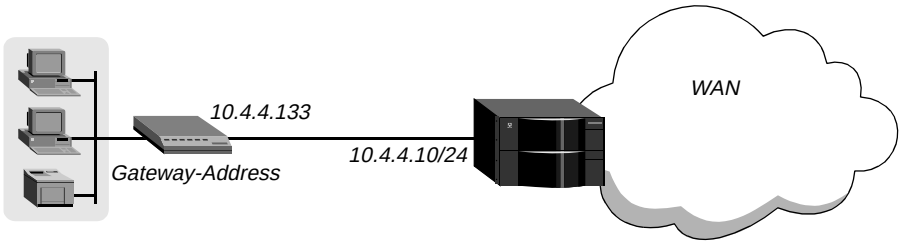


Figure 4-7. Default route to a local IP router

Because the MAX TNT is located on a subnet, it needs to be informed about other backbone routers that can route beyond the subnet. In this example, the MAX TNT 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "0.0.0.0 10.4.4.133"
```

Examples of a default route across a WAN link

Figure 4-8 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 MAX TNT removes the route from its routing table.

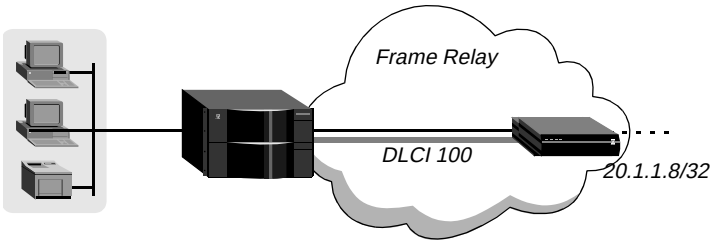


Figure 4-8. Default route across a Frame Relay DLCI interface

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
```

and 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "0.0.0.0 20.1.1.8 y"
```

Examples 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 4-9 shows an example.

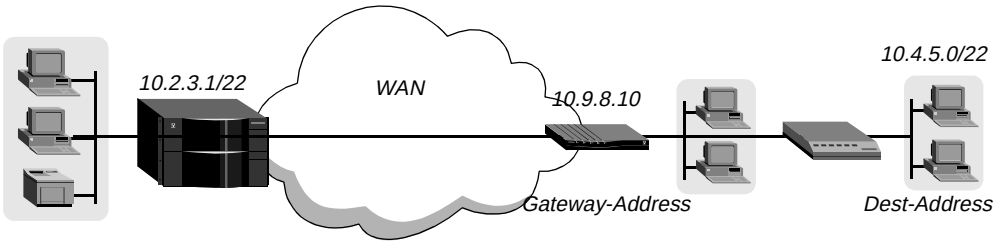


Figure 4-9. Static route to a remote subnet

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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.4.5.0/22 10.9.8.10"
```

Examples 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 MAX TNT 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
```

Following is a comparable RADIUS profile:

```
route-tnt-2 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.76.109.0/24 11.65.212.1 2",
    Framed-Route = "10.76.109.0/24 11.65.210.1 2"
```

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
```

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 user profile that creates three private routes associated with this caller:

```
pipe50 Password = "ascend" User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.1.1.1,
    Framed-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 this connection contains the following routes, including a 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 may also specify the Ascend-Client-Gateway attribute, but it will *not* modify the private default route if one has been specified via the Ascend-Private-Route attribute.

When the next-hop router address in 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, with the private routes defined in the following RADIUS user profile:

```
pipe50 Password = "ascend" User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.1.1.1,
    Framed-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 table, a route lookup for the 20.1.0.0/16 network proceeds to the global routing table.

Setting TCP/IP routing policies

The MAX TNT 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 MAX TNT to set QoS priority bits and TOS classes of service on behalf of customer applications, which 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 “Examples of setting QoS and TOS policy” on page 4-22.

Setting a system source IP address

The system IP address is the source address used for all packets generated by the system, such as 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 interface-independent IP address” on page 4-9.

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 MAX TNT 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. 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 6-2.

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
    66  09/14/1998  10:13:24  { { shelf-1 controller 1 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 2 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 3 } 0 }
     8  09/14/1998  11:36:32  { { shelf-1 slot-12 4 } 0 }
     8  09/14/1998  11:36:59  { { shelf-1 slot-12 5 } 0 }
    64  09/14/1998  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	Enables/disables rejection of an assigned IP address by an incoming caller during PPP negotiation.
Shared-Prof	Enables/disables shared profiles. Sharing profiles is recommended only in low-security networks.
Telnet-Password	Password required for Telnet access to the 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 MAX TNT 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 MAX TNT 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 4-56.

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 cannot result in a shared IP address (two callers at different locations sharing the same address). So, the profile must either 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 on dynamic IP address assignment, see "Examples of assigning an address from a pool" on page 4-56.

Restricting Telnet access to the system:

A user can initiate a Telnet session to the MAX TNT command line from a local workstation or from a WAN connection. In both cases, the MAX TNT 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 *MAX TNT Reference Guide*.)

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 = Ascend

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 MAX TNT prompts again for a user name and password to authenticate a User profile. In the following example, a user starts a Telnet session to a MAX TNT unit named TNT01, which has a configured Telnet password.

```
% telnet tnt01
<tnt01> Enter Password:

Trying 10.1.2.3 ...
Connected to tnt01.abc.com.
Escape character is '^]'.
User:
```

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

Setting system-wide 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	Enables/disables processing of ICMP Redirect packets.
ICMP-Reply-Directed-Bcast	Enables/disables responding as a host to directed-broadcast ICMP Echo requests.
Drop-Source-Routed-IP-Packets	Enables/disables 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. Many sites choose to ignore ICMP Redirects for security purposes.

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

The following commands configure the system to ignore both types of ICMP packets. (It does not respond to ICMP Echo requests to the broadcast address by default.)

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

admin> set ignore-icmp-redirects = yes
```

```
admin> write
IP-GLOBAL written
```

Dropping source-routed packets

The Drop-Source-Routed-IP-Packets parameter default is No, which causes the router to forward all source routed packets as described in RFC1812, *Requirements For Routers*. When 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 MAX TNT 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, using 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 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, 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 MAX TNT 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	A policy for sending update packets that include routes received on the same interface.
Summarize-RIP-Routes	Enables/disables summarization of subnet information in RIP-v1 updates. This setting has no effect on RIP-v2 updates.
RIP-Trigger	Enables/disables RIP triggering. If set to Yes (the default), RIP updates include only changed routes.
RIP-Pref	Preference setting for routes learned from RIP.
Dialout-Poison	Enables/disables advertisement of dialout routes when no trunks are available, to allow a redundant unit to take over.
Ignore-Def-Route	Enables/disables 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 MAX TNT will not drop any RIP packets, no matter how far behind it gets.
Suppress-Host-Routes	Enables/disables suppression of host routes for interfaces with a subnet mask less than 32 bits.
OSPF-Pref	OSPF option (see “Configuring route options” on page 5-14).
OSPF-ASE-Pref	OSPF option (see “Configuring route options” on page 5-14).
RIP-Tag	OSPF option (see “Configuring route options” on page 5-14).
RIP-ASE-Type	OSPF option (see “Configuring route options” on page 5-14).
AS-Boundary-Router	OSPF option (see “Configuring route options” on page 5-14).

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 command 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 in the MAX TNT router as well as 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 5 to 8 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. The full table update is no longer broadcast at fixed 30-second intervals, to prevent RIP routers on a network synchronizing and sending large updates in unison.

Setting the preference value for routes learned from RIP updates

For an introduction to route preferences, see “Setting static route preferences” on page 4-34. The following command increases the preference value of routes learned from RIP updates, instructing the router to use those routes only if no other route exists to the same destination:

```
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 Ascend unit

If you have another Ascend unit backing up the MAX TNT 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 MAX TNT unit’s trunks experience an alarm condition, the MAX TNT 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 MAX TNT 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 MAX TNT 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, as well as the total packets received and total packets dropped on each port. The total packets received count includes the total packets dropped. 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 specifies a subnet mask 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 specifies 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 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 intra-shelf and inter-shelf routing and route caching:

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

Parameter	Specifies
IProute-Cache-Enable	Enables/disables the route cache. If you must control memory usage for a card, you can restrict the cache size or disable the route cache. *Ascend recommends that you do not disable route caches or change their 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	Enables/disables IP packet forwarding card-to-card based on the packet destination IP address and port. If set to No, packets destined for the MAX TNT 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 MAX TNT 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 (an Ethernet card, for example).
- 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 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 MAX TNT itself at a higher protocol layer, such as 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 MAX TNT 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 going 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 MAX TNT system itself. So the packets are delivered to the router, which forward 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), packets destined for the MAX TNT are routed from the slot card that receives them (such as the Ethernet card) to the destination slot card (such as the modem card) directly, rather than going 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	Enables/disables querying a BOOTP server.
RARP-Enabled	Enables/disables obtaining the system's IP addresses from a RARP server.
UDP-Cksum	Enables/disables UDP checksums.
TCP-Timeout	Interval for TCP retry attempts. Valid values are from 0 to 200 seconds.
Finger	Enables/disables response to remote Finger queries. When Finger is set to No (the default), the MAX TNT rejects queries from Finger clients and sends a message that the Finger online user list is denied.
BOOTP-Relay:Active	Enables/disables 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	Enables/disables the SNTP protocol.
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 Bootstrap Protocol and Reverse-ARP

The Bootstrap 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 MAX TNT, including Telnet, Rlogin, TCP-clear, and the TCP portion of DNS queries. It applies to established TCP connections as well as to initial attempts to connect. You might adjust the TCP retry timer because, for example, when a user employs client software to enter a host name 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 must be determined by experience. It depends on the characteristics of the TCP destination (server) hosts. For example, if the destinations are all on a LAN under the same administrative control as the MAX TNT and are lightly loaded, then 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 MAX TNT can return user information to a remote Finger query. The following commands enable the MAX TNT 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 TNT1 by using the following command:

```
# finger @tnt1
```

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 @tnt1
```

displays 140-character-wide format of session information for the system named TNT1. The client can also request the details of all sessions, or of a single session. For example, to request information about a single user named Gavin:

```
# finger gavin@tnt1
```

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 and a BOOTP server do not reside on the same IP network, 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 MAX TNT uses the first server until it becomes unavailable. Once it starts using the second server, it continues using that server until it becomes unavailable, at which time it switches back to using the first server again.

For information about configuring BOOTP-Relay to access a DHCP server in support of DSLPipe Plug & Play, see the *MAX TNT Hardware Installation Guide*.

Using SNTP to set and maintain the MAX TNT system time

The MAX TNT 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 UTC, so the offset is UTC -0130. For San Francisco, which is 8 hours earlier UTC, the offset is UTC -0800. For Frankfurt, which is 1 hour later than UTC, it 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 MAX TNT always communicates with the first address unless it is inaccessible. In that case, the MAX TNT attempts to communicate with the second address, trying the third address only if the other two are inaccessible.

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 MAX TNT, 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 DNS list

Following are the parameters (shown with default settings) for configuring DNS to allow lookups and support 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 MAX TNT appends this domain name to host names 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	Enables/disables 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 host name is not found in the primary domain.

Specifying domain names for lookups

When the MAX TNT receives a host name 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 in the first domain name, the router tries again with the secondary domain name.

Specifying local DNS server addresses

To enable the MAX TNT 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 MAX TNT 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 4-49.

Supporting DNS list

Some DNS servers support a list feature that enables them to return multiple addresses for a host name 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 physical links when hosts are unavailable, you can support DNS list in the MAX TNT. 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 4-48.)

Setting up a local DNS table

The MAX TNT can maintain in RAM a DNS table of up to 8 host names 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 MAX TNT can resolve the local set of DNS names in case 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

the administrator subsequently modifies 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 (the limit set by the maximum DNS-List-Size). The DNS-Local-Table subprofile allows a single IP address per host name. (For related information, see “Using the Auto-Update feature” on page 4-48.)

To set up the local DNS table, the administrator configures 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
```

Parameter	Specifies
DNS-Local-Table:Enabled	Determines 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. If set to Yes, the MAX TNT attempts to resolve the query by consulting the DNS table in RAM. If the host name in the DNS query has an entry in the table in RAM, the system returns the associated IP address(es) to the requester.
DNS-Local-Table:Auto-Update	Determines whether regular successful DNS queries update the local DNS table.For details about Auto-Update, see “Using the Auto-Update feature” on page 4-48
DNS-Local-Table:Table-Config[1–8]	An array of up to 8 host names and IP addresses for inclusion in the local DNS table.
DNS-Local-Table:Table-Config:Host-Name	A host name, which must be unique within the table and meet the requirements described in the next section.
DNS-Local-Table:Table-Config:IP-Address	A valid IP address for the Host-Name, 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.

Host name matching

A host name 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 may be a host name or a fully qualified domain name. If the name does not include a domain name, and the administrator has specified one or more Domain-Name settings (see "Configuring DNS" on page 4-43), the system appends the specified domain name when looking up the host name. For example, for a DNS query on the following host name:

```
host-name = wheelers
```

The MAX TNT searches for the host name and for the following 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 host name, 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 host name, 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 host name in the local table. If there is an entry for the host name, the entry's IP address(es) is replaced by the query response. The following parameters, which are shown with their default values, affect how the table is updated when Auto-Update is set to Yes:

```
[in IP-GLOBAL]
dns-list-attempt = no
dns-list-size = 6
```

If DNS-List-Attempt is set to No, a successful DNS query returns a single address for a given host name. 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 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 the administrator modifies 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 Auto-Update 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, the administrator configures 8 host names with null addresses and then sets Auto-Update to Yes. The DNS-Local-Table changes will be propagated to RAM, and successful DNS queries to the specified host names will build the 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 system-wide to allow all dial-in clients access to one or two DNS servers. Or it can be configured on a connection basis, to allow that 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.
Allow-As-Client-DNS-Info	Enables/disables 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	Enables/disables client DNS for the connection. If set to True (the default), the system presents client DNS server addresses while negotiating the connection. The addresses it presents may 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:

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)	Enables/disables client DNS for the connection. If set to DNS-Assign-Yes (1), the system presents client DNS server addresses while negotiating the connection. The addresses it presents may 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 both of these client DNS servers are not accessible and the caller's profile does not specify client DNS servers, the MAX TNT 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"
    User-Service = 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 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 so it is 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).

See “Defining address pools for a VRouter” on page 4-72 for related information.

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, 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. For details on installing RADIPAD, see the *MAX TNT RADIUS Guide*.

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	Sets the Pool Summary flag (see "Examples of configuring summarized address pools" on page 4-55).
Pool-OSPF-Adv-Type	OSPF option (see "Configuring route options" on page 5-14).
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. A pools pseudo-user profile uses the following format on its first line:

`pools-`*`name`* `Password = "ascend", User-Service = Dialout-Framed-User`

The *name* argument is the MAX TNT 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 designate two pools by the same number, 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 MAX TNT 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 MAX TNT 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 MAX TNT or other Ascend units 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 may 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-pool pseudo-user profile on the server running RADIPAD. The first line of a global-pool pseudo-user profile uses the following format:

`global-pools-`*`name`* `Password = "ascend", User-Service = Dialout-Framed-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 4-52, and it follows the same rules for global pools.

In addition to the definitions described in the preceding section for Ascend-IP-Pool-Definition (217), when the MAX TNT 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 pool with the first available IP address.

Specifying the RADIPAD host

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

```
radipa-hosts Password = "ascend", User-Service = Dialout-Framed-User
```

Subsequent lines in the profile define which Ascend units can assign addresses from the pools managed by RADIPAD, using the following attribute value pairs:

Attribute	Value
Ascend-Assign-IP-Client (144)	Address of an Ascend 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 right IP address for RADIPAD to work.

For example:

```
radipa-hosts Password ="ascend", User-Service = Dialout-Framed-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 can include multiple clients. The sample profile indicates that two Ascend units (10.31.4.10 and 10.31.4.11) can access RADIPAD pools as clients.

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-tnt01 Password = "ascend", User-Service = Dialout-Framed-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", User-Service = Dialout-Framed-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 255.255.255.0 netmask for PPP interfaces, you can define pools on networks wider than /24. For example, the following commands define an address pool on a /23 network:

```
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 255.255.252.0). Following are comparable RADIUS definitions:

```
pools-tnt01 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-IP-Pool-Definition = "1 10.55.178.1 510"

global-pool-ppp Password ="ascend", User-Service = Dialout-Framed-User
    Ascend-IP-Pool-Definition = "1 10.55.178.1 510"
```

Note: 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 and x.y.z.255.

Examples 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 MAX TNT 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 two to Assign-Count 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 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 example commands, the Assign-Count is set to 62. When you add two to the Assign-Count, you get 64. The subnet mask for 64 addresses is 255.255.255.192 (256–64 = 192). The Ascend subnet notation for a 255.255.255.192 mask is /26.

The Pool-Base-Address is set to 10.12.253.1. When you subtract one from this address, 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-tnt01 Password = "ascend", User-Service = Dialout-Framed-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", User-Service = Dialout-Framed-User
    Ascend-IP-Pool-Definition = "1 10.12.253.1 62"
```

The MAX TNT 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 MAX TNT 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 MAX TNT 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 MAX TNT assigns one from a pool. A host requests an address by configuring its client software with 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 4-10 shows a dial-in host requesting and being assigned an IP address:

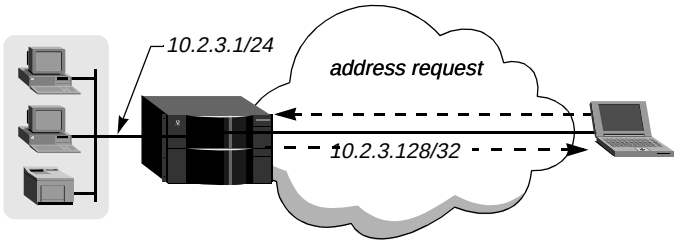


Figure 4-10. Dial-in host requiring assigned IP address

The following commands enable dynamic address assignment system-wide:

```
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 4-31.

The following commands configure a profile to acquire an address from the first pool that has available addresses (Pool 0):

```
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"
    User-Service = 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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Global-Pool ="global-pool-ppp"
```

Setting up multicast forwarding

Video and audio transmissions use one-to-many and many-to-many communication, rather than the point-to-point communications that many other types of network applications use. This type of transmission is provided by the IP Multicast Backbone (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 using the Internet Group Management Protocol (IGMP). The MAX TNT forwards IGMP version-1 or version-2 packets, including IGMP MTRACE (multicast trace).

Figure 4-11 shows a MAX TNT forwarding multicast traffic from an MBONE router across the WAN to two WAN multicast client interfaces and a LAN multicast client interface:

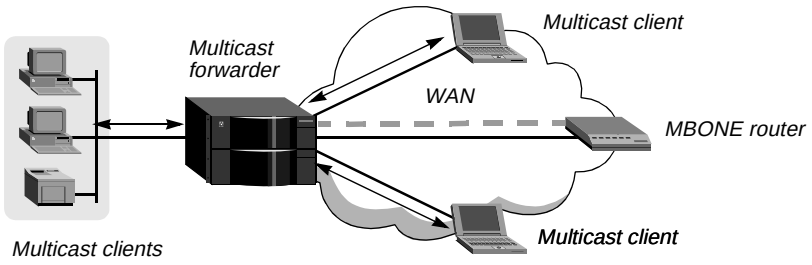


Figure 4-11. MAX TNT forwarding multicast traffic to LAN and WAN clients

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

To MBONE routers, the MAX TNT appears to be a multicast client, because it responds as a client to IGMP packets. To multicast clients, the MAX TNT 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	Enables/disables multicast forwarding in the MAX TNT. 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 and the MBONE-LAN-Interface parameter are mutually exclusive. For details, see "Configuring the MBONE interface" on page 4-61.
MBONE-LAN-Interface	Interface address (shelf, slot, and port) to MBONE router on a LAN interface. This and the MBONE-Profile parameter are mutually exclusive. For details, see "Configuring the MBONE interface" on page 4-61.
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 MAX TNT only counts packets received on this port.
Multicast-Hbeat-Slot-Time	Polling interval (in seconds) during which the MAX TNT 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 alarm-threshold.
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 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 MAX TNT 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 MAX TNT 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 MAX TNT 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, it 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 the MAX TNT 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	Enables/disables handling of IGMP requests and responses on the interface. The MAX TNT does *not* forward multicast traffic based on this setting.

Example of a local MBONE router

Figure 4-12 shows an MBONE router on one of the system's LAN IP interfaces:

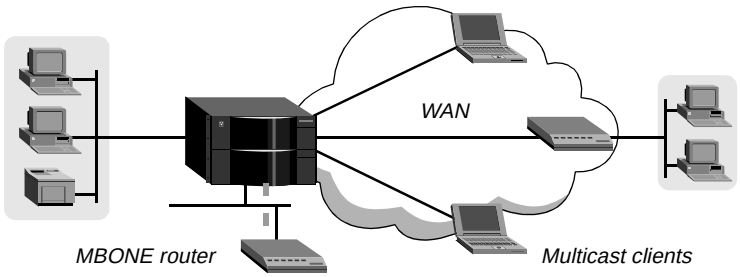


Figure 4-12. MBONE router on a LAN interface

The following commands configure the 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 c 1} 0}

admin> write
IP-GLOBAL written

admin> read ip-interface {{1 c 1}0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> set multicast-allowed = yes

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

Example of an MBONE router on a WAN interface

Figure 4-13 shows an MBONE router on a WAN interface:

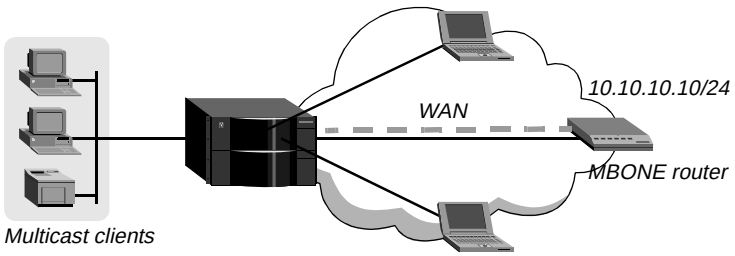


Figure 4-13. MBONE router on a WAN interface

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 MAX TNT 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 MAX TNT 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 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	Enables/disables handling of IGMP requests and responses on the interface.The MAX TNT does *not* forward multicast traffic based on this setting.
Multicast-Rate-Limit	Rate at which the MAX TNT 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 4-64.
Multicast-Group-Leave-Delay	Number of seconds the MAX TNT 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 4-64.

Settings in RADIUS profiles

The following attribute-value pairs can be specified in RADIUS profiles for WAN multicast client interfaces:

Attribute	Value
Ascend-Multicast-Client (155)	Enables/disables handling of IGMP requests and responses on the interface.The MAX TNT does *not* forward multicast traffic based on this setting.
Ascend-Multicast-Rate-Limit (152)	Rate at which the MAX TNT 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 4-64.
Ascend-Multicast-GRP-Leave-Delay(111)	Number of seconds the MAX TNT 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 4-64.

Setting the multicast rate limit

Multicast-Rate-Limit specifies the rate at which the MAX TNT accepts multicast packets from clients on the interface.

Note: By default, Multicast-Rate-Limit is set to 100. This 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 MAX TNT accepts one packet every five seconds from multicast clients on the interface . Any subsequent packets received within that 5-second window are discarded.

For high-bandwidth data, voice, and audio multicast applications, the MAX TNT supports both multicast rate limiting (described immediately above) and prioritized packet dropping. If the MAX TNT 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 MAX TNT 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 MAX TNT 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 MAX TNT forwards the Leave Group messages immediately.

If you set Multicast-Group-Leave-Delay to a nonzero value, the MAX TNT does not immediate 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 MAX TNT receives a response before the specified Multicast-Group-Leave-Delay interval, it does not forward the Leave Group message. Otherwise, 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 between 10 and 20.

Example of configuring a LAN multicast client interface

Figure 4-14 shows multicast clients on a LAN interface:

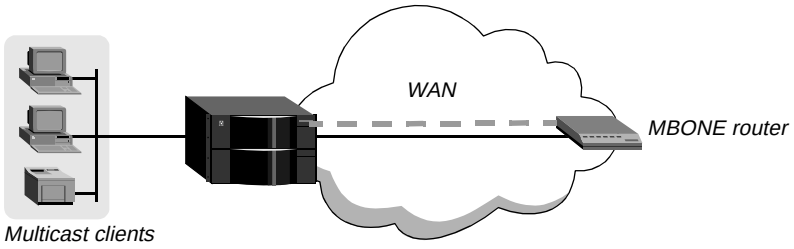


Figure 4-14. LAN multicast client interface

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
```

Examples of configuring WAN multicast client interfaces

Figure 4-15 shows multicast clients on WAN interfaces:

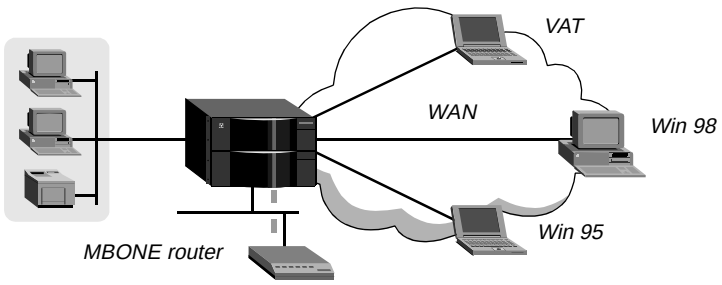


Figure 4-15. WAN multicast client interfaces

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"
    User-Service = Framed-User,
    Ascend-Multicast-Client = Multicast-Yes,
    Ascend-Multicast-GRP-Leave-Delay = 20,
    Ascend-Multicast-Rate-Limit = 5

w98-1 Password = "w98-1pw"
    User-Service = Framed-User,
    Ascend-Multicast-Client = Multicast-Yes,
    Ascend-Multicast-GRP-Leave-Delay = 20,
    Ascend-Multicast-Rate-Limit = 5

w95-1 Password = "w95-1pw"
    User-Service = Framed-User,
    Ascend-Multicast-Client = Multicast-Yes,
    Ascend-Multicast-GRP-Leave-Delay = 20,
    Ascend-Multicast-Rate-Limit = 5
```

Configuring virtual routers

A Virtual Router (also called a *VRouter*) is a grouping of interfaces in the MAX TNT system. Each Virtual Router has its own associated routing table, ARP table, route cache, and address pools, and maintains its own routing and packet statistics.

If you don't configure any VRouters, the MAX TNT router operates exactly as it has in previous releases. 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 4-16 shows a MAX TNT with one VRouter operating for Corporation A. Interfaces related to Corporation A are grouped and handled by one VRouter, creating a Virtual Private Network for Corporation A. Corporation A's WAN interfaces can dial-in to a local MAX TNT, which may be on a public network, to reach Corporation A's private LANs.

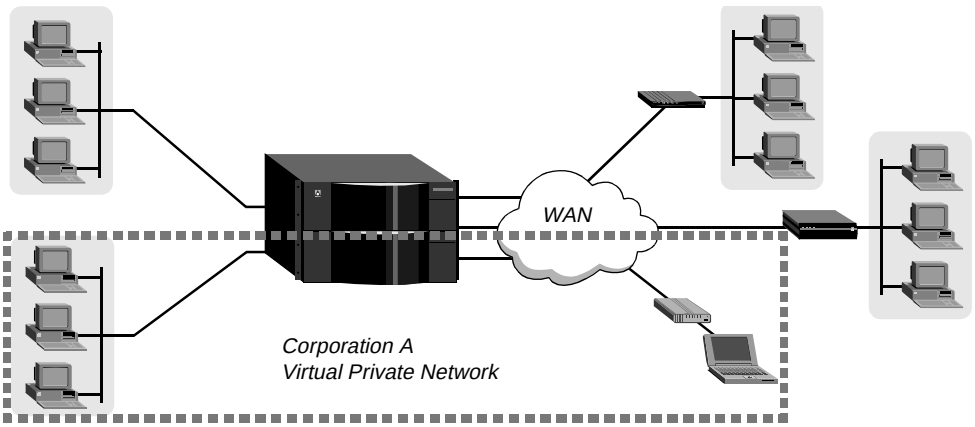


Figure 4-16. Virtual IP routing

How VRouters affect the routing table

Before the introduction of VRouters, the MAX TNT maintained a single IP routing table that enabled the router to reach any of its many interfaces. In that context, each interface known to the system required a unique address.

With VRouters, addresses must be unique within the VRouter's routing domain, but not necessarily within the MAX TNT system. 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 now 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]`

Command	Usage with optional VRouter arguments
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 <nqueries>] [-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 limitations

Currently, SNMP management does not present the view of the MAX TNT on per-VRouter basis. Errors and events are not logged on per-VRouter basis. The Syslog host defined in the system's Log profile must be accessible to the main VRouter.

Currently, ATMP presents incoming packets only to the main VRouter. In addition, servers defined in the following profiles must be accessible to the main VRouter:

- Debug
- SNTP
- Trap
- External-Auth

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 +
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 for 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 4-35.)
Summarize-RIP-Routes	If the VRouter is running RIP-v1, the Summarize-RIP-Routes parameter specifies whether to summarize subnet information when advertising routes. 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	Enables/disables RIP triggering. If set to Yes (the default), RIP updates include only changed routes. (For details, see "RIP triggering" on page 4-36.)

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 0.0.0.0+
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 +
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
```

Viewing the VRouter's routing and interface tables

The new VRouter defined for Corporation A 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 130.200.200.100/32 130.200.200.100    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
```

The new VRouter has also started maintaining 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 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:

```
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-tnt01 Password = "ascend", User-Service = Dialout-Framed-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 4-51. 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

Following are the related parameters in local profiles, shown here with sample values:

```
[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 indicates the global VRouter.

Settings in RADIUS profiles

RADIUS uses the following attribute-value pair to support the concept of a VRouter:

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 indicates the global VRouter.

Examples of assigning VRouter membership to interfaces

The following commands group three WAN interfaces with the Corporation A 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"
    User-Service = Framed-User,
```

```
    Framed-Protocol = MPP,
    Framed-Address = 10.1.1.1,
    Framed-Netmask = 255.255.255.0,
    Ascend-Vrouter-Name = "corpa"

dialin-2 Password = "pwd2"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 11.1.1.1,
    Framed-Netmask = 255.255.255.0,
    Ascend-Vrouter-Name = "corpa"

dialin-3 Password = "pwd1"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 12.1.1.1,
    Framed-Netmask = 255.255.255.0,
    Ascend-Vrouter-Name = "corpa"
```

Viewing assigned interfaces in the VRouter's tables

The 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 130.200.200.100/32 130.200.200.100     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          130.200.200.100     0    0      0    0
wan31      1500 11.1.1.1          130.200.200.100     0    0      0    0
wan32      1500 12.1.1.1          130.200.200.100     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 parameters related to VRouters in IP-Route profiles, shown here with default values:

```
[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 Dest-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 accept a VRouter name in the following syntax:

"*dest-addr gateway-addr metric* [*private*] [*profile*] [*vrouter-name*]"

Examples of defining a route on a per-VRouter basis

Following is an example that defines 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.5.6.7/28 10.1.1.1 corpa"
```

Viewing the static route in the VRouter's table

The new static route is added to the Corporation A VRouter's routing table, as shown in the following sample output:

```
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 next 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "11.0.0.0/28 0.0.0.0 corpa"
```

Viewing the inter-VRouter route in the global table

In this case, the route is added to the global VRouter's routing table, not to the Corporation A VRouter. For example:

```
admin> netstat -rn
Destination      Gateway       IF        Flg   Pref Met    Use     Age
0.0.0.0/0       10.168.6.1     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    2347
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
130.100.100.10/32  -           sip0       C        0   0      0    2378
130.100.100.252/30 -           rj0        C        0   0      0    2378
100.168.6.0/24    100.168.6.221 wanabe     SG      60   1      0       4
101.168.6.0/24     -           ie0        C        0   0   2531    2378
101.168.6.234/32   -           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
```

Deleting a VRouter

Deleting a VRouter profile deletes the virtual router. For example:

```
admin> delete vrouter corpa
```

Note: If you delete a VRouter with active connections, a reset is recommended. 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.

OSPF Routing

5

Introduction to OSPF 5-1

Adding the MAX TNT to an OSPF network 5-9

Configuring route options 5-14

Configuring OSPF static route information 5-16

Introduction to OSPF

Open Shortest Path First (OSPF) is the 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 “The link-state routing algorithm” on page 5-7.)

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 5-4.)

Ascend implementation of OSPF

The primary goal of Ascend’s OSPF implementation is to allow the MAX TNT to communicate with other routers within a single Autonomous System (AS).

Limited border router capability

The MAX TNT acts as an OSPF internal router with limited border router capability. At this release, Ascend does not recommend an Area Border Router (ABR) configuration for the MAX TNT, so its LAN and WAN interfaces must all be in the same area and area-type.

The MAX TNT does not currently function as an IGP gateway, although it performs Autonomous System Boundary Router (ASBR) calculations for external routes (such as WAN links that do not support OSPF). The MAX TNT 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 MAX TNT supports null, simple, and MD5 cryptographic authentication. For details, see “Security” on page 5-3.

One active IP interface per port

The Ascend 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 the 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 *MAX TNT Reference Guide* or the *MAX TNT Administration Guide*.

OSPF features

This section provides a brief overview of OSPF routing to help you configure the MAX TNT properly. (For details about how OSPF works, see RFC 1583, *OSPF Version 2*.)

An Autonomous System (AS) is a group of OSPF routers exchanging information, typically under the control of one company. An AS can include a large number of networks, all of which are assigned the same AS number. All information exchanged within the AS 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 AS number may 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. This means that only trusted routers can participate in the AS'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 5-6.)

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 5-4.) 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, MAX TNT now supports the MD5 cryptographic authentication method for OSPF, making it compliant with RFC 2178. For details about MD5 encryption, see RFC 2178.

Support for variable length subnet masks

OSPF routers handle variable-length subnet masks (VLSM). Each route distributed by OSPF has a destination address and subnet mask, and two different subnets of the same IP network number 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, Ascend recommends that you 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.

Interior gateway protocol (IGP)

OSPF keeps all AS-internal routing information within the AS. All information exchanged within the AS is interior.

An AS boundary router (ASBR) is required for communication with other Autonomous Systems. ASBRs use an exterior gateway protocol (EGP), as shown in Figure 5-1. An EGP acts as a shuttle service between Autonomous Systems.

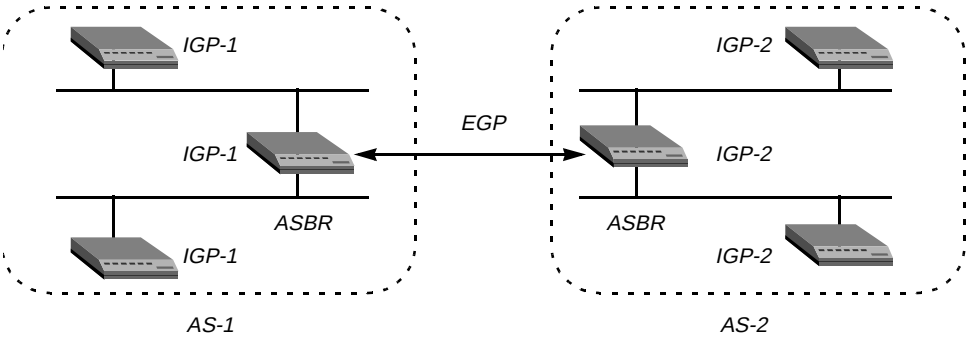


Figure 5-1. OSPF Autonomous System Boundary Routers (ASBRs)

ASBRs perform calculations related to external routes. The MAX TNT imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) and performs the ASBR calculations.

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 multi-access networks, all routers become adjacent to both the Designated Router and the Backup Designated Router.

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 results in quick convergence among routers. OSPF routes can also be summarized in Link-State Advertisements (LSAs).

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.

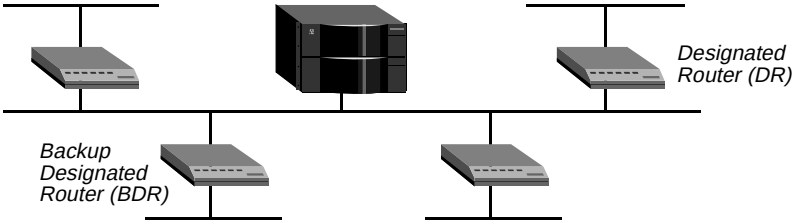


Figure 5-2. OSPF Designated Router (DR) and Backup Designated Router (BDR)

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 router, 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.

The administrator chooses the Designated Router on the basis of the processing power, speed, and memory of the system, then assigns priorities to other routers on the network in case the Backup Designated Router is also down at the same time.

Note: The MAX TNT can function as a Designated Router (DR) or Backup Designated Router (BDR). However, many sites choose to assign a LAN-based router for these roles in order to dedicate the MAX TNT to WAN processing.

Configurable cost metrics

The administrator assigns 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 5-3 shows how costs are used to direct traffic over high-speed links. For example, if Router-2 in Figure 5-3 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).

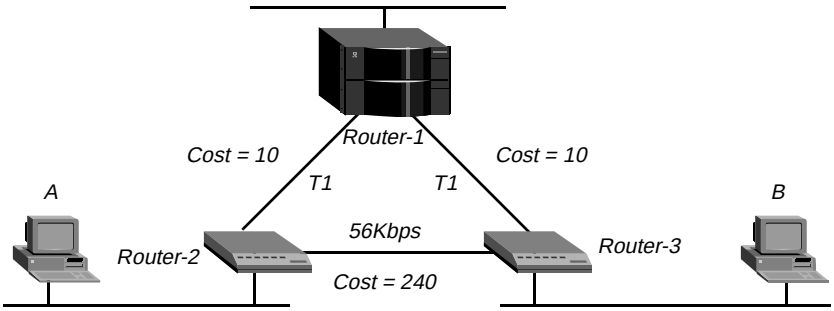


Figure 5-3. OSPF costs for different types of links

The MAX TNT 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 4, "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. An administrator 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 AS.

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 to one of the other areas. These routers are Area Border Routers (ABRs). In Figure 5-4, all of the routers are ABRs.

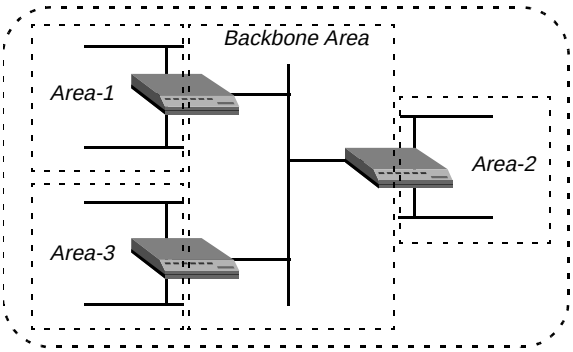


Figure 5-4. Dividing an OSPF Autonomous System (AS) into areas

Note: The MAX TNT does not currently operate as an ABR, so you must use the same area number for each OSPF interface. That area number does not have to be the default backbone area (0.0.0.0).

With the ABRs and area boundaries set up correctly, link-state databases are unique to an area. You can configure the MAX TNT to route in three kinds of area, which differ in their handling of external routes.

- Normal
- Stub
- Not So Stubby Area (NSSA)

Normal areas

AS External (ASE) routes are originated by ASBRs as Type-5 LSAs. 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.

Because the MAX TNT does not currently operate as an ABR, you should not configure it to route OSPF in a stub area if any of its links are ASE.

NSSAs

NSSAs are like stub areas in that they do not receive or originate Type-5 LSAs. However, stub areas do not allow any Type-5 LSAs into the area (they rely solely on default routing), while NSSAs 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 MAX TNT 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.

Note: For details about the NSSA specification, see RFC 1587.

The link-state routing algorithm

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 may be an AS or an area within an AS.

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 5-4). 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 5-5.

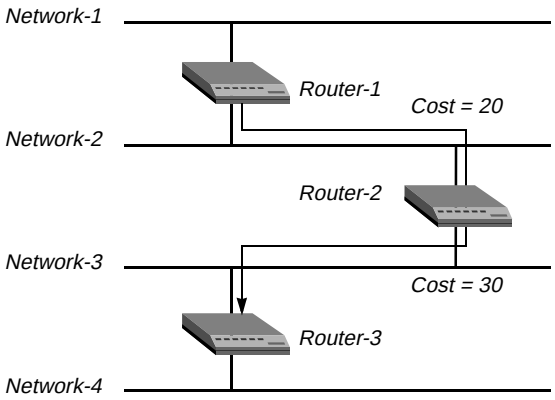


Figure 5-5. Sample OSPF topology

Table 5-1 shows the relevant information in the routers' link-state databases.

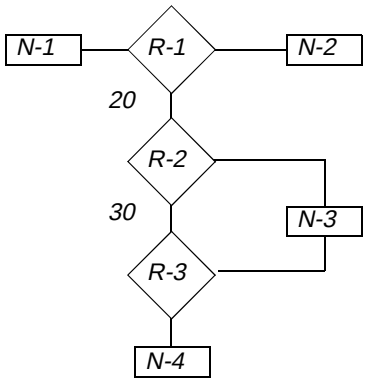
Table 5-1. Link state databases for OSPF topology in Figure 5-5

Router-1	**Router-2**	**Router-3**
Network-1/Cost 0	Network-2/Cost 0	Network-3/Cost 0
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 AS. (The table also includes externally derived routing information.)

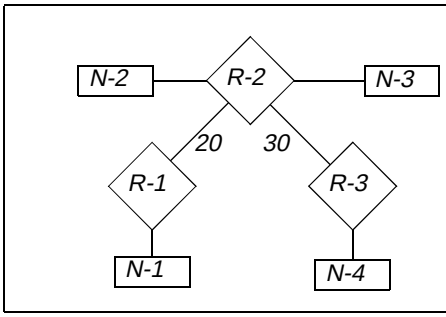
All of the routers calculate a routing table of shortest paths, based on the link-state database. Externally derived routing data is advertised throughout the AS but is kept separate from the link-state data. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

Table 5-2. Shortest-path tree and resulting routing table for Router-1



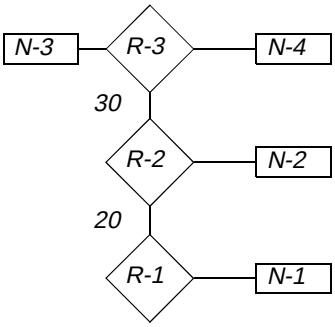
Destination	*Next Hop*	*Metric*
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-2	50

Table 5-3. Shortest-path tree and resulting routing table for Router-2



Destination	*Next Hop*	*Metric*
Network-1	Router-1	20
Network-2	Direct	0
Network-3	Direct	0
Network-4	Router-2	30

Table 5-4. 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 the MAX TNT to an OSPF network

Before it can run OSPF, the MAX TNT must be configured for IP routing, as described in Chapter 4, “IP Routing.”

System reset requirement

After enabling OSPF routing, you must reset the system. The system brings up OSPF routing on an interface only following a reset. As the system comes up with OSPF enabled on one or more interfaces, it begins forming adjacencies and building its routing table.

If you change the value of the Pool-OSPF-Adv-Type parameter in the IP-Global profile, you must reset the system for the change to take effect.

If you change the OSPF Area-Type from Normal to NSSA or vice versa, a system reset is required to recognize the change.

Overview of LAN and WAN OSPF settings

The same parameters appear in the OSPF subprofiles of the IP-Interface and Connection profiles (for configuring local and WAN interfaces, respectively). 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
key-id = 0
cost = 1
down-cost = 16777215
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5

[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
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
```

Parameter	Specifies
Active	Enables/disables 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 5-6.) **Note:** Because the MAX TNT does not operate as an area border router (ABR), all of its interfaces must be in the same area.
Area-Type	Type of area. The default is the Normal area type, in which external routes are advertised throughout the AS. **Note:** Because the MAX TNT does not operate as an area border router (ABR), all of its interfaces must specify the same area.
Hello-Interval	Number of seconds between Hello packets. (For information about how the router uses these packets, see “Exchange of routing information” on page 5-4.)
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 (as described in “Exchange of routing information” on page 5-4.)

Parameter	Specifies
Priority	Priority value, used to elect a DR and BDR. A setting of 1 or greater places the MAX TNT on the list of possible DRs. A setting of 0 excludes the MAX TNT from becoming a DR/BDR. The higher the priority value of the MAX TNT relative to other OSPF routers on the network, the better the chances that it will become a BDR/DR (as described in "Designated and Backup Designated Routers" on page 5-4.)
Authen-Type	Type of authentication to use for validating OSPF packet exchanges. If set to None, no authentication is required. If set to Simple (the default), the router validates OSPF packet exchanges using the password supplied in the Auth-Key parameter. If set to MD5, the router validates OSPF packet exchanges using MD5 encryption and the authentication Key ID supplied in the Key-ID parameter. (See "Security" on page 5-3 for related information.)
Auth-Key	Key (password) required for packets to access the router's area when Authen-Type is set to Simple.
Key-ID	Number from 0 to 255. If Authen-Type is set to MD5, the number is used to validate OSPF packet exchanges. Packets must contain the specified value in the OSPF header Key ID field to be allowed into the router's area.
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 5-5.)
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 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.

Example of configuring a LAN OSPF interface

Figure 5-6 shows three OSPF routers in the backbone area of an AS. 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 MAX-TNT-2 in Figure 5-6.

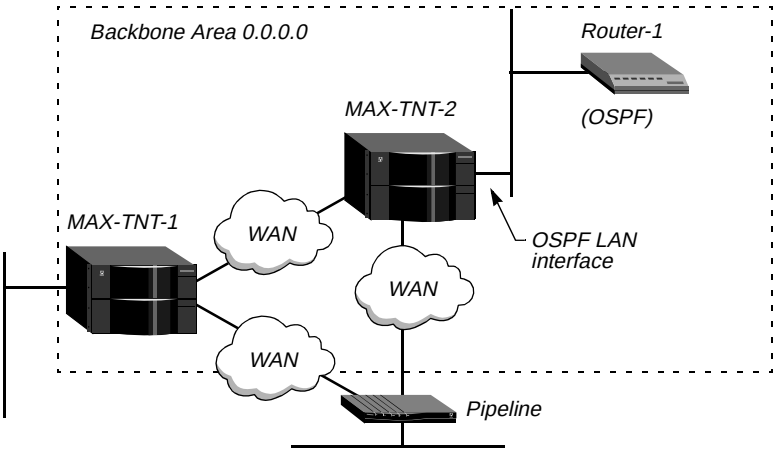


Figure 5-6. OSPF on a LAN interface

All OSPF routers in Figure 5-6 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 AS. 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 MAX TNT to that area. You could then assign the same area number (0.0.0.1) to all OSPF routers reached through the MAX TNT across a WAN link.

Following is an example that shows how to configure MAX-TNT-2 in Figure 5-6. The commands assign the IP address 10.168.8.17/24 on 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
```

Examples of configuring WAN OSPF interfaces

This example shows how to configure Connection profiles in the MAX TNT units shown in Figure 5-7, to enable them to route OSPF across the WAN that separates them. In this example, the unit labeled MAX-TNT-1 has the IP address 10.2.3.4/24, and the unit labeled MAX-TNT-2 has the address 10.168.8.17/24.

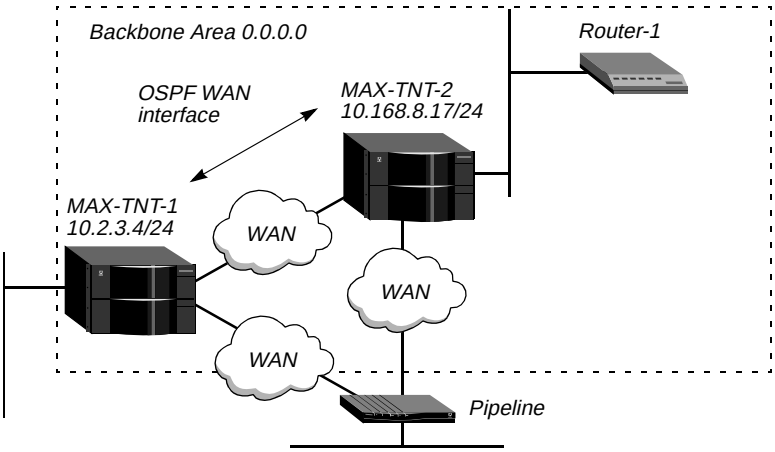


Figure 5-7. OSPF on a WAN interface

The WAN interfaces of the MAX TNT 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 MAX-TNT-1 in Figure 5-7:

```
admin> read conn maxtnt2ink
CONNECTION/maxtnt2link 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/maxtnt2link written
```

The following commands configure the OSPF WAN link in MAX-TNT-2 in Figure 5-7:

```
admin> read conn maxtnt1link
CONNECTION/maxtnt1link 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/maxtnt1link written
```

Example of integrating a RIP-v2 interface

In Figure 5-8, each MAX TNT 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, as well as any routes the MAX TNT learns about from the remote Pipeline, are ASE routes (external to the OSPF Autonomous System).

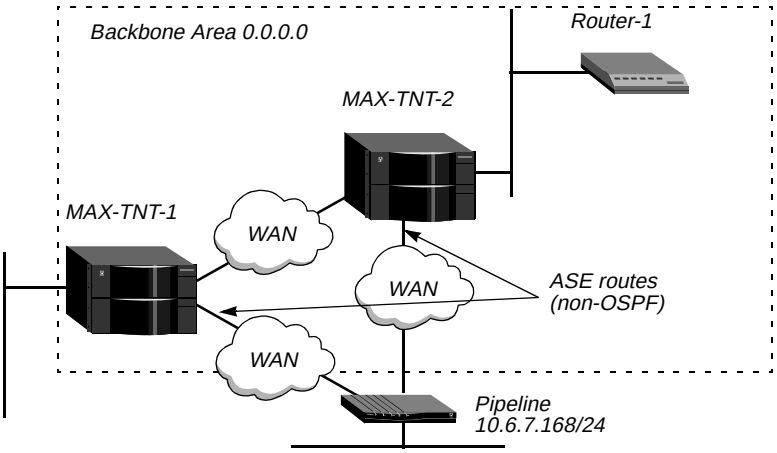


Figure 5-8. Including ASE routes in the OSPF environment

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 option 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 5-14.

However, in the following example, RIP is turned off on the link, so the MAX TNT 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 to tag it with the specified hexadecimal number. The cost assigned is appropriate for the bandwidth of a single B-channel connection (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 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	Enables/disables Autonomous System Boundary Router (ASBR) calculations related to external routes. Normally, when the MAX TNT 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 MAX TNT 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 “Examples of configuring summarized address pools” on page 4-55. 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 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 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 from the default of 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 5-5.
Third-Party	Enables/disables advertisement of routes to external destinations on behalf of another gateway (a third party). See “Example of specifying a third-party route” on page 5-18.
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 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 previous releases, 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 MAX TNT 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 5-6. To configure the MAX TNT to route OSPF in an NSSA, *all* OSPF interfaces in the MAX TNT must specify the NSSA Area-Type. The MAX TNT does not operate as an ABR, so the Area-Type as well as the area number must be the same on all interfaces running OSPF.

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 example shows how to configure the MAX TNT 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 Reset the system.

3 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
```

4 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 MAX TNT 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, the 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 is commonly known as advertising a forwarding address. If third-party routing is disabled, the MAX TNT advertises itself as the forwarding address to an external destination. When third-party routing is enabled, the MAX TNT 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. This usually means that the forwarding address is on a local network that has an OSPF router acting as the forwarding router, or that a Designated Router is sending LSAs for that Ethernet 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 MAX TNT 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
```

Ascend Tunnel Management Protocol 6

Introduction to ATMP 6-1
Network settings for ATMP 6-2
Configuring a Foreign Agent 6-7
Configuring Home Agents 6-16
Configuring a Home-and-Foreign-Agent. 6-25
Configuring IPX over ATMP 6-29

The MAX TNT supports Ascend Tunnel Management Protocol (ATMP) for Virtual Private Network (VPN) connectivity. For information about using other tunneling protocols for VPN connectivity, see Chapter 7, "L2TP, PPTP, and IP-in-IP Tunneling."

Introduction to ATMP

ATMP is a UDP/IP-based protocol for tunneling between two Ascend 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 6-1 shows one use for ATMP tunneling: mobile clients dial into a local ISP to log into a distant LAN across the Internet. ATMP creates and tears down a cross-Internet tunnel between the two Ascend units. In effect, the tunnel collapses the IP cloud and provides what looks like direct access to a home network.

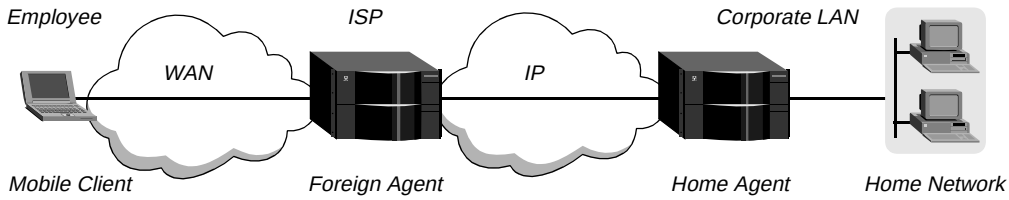


Figure 6-1. ATMP tunnel from an ISP to a corporate home network

A mobile client dials into 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 a 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 6-16.

Network settings for ATMP

Network settings for ATMP include settings related to the IP connection between Ascend 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

Ascend recommends that you set the System-IP-Addr parameter in a MAX TNT 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, the Connection profile for mobile clients should specify the System-IP-Addr of a Home Agent rather than the interface address on which the Home Agent accepts tunneled data. This 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-Addr. This 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 6-2 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.)

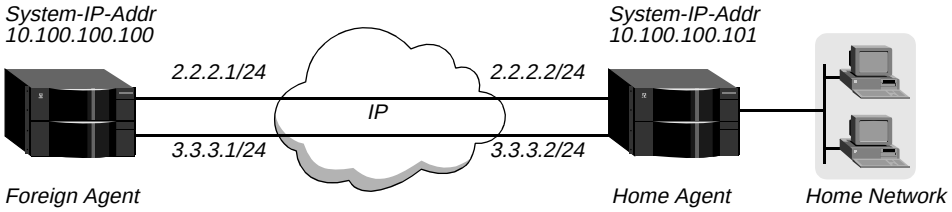


Figure 6-2. System IP addresses and routes between ATMP agents

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
```

and 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 requests 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 may be a switched dial-out connection, a Frame Relay connection, or an Ethernet link, and it may 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 6-1 shows an ATMP setup across a 100-BaseT Ethernet segment, which limits the path MTU to 1500 bytes.

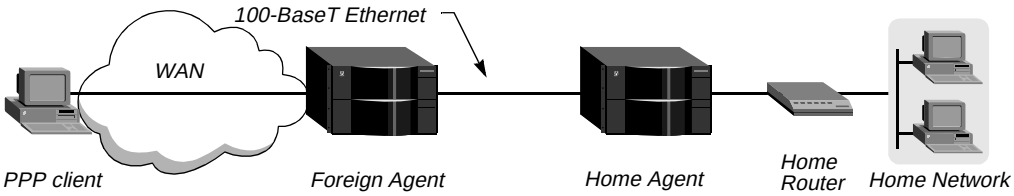


Figure 6-3. Path MTU on an Ethernet segment

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 then 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 MAX TNT 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 MAX TNT 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 MAX TNT 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 MAX TNT 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 on the ATMP agents.

For example, if the MAX TNT 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 full-size packets that include the 8-byte GRE header and a 20-byte IP header without fragmenting the packets first:

```
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 MAX TNT 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 MAX TNT to interoperate with these clients, you can configure the MAX TNT to ignore the DF bit and perform the fragmentation that normally should be performed by the client software. This function in the MAX TNT is sometimes 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 MAX TNT 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 MAX TNT 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.

Network isolation and duplicate IP addresses

A Foreign Agent will accept multiple ATMP connections using the same IP address as long as they request a different Home Agent or different home network names. This feature allows the use of unregistered IP addresses on multiple independent private networks.

Multiple connections using the same IP address is possible because ATMP provides full network isolation between different home networks. Mobile clients are allowed to reach only the home network where they are registered. They are not permitted to reach the IP network between the Foreign Agent and the Home Agent or any other home network. This 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.

For example, Figure 6-1 shows two mobile clients, one registered with Corporation A's home network and one with Corporation B's home network. Neither of the mobile clients is able to access the IP network between the Foreign Agent and the Home Agent or the other home network.

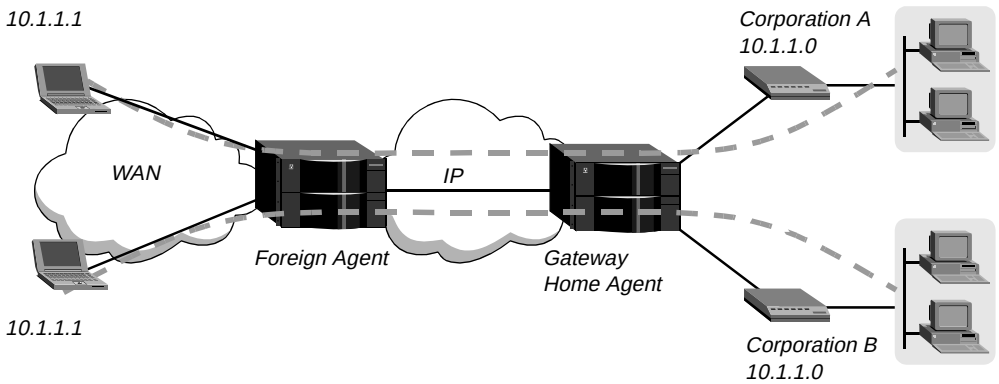


Table 6-1. Foreign Agent supporting duplicate IP addresses

To provide network isolation, the 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.

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 may be 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. The Home Agent uses this 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 4, “IP Routing.”

If the system uses RADIUS for authentication or accounting (or both), see the *MAX TNT RADIUS Guide* for details about installing and configuring a basic RADIUS setup.

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 endpoints 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 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 6-7.

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 6-4.)
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 6-4).
Force-Fragmentation	If outdated client software sends large packets with the DF bit set, you can set this parameter to force the MAX TNT to fragment the packets anyway (as described in “Forcing fragmentation for interoperation with outdated clients” on page 6-5).

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-Addr or hostname of a Home Agent.
Secondary-Tunnel-Server	Specifies the System-IP-Addr 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 set 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 set in the ATMP profile of the Home Agent, if any (up to 21 characters).

Parameter	Usage for mobile client configuration
Home-Network-Name	If the Home Agent is operating in gateway mode, must specify the name of the gateway profile to the home network.

Settings in RADIUS profiles

RADIUS uses following attribute-value pairs to specify mobile client connections:

Attribute	Value
Tunnel-Type (64)	Type of protocol used for the tunnel. To ensure forward compatibility, the Ascend-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)	The System-IP-Addr or hostname of a Home Agent. The string may 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)	The System-IP-Addr 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)	A UDP port set 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)	The password set 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-21.
Tunnel-Private-Group-ID (81)	If the Home Agent is operating in gateway mode, you must specify the name of the gateway profile to the home network using this attribute or the Ascend vendor-specific Ascend-Home-Network-Name (185).

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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.1.1.1,
    Framed-Netmask = 255.255.255.255,
    Tunnel-Type = ATMP,
    Tunnel-Server-Endpoint = "atmp-ha1.example.com",
    Tunnel-Password = "tunnel-password"

user1 Password = "pass1"
    User-Service = Framed-User,
```

```
    Framed-Protocol = PPP,
    Framed-Address = 10.1.1.1,
    Framed-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 command to the IP address of the primary Home Agent. (If the Home Agent is specified as a hostname, the Foreign Agent performs a DNS lookup first.) Depending on the network configuration, the Foreign Agent may 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"
    User-Service = Framed-User,
    Framed-Address = 10.1.1.1,
    Framed-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:

```
admin> set primary-tunnel-server = 2.2.2.2
```

```
admin> set secondary-tunnel-server = ha2.company.com:6789
admin> set udp-port = 8877
```

the Foreign Agent dials the connection to the Primary-Tunnel-Server and requests a tunnel on port 8877. If that attempt fails, it 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 6-16. 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, for 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
```

The mobile client's profile would specify the following home network name:

```
admin> set home-network-name = homenet
```

Or 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 leave the Home-Network parameter blank, or omit the Tunnel-Private-Group-ID or Ascend-Home-Network-Name attributes, in mobile-client profiles.

Example of a Foreign Agent configuration

Figure 6-4 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.

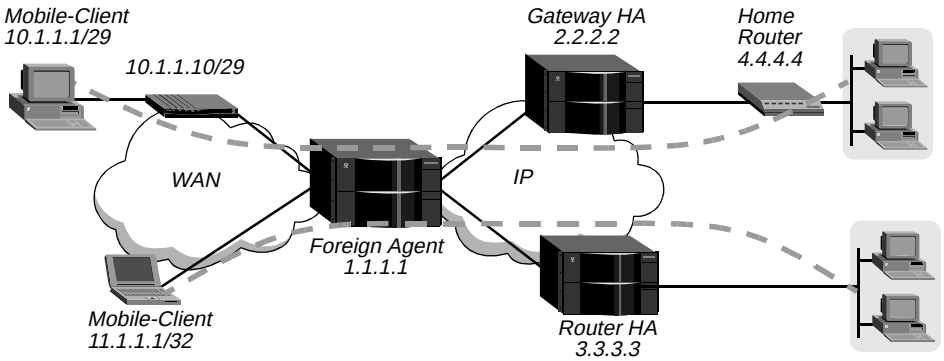


Figure 6-4. Foreign Agent tunneling to two Home Agents

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 6-4.

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 next 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "2.0.0.0 2.2.2.2 1 n hagateway-out"

hagateway-out Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "hagateway",
    Framed-Protocol = MPP,
    Ascend-Route-IP = Route-IP-Yes,
    Framed-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 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-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "3.0.0.0 3.3.3.3 1 n harouter-out"

harouter-out Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "harouter",
    Framed-Protocol = MPP,
    Ascend-Route-IP = Route-IP-Yes,
    Framed-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 next commands configure a mobile client connection on the Foreign Agent 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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-IP-Route = Route-IP-Yes,
    Framed-Address = 10.1.1.1,
    Framed-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 commands configure a mobile client connection on the Foreign Agent 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", User-Service= Framed-User
    Framed-Protocol = MPP,
    Ascend-IP-Route = Route-IP-Yes,
    Framed-Address = 11.1.1.1,
    Framed-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 the MAX TNT is operating as a Foreign Agent tunneling to a GRF switch Home Agent, setting the MTU-Limit becomes a requirement rather than a recommendation. To maintain its very high throughput, the GRF does not perform packet reassembly. If MTU-Limit is not specified and a mobile client sends a large packet, the Foreign Agent may be forced to fragment it before sending it to the Home Agent. The GRF switch Home Agent drops such packets.

Figure 6-5 shows a Foreign Agent tunneling to a GRF Home Agent across a 100-BaseT Ethernet segment:

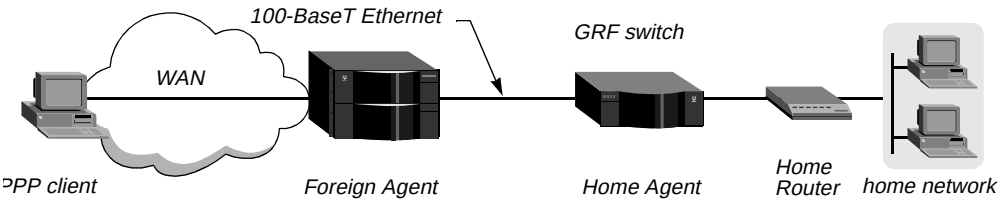


Figure 6-5. Foreign Agent tunneling to a GRF switch

The following commands configure the Foreign Agent ATMP profile for the MAX TNT in Figure 6-5:

```
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 should specify the same MTU-Limit.

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 6-7.

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	Specify 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 6-3.
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 6-4.
Idle-Timer	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.

Parameter	Usage for Home Agent configuration
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 6-4.
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 6-5.

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 6-6:

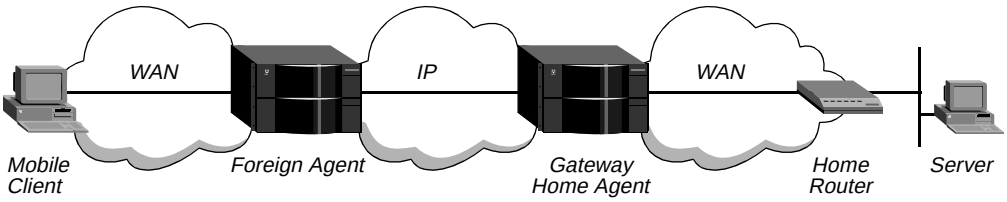


Figure 6-6. How a Gateway Home Agent works

The link to the home network cannot be a regular switched dial-out connection, because the Home Agent will not dial the connection on 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 6-19.

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.

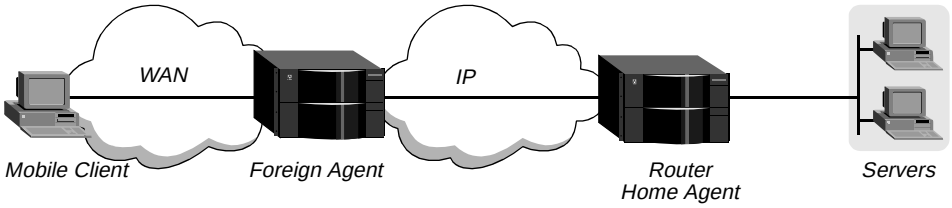


Figure 6-7. How a Router Home Agent works

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, it adds 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-21.

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 hold 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 y 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 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 AM and disconnect at 5:00 PM, 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 specified in 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 Gateway-Profile. The parameter operates independently of the RIP parameter in the IP-Options subprofile. For gateway profiles, the IP-Options RIP parameter should 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 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, where a secondary Home Agent can take over for a primary Home Agent when the primary agent becomes unavailable.

Informing the home router about routes to mobile clients

The router at the far end of 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, the next hop = 0.0.0.0, metric = 1. RIP-v2 authentication and route tags are not supported.

The following commands enable ATMP-HA-RIP in the gateway profile 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, like 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, where 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 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 encompass 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. In some cases, the two Home Agents connect to two home routers, as shown in Figure 6-8, or the Home Agents might connect to the same home router.

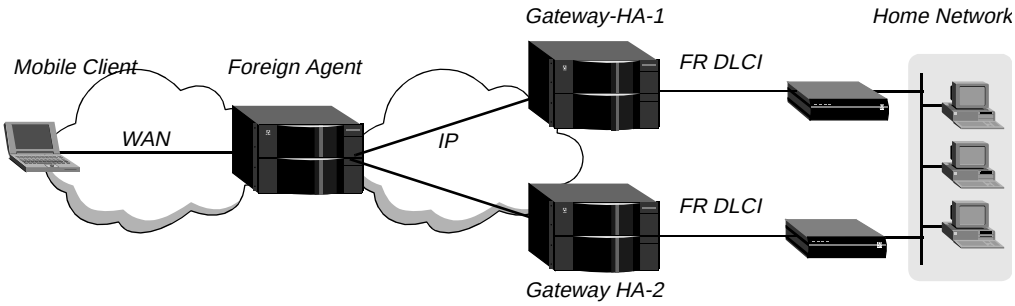


Figure 6-8. Resilient ATMP installation

Mobile clients access the home network through one of the Home Agents, but not always the same Home Agent. In this case, 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 6-8:

```
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 6-9 shows a Gateway Home Agent with a fractional T1 connection to the home network. For details about fractional T1, see the *MAX TNT Hardware Installation Guide*.

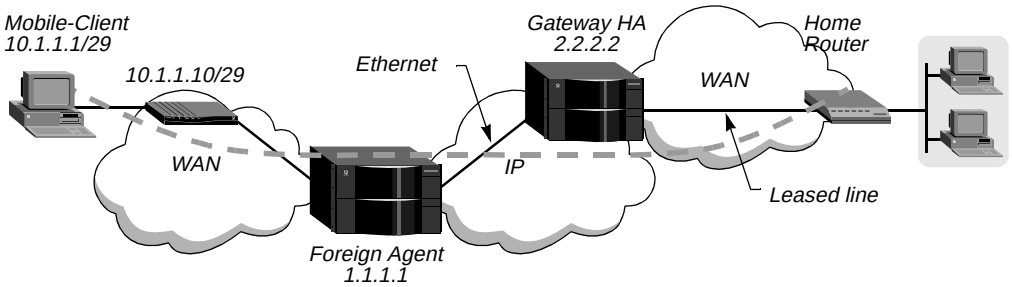


Figure 6-9. Gateway Home Agent with leased line to home network

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 next 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"
    User-Service = 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 6-10 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.

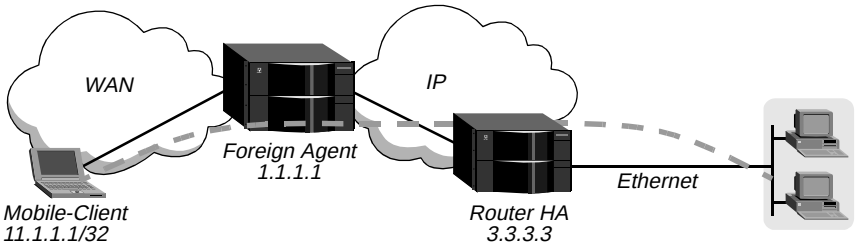


Figure 6-10. Router Home Agent on the home network

For information about configuring a connection to the Foreign Agent, see “Configuring the agent-to-agent connection” on page 6-7.

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 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 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 = 3.3.3.3
password = tunnel-password
```

Or comparable tunnel settings in a RADIUS profile:

```
mclient Password = "local-password"
    User-Service = 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, the MAX TNT 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 related to the Home-and-Foreign-Agent configuration, shown with sample values:

```
[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 6-16 or “Configuring a Foreign Agent” on page 6-7.

Example of a Home-and-Foreign-Agent configuration

Figure 6-11 shows a MAX TNT operating as Home Agent for home network B and as Foreign Agent for mobile clients tunneling into home network A:

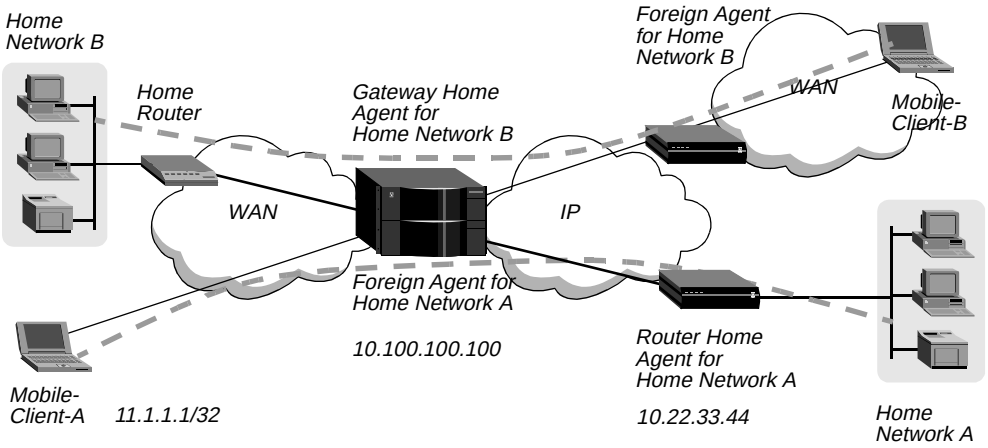


Figure 6-11. MAX TNT acting as both Home Agent and Foreign Agent

For information about configuring connections between Home Agents and Foreign Agents, see "Configuring the agent-to-agent connection" on page 6-7.

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 next commands configure 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 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 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 next commands configure a Connection profile for Mobile-Client-A in Figure 6-11. For this profile, the MAX TNT 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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-IP-Route = Route-IP-Yes,
    Framed-Address = 11.1.1.1,
    Framed-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 6-12 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 TNT-2 as their Home Agent. The two ATMP units are geographically distant.

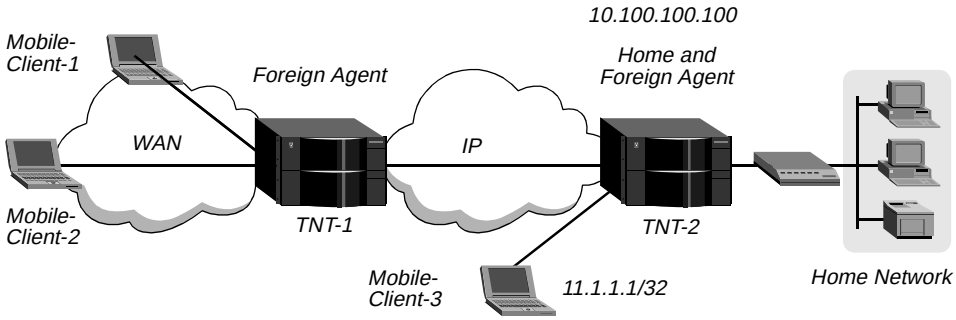


Figure 6-12. Enabling a mobile client to bypass the Foreign Agent connection

Mobile-Client-1 and Mobile-Client-2 make local calls to dial into the Foreign Agent (TNT-1) and then tunnel to the Home Agent. However, Mobile-Client-3 is geographically closer to TNT-2, and would prefer to dial directly into TNT-2. In this case, TNT-2 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 TNT-2'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 TNT-2:

```
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.

TNT-1 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 commands configure a Connection profile for Mobile-Client-3 in Figure 6-12. For this profile, the MAX TNT 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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-IP-Route = Route-IP-Yes,
    Framed-Address = 11.1.1.1,
    Framed-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. 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 6-13:

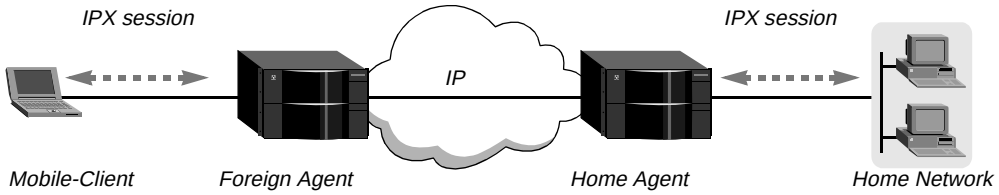


Figure 6-13. IPX routing connections for IPX ATMP

For details about configuring IPX, see Chapter 8, "IPX Routing."

For information about configuring connections between Home Agents and Foreign Agents, see "Configuring the agent-to-agent connection" on page 6-7.

Configuring the agents for IPX routing

For details about configuring the MAX TNT to route IPX, see Chapter 8, "IPX Routing." The next commands configure a minimal IPX configuration to enable the MAX TNT 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 the preceding section), 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, 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).

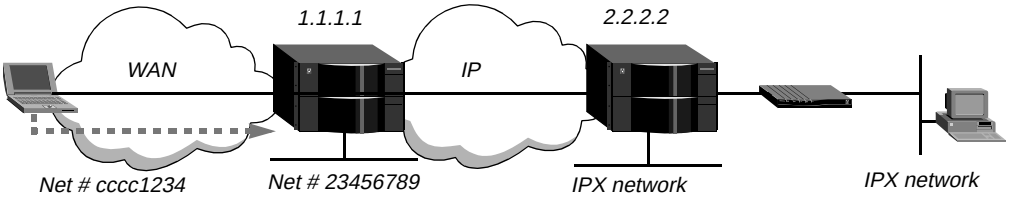


Figure 6-14. IPX ATMP with a Gateway Home Agent

The Gateway Home Agent communicates with an Ascend Pipeline unit configured for IPX routing (the home router). After the configurations described in the next sections have been set up, the mobile client can dial into the Foreign Agent and once connected, click on the NetworkNeighborhood icon to see the destination NetWare server and its contents.

Configuring a mobile client IPX connection

The next set commands configures a Connection profile for the mobile client in Figure 6-14:

```
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"
    User-Service = 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 6-30).

The next commands configure a Connection profile to the home router. Note that IPX RIP and 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 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 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 # field specifies the number of the Pipeline unit’s IPX-routing Connection profile 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 6-7), you must configure the IPX connections between the mobile client and Foreign Agent, and between the Home Agent and home network.

In this example, 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).

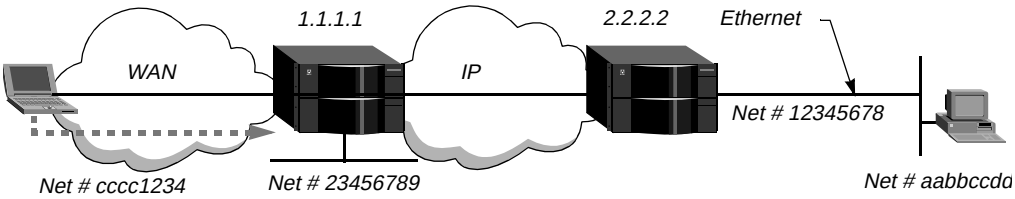


Figure 6-15. IPX ATMP with a Router Home Agent

After the configurations described in the next sections have been set up, the mobile client can dial into the Foreign Agent and once connected, click on the NetworkNeighborhood icon to see the destination NetWare server and its contents.

Configuring a mobile client IPX connection

The next set commands configures a Connection profile for the mobile client in Figure 6-15:

```
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> write
CONNECTION/mobile-client-1 written
```

Following is a comparable RADIUS profile:

```
mobile-client-1 Password = "mc-password"
    User-Service = 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 next 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, PPTP, and IP-in-IP Tunneling 7

Layer 2 Tunneling Protocol (L2TP). 7-1

Point-to-Point Tunneling Protocol (PPTP). 7-6

IP-in-IP encapsulation 7-11

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) provides tunneling at OSI layer 2 (at the HDLC layer of a PPP connection). The MAX TNT currently operates as an L2TP Access Concentrator (LAC) only, which means that it receives incoming PPP calls and initiates a connection to an L2TP Network Server (LNS).

Components of an L2TP tunnel

Figure 7-1 shows the elements of an L2TP tunnel. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within PPP. The MAX TNT answers the call and passes it to the LNS. LAC-to-LNS communication requires IP connectivity.

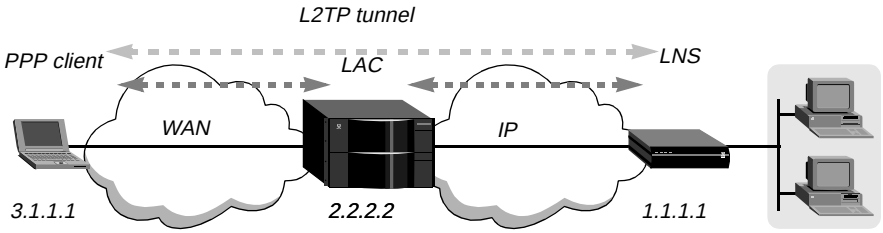


Figure 7-1. L2TP tunneling

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 LAC and the LNS can be a switched or nailed connection, or 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 use UDP port 1701 and are encapsulated in UDP.

The control link carries information used 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 doesn't 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 L2TP operations

Following are the global L2TP parameters (shown with default values):

```
[in L2-TUNNEL-GLOBAL]
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0

[in TUNNEL-SERVER/""]
server-endpoint* = ""
enabled = yes
shared-secret = ""
```

Parameter	Specifies
L2TP-Mode	Enables/disables L2TP operations. Specify LAC to enable L2TP operations in the MAX TNT.
L2TP-Auth-Enabled	Enables/disables L2TP tunnel authentication. If set to Yes, the MAX TNT authenticates the LNS with a Shared-Secret before bringing up an L2TP control channel .
L2TP-Rx-Window	Advertised L2TP receive window size for data channels. The default zero indicates that the MAX TNT will ask for no flow control for inbound L2TP payloads.
Server-Endpoint	DNS hostname or dotted IP address of the LNS endpoint. If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.
Enabled	Enables/disables tunnels to the specified Server-Endpoint.
Shared-Secret	Shared secret for authenticating L2TP tunnels. For details, see "Tunnel authentication" on page A-21.

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 = 1024
admin> write
L2-TUNNEL-GLOBAL written
admin> read tunnel-server l2tp-1
TUNNEL-SERVER/l2tp-1 read
admin> set enabled = yes
admin> set shared-secret = secret1
```

```
admin> write
TUNNEL-SERVER/l2tp-1 read
```

Configuring a connection to the LNS

If the LNS is on a remote IP network, the MAX TNT requires an IP-routed Connection profile or RADIUS profile to the LNS. For example:

```
admin> read conn l2tp-1
CONNECTION/l2tp-1 read

admin> set active = yes

admin> set dial-number = 9-1-333-555-1212

admin> set ppp send-password = lns-pw

admin> set ppp recv-password = lac-pw

admin> set ip-options remote = 1.1.1.1

admin> write
CONNECTION/l2tp-1 written
```

Following are comparable RADIUS profiles:

```
l2tp-1 Password = "lac-pw"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1

route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "1.0.0.0 1.1.1.1 1 n l2tp-1-out"

l2tp-1-out Password = "lac-pw" User-Service = Dialout-Framed-User
    User-Name = "l2tp-1",
    Ascend-Dial-Number = "9-1-333-555-1212",
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1,
    Ascend-Send-Secret = "lns-pw"
```

For details about configuring IP WAN interfaces, see Chapter 4, “IP Routing.”

Configuring L2TP mobile client profiles

If a PPP client’s profile is configured to initiate an L2TP tunnel, the MAX TNT attempts to open a tunnel following initial authentication of the connection. It can open a tunnel after pre-authenticating the call (using CLID or DNIS authentication) or after authenticating the caller’s name and password.

If the LAC opens a tunnel after pre-authenticating the call, the LNS performs all PPP negotiations and terminates 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: Due to tunneling protocol requirements, the LNS can only authenticate a tunneled call by using a PPP authentication protocol. The LNS cannot use other authentication methods (such as CLID, DNIS, or terminal server authentication) for tunneled calls. For the system to

pre-authenticate a call using CLID or DNIS, the telco switch must send the information as part of the call, and the MAX TNT must be configured to extract and use the information.

For details about pre-authentication and password authentication, see Appendix A, "Authentication Methods."

L2TP settings in Connection profiles

Following are the L2TP tunnel parameters (shown with sample values) in a Connection profile:

```
[in CONNECTION/tunnelcx:tunnel-options]
profile-type = mobile-client
tunneling-protocol = l2tp-protocol
primary-tunnel-server = l2tp-1
```

Parameter	Specifies
Profile-Type	Type of tunnel profile. Specify Mobile-Client for L2TP tunneling.
Tunneling-Protocol	Protocol to use when creating a tunnel for this profile. Set to L2TP to pass traffic to an LNS.
Primary-Tunnel-Server	DNS hostname or dotted IP address of the LNS endpoint. If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.

L2TP settings in RADIUS profiles

RADIUS uses the following attribute-value pairs to specify L2TP tunnels:

Attribute	Value
Tunnel-Type (64)	Tunneling protocol to be used. Set to L2TP (3) for L2TP tunneling.
Tunnel-Medium-Type (65)	Media to be used for the tunnel. Only IP (1) is supported at this time.
Tunnel-Server-Endpoint (66)	DNS hostname or dotted IP address of the LNS endpoint (a string value). If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.
Tunnel-Password (69)	Shared secret for authenticating L2TP tunnels. For details, see "Tunnel authentication" on page A-21.

Examples of opening a tunnel after pre-authenticating the call

To enable the MAX TNT to pre-authenticate 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 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-sever = 1.1.1.1
admin> write
CONNECTION/l2test written
```

Following is a comparable RADIUS profile:

```
5551000 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    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-sever = l2tp-1.example.com
admin> write
CONNECTION/tunnelcx
```

Following is a comparable RADIUS profile:

```
8001234567 Password = "Ascend-DNIS", User-Service=Dialout-Framed-User
    Tunnel-Server-Endpoint = "l2tp-1.example.com",
    Tunnel-Type = L2TP,
    Tunnel-Medium-Type = IP
```

Examples of opening a tunnel after password authentication

In this example, the MAX TNT 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 MAX TNT 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 ip remote-address = 3.1.1.1
```

```
admin> set ppp recv-password = localpw
admin> set tunnel profile-type = mobile-client
admin> set tunnel primary-tunnel-sever = 1.1.1.1
admin> set tunnel tunneling-protocol = l2tp
admin> write
CONNECTION/l2test written
```

Following is a comparable RADIUS profile:

```
l2test Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 3.1.1.1,
    Tunnel-Server-Endpoint = "1.1.1.1",
    Tunnel-Type = L2TP,
    Tunnel-Medium-Type = IP
```

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 MAX TNT as if the connection were directly terminated at the server.

The MAX TNT operates as a PPTP Access Concentrator (PAC) only, which means that it receives incoming PPP calls and initiates a connection to the NT server configured as a PPTP Network Server (PNS).

Components of a PPTP tunnel

Figure 7-2 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 MAX TNT answers the call and passes it to the PNS. PAC-to-PNS communication requires an IP connection.

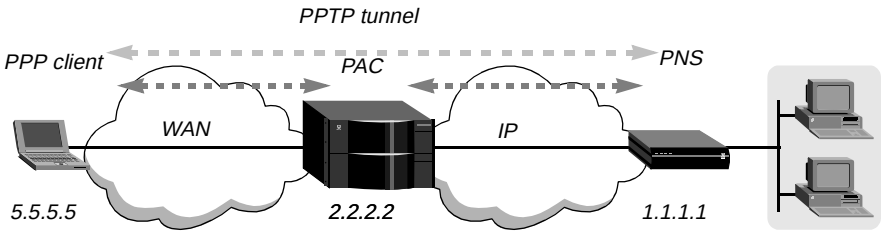


Figure 7-2. PPTP tunneling

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 an Ethernet link. The 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 used 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 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 doesn't 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

[in TUNNEL-SERVER/""]
server-endpoint* = ""
enabled = yes
```

Parameter	Specifies
PPTP-Enabled	Enables/disables PPTP operations.
Server-Profile-Required	Enables/disables a requirement for a configured Tunnel-Server profile to the PNS. If set to Yes, PPTP requires a Tunnel-Server profile that matches the PNS specification in a Connection before it creates a tunnel to the server. If set to 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.
Server-Endpoint	DNS hostname or dotted IP address of the PNS endpoint. If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.
Enabled	Enables/disables tunnels to the specified Server-Endpoint.

The following commands configure the MAX TNT 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 a connection to the PNS

If the PNS is on a remote IP network, the MAX TNT requires an IP-routing Connection profile or RADIUS profile to the PNS, such as the following sample profile:

```
admin> read conn pptp-1
CONNECTION/pptp-1 read

admin> set active = yes

admin> set dial-number = 9-1-222-555-1212

admin> set ppp send-password = pns-pw

admin> set ppp recv-password = pac-pw

admin> set ip-options remote = 1.1.1.1

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

Following are comparable RADIUS profiles:

```
pptp-1 Password = "pac-pw"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1

route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "1.0.0.0 1.1.1.1 1 n pptp-1-out"

pptp-1-out Password = "pac-pw" User-Service = Dialout-Framed-User
    User-Name = "pptp-1",
    Ascend-Dial-Number = "9-1-222-555-1212",
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1,
    Ascend-Send-Secret = "pns-pw"
```

For details about configuring IP WAN interfaces, see Chapter 4, “IP Routing.”

Configuring PPTP mobile client profiles

If a PPP client’s profile is configured to initiate a PPTP tunnel, the MAX TNT attempts to open a tunnel following initial authentication of the connection. It can open a tunnel after pre-authenticating the call (using CLID or DNIS authentication) or after authenticating the caller’s name and password.

If the PAC opens a tunnel after pre-authenticating 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: Due to tunneling protocol requirements, the PNS can only authenticate a tunneled call by using a PPP authentication protocol. The PNS cannot use other authentication methods (such as CLID, DNIS, or terminal server authentication) for tunneled calls.

For the system to pre-authenticate a call using CLID or DNIS, the telco switch must send the information as part of the call, and the MAX TNT must be configured to extract and use the information.

For details about pre-authentication 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
```

Parameter	Specifies
Profile-Type	Type of tunnel profile.Specify Mobile-Client for PPTP tunneling.
Tunneling-Protocol	Protocol to use when creating a tunnel for this profile. Set to PPTP to pass traffic to a PNS.
Primary-Tunnel-Server	DNS hostname or dotted IP address of the PNS endpoint. If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.

PPTP settings in RADIUS profiles

RADIUS uses the following attribute-value pairs to specify PPTP tunnels:

Attribute	Value
Tunnel-Type (64)	The tunneling protocol to be used. Set to PPTP (1) for PPTP tunneling.
Tunnel-Medium-Type (65)	The media to be used for the tunnel. Only IP (1) is supported at this time.
Tunnel-Server-Endpoint (66)	The DNS hostname or dotted IP address of the PNS endpoint (a string value). If it specifies a hostname, the MAX TNT executes a DNS lookup for the host's address.

Examples of opening a tunnel after pre-authenticating the call

To enable the MAX TNT to pre-authenticate 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 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-sever = 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", User-Service = Dialout-Framed-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-sever = pptp-1.example.com

admin> write
CONNECTION/tunnelcx
```

Following is a comparable RADIUS profile:

```
8001234567 Password = "Ascend-DNIS", User-Service = Dialout-Framed-user
    Tunnel-Server-Endpoint = "pptp-1.example.com",
    Tunnel-Type = PPTP,
    Tunnel-Medium-Type = IP
```

Examples of opening a tunnel after password authentication

In this example, the MAX TNT 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 MAX TNT authenticates the caller before bringing up a tunnel to an 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 ip remote-address = 5.5.5.5

admin> set ppp recv-password = localpw

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-sever = 1.1.1.1

admin> set tunnel tunneling-protocol = pptp
```

```
admin> write
CONNECTION/pptp-test written
```

Following is a comparable RADIUS profile:

```
pptp-test Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 5.5.5.5,
    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 *endpoints* 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 this release, the MAX TNT encapsulates the incoming IP packet in another IP packet, forming an IP-in-IP packet. It does not decapsulate an IP-in-IP packet. In other words, the MAX TNT 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 relevant Connection profile parameters, shown here with sample settings:

```
[in CONNECTION/p50:tunnel-options]
profile-type = mobile-client
tunneling-protocol = ipinip-protocol
primary-tunnel-server = "10.2.3.4"
```

Parameter	Specifies
Profile-Type	Type of tunnel profile. For IP-in-IP tunneling, must specify Mobile-Client.
Tunneling-Protocol	Protocol to use when creating a tunnel for this profile. Must specify IPINIP-Protocol to encapsulate IP packets within IP.
Primary-Tunnel-Server	DNS hostname or dotted IP address of the Tunnel Server endpoint (the intermediate destination that will decapsulate the IP packets). If it specifies a hostname, the MAX TNT 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.

Settings in a RADIUS profile

The following RADIUS attributes can be used to indicate IP-in-IP encapsulation:

Attribute	Value
Tunnel-Type (64)	Protocol to use when creating a tunnel for this profile. Must be set to IP-in-IP (7) to encapsulate IP packets within IP.
Tunnel-Server-Endpoint (67)	DNS hostname or dotted IP address of the Tunnel Server endpoint (the intermediate destination that will decapsulate the IP packets). The value is accepted as a string. If it specifies a hostname, the MAX TNT 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.

Examples of an IP-in-IP connection

The Pipeline unit shown at the right of Figure 7-3 dials in to the MAX TNT to log into the 10.156.7.0/29 network. After the connection has been established, the MAX TNT 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.

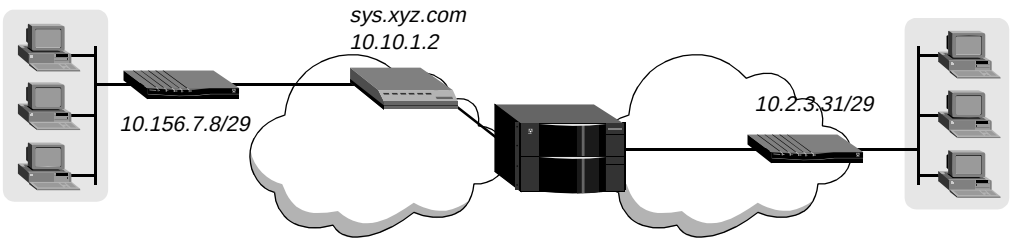


Figure 7-3. IP-in-IP tunneling

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 are is a comparable RADIUS profile:

```
p50 Password = "localpw"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.2.3.31
    Framed-Netmask = 255.255.255.248
    Tunnel-Type = IP-in-IP,
    Tunnel-Server-Endpoint = "sys.xyz.com"
```

IPX Routing

8

IPX routing on the WAN 8-1
Configuring the IPX-Global profile 8-4
Configuring LAN IPX interfaces 8-5
Configuring WAN IPX interfaces 8-7
Configuring static IPX routes 8-12
Defining and applying IPX SAP filters 8-15

IPX routing on the WAN

A MAX TNT configured for IPX routing enables NetWare clients and distributed Novell networks to use NetWare services across the WAN. Ascend has optimized IPX routing for the WAN, which required some modifications of standard IPX behavior as well as IPX extensions to enable the MAX TNT to operate as clients expect for NetWare LANs. This section discusses issues related to scaling LAN protocols to the WAN.

How Ascend units use IPX SAP

The MAX TNT follows standard IPX SAP behavior for routers when connecting to non-Ascend units across the WAN. However, when it connects to another Ascend unit configured for IPX routing, both ends of the connection exchange their entire SAP tables, so all remote services are immediately added to the MAX TNT unit's SAP table and vice versa.

When a NetWare client sends a SAP request to locate a service, the MAX TNT 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 MAX TNT receives those packets, it consults its RIP table. If it finds an entry for that destination address, it brings up the connection (unless it is already up) and forwards the packet.

How Ascend units use IPX RIP

The MAX TNT follows standard IPX RIP behavior for routers when connecting to non-Ascend units. However, when it connects to another Ascend unit configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, the MAX TNT maintains those 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 periodically and when a WAN connection is established. The MAX TNT 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.

The IPX RIP default route

The MAX TNT recognizes network number –2 (0xFFFFFFFE) as the IPX RIP default route. When it receives a packet for an unknown destination, the MAX TNT forwards the packet to the IPX router advertising the default route. If more than one IPX router is advertising the default route, the unit makes a routing decision based on Hop and Tick count. For example, if the MAX TNT receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the MAX TNT forwards the packet towards network number FFFFFFFE, if available, instead of simply dropping the packet.

Support for IPXWAN negotiation

The MAX TNT supports the IPXWAN protocol, which is essential for communicating with Novell software (such as NetWare Connect2) that supports dial-in connections, and with the Multi-Protocol Router. For full specifications of the IPXWAN protocol, see RFC 1634 and *NetWare Link Services Protocol Specification—IPX WAN Version 2*.

When an IPX connection is brought up between two Ascend units, all options are negotiated during the IPXCP phase. IPXWAN negotiation never takes place between two Ascend units, because neither unit initiates the negotiation process by sending out an IPXWAN Timer_Request packet.

Connections with non-Ascend devices that 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 MAX TNT. 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 MAX TNT supports the following routing options:

- Ascend Routing (Unnumbered RIP/SAP without aging).
- Novell Routing (Unnumbered RIP/SAP with aging).
- None (The peer is a dial-in client. No RIP/SAP except on request and we may 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, Ascend provides extensions to standard IPX. The added features enhance WAN functionality, as shown in Table 8-1

Table 8-1. Ascend extensions to IPX

Ascend extension	Purpose
Virtual network for dial-in clients	To enable the MAX TNT to route IPX to non-routers (NetWare clients), it supports a virtual IPX network defined in the MAX TNT unit's IPX-Global profile. The unit can then assign a unique network address to the client. The client's connection must specify that it is a Dialin-Peer.
Accepting or rejecting RIP and SAP updates	The MAX TNT 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 MAX TNT 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 MAX TNT 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 MAX TNT 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.

Due to 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 MAX TNT must support AppleTalk routing. Otherwise, AppleTalk packets will not make it across the connection. If UNIX clients access NetWare servers via

TCP/IP (rather than UNIXWare), the MAX TNT 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 to define 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	Enables/disables IPX routing for the interface. When you write the profile, the MAX TNT 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" (next).

Defining a virtual IPX network for dial-in clients

When a NetWare client dials in, the MAX TNT negotiates a routing session with the client by assigning the client a node address on the virtual IPX network. The client must accept the network number defined in this pool. If it has its own node number, the MAX TNT uses that number to form the full network:node address. If the client does not have a node number, the MAX TNT 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 MAX TNT. The MAX TNT 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 MAX TNT comes up in 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 MAX TNT 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 MAX TNT 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 port.

Overview of LAN IPX settings

The IPX-Interface profiles contain the following parameters, which are 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	Enables/disables IPX routing on the interface, provided that the IPX-Frame type is also set.
IPX-Frame	Specifies the IPX frame type the MAX TNT will route and spoof. If set to 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” (below).
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 8-17.

Enabling IPX routing and spoofing on the interface

To enable the MAX TNT 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 MAX TNT will route and spoof.

Note: The MAX TNT 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 MAX TNT drops those packets. If you are not familiar with the concept of packet frames, see the Novell documentation.

To see which frame type to use on a LAN interface, go to a NetWare server's console on that segment and type LOAD INSTALL to view the AUTOEXEC.NCF file. Following is an example 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 MAX TNT for that interface must be consistent with the number in use by the other routers. The best way to ensure this is to leave the default null address in the IPX-Net-Number parameter. The null address causes the MAX TNT 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 MAX TNT becomes a seed router, and other routers can learn their IPX network number from the MAX TNT. 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, these broadcasts are not propagated over routed links (as Novell recommends) and are not forwarded over links that have less than 1 Mbps throughput. However, if you are using an application such as NetBIOS over IPX, which 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 MAX TNT to route 802.3 IPX frames to and from the LAN interface and 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, which means the MAX TNT 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 the current "Authenticating framed protocol sessions" on page A-6), because the MAX TNT 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 one or more of the following IPX options, which are 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	Enables/disables 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. If set to Dialin-Peer, the MAX TNT assigns an IPX network number on the virtual IPX network described in "Defining a virtual IPX network for dial-in clients" on page 8-4.
RIP	If Peer-Mode is set to Router, enables/disables 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, enables/disables IPX SAP updates on the interface. Does not apply if Peer-Mode is set to Dialin-Peer.
Dial-Query	Enables/disables initiating a connection on 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	A second IPX network number, to be used only when connecting to non-Ascend routers that use numbered interfaces.
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 8-17.
IPX-SAP-HS-Proxy	Enables/disables 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	Enables/disables 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	Value
Ascend-Route-IPX (229)	Enables/disables 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 set to Peer-Dialin, the MAX TNT assigns an IPX network number on the virtual IPX network described in “Defining a virtual IPX network for dial-in clients” on page 8-4
Framed-IPX-Network (23)	Four-byte hexadecimal IPX network number for the link to the client. This address is used in Access-Accept packets.
Ascend-IPX-Alias (224)	A second IPX network number, to be used only when connecting to non-Ascend routers that use numbered interfaces.

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 for RADIUS profiles, see “Answer-Defaults IPX Peer-Mode setting” on page 8-9.

When the Peer-Mode specifies a Dialin-Peer, the MAX TNT 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 MAX TNT uses that number to form the full network address. If it does not have a node number, the MAX TNT assigns it a unique node address on the virtual network.

Note: When connecting to a Dialin-Peer, the MAX TNT 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

The MAX TNT supports 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 the remote router

When the remote end of the connection is a router, you can specify how RIP and SAP packets are handled across this WAN connection. Both parameters are set to Both by default, which means that the MAX TNT 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).

You can set the RIP parameter to Send to cause the MAX TNT to send its routes to the remote router, but not to receive any updates on this interface. Or, you can set it to Recv to receive updates from the remote router, but not propagate the local IPX routes to the remote site. If you set it 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 MAX TNT 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 disable the exchange of SAP broadcasts across a WAN connection, or specify that the MAX TNT will only send or only receive SAP broadcasts on that connection.

When to use net-number and net-alias

The 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 MAX TNT to know that router's network number before connecting.

The Net-Alias parameter may specify a second IPX network number, to be used only when connecting to non-Ascend routers that use numbered interfaces.

Using dial-query

Dial-Query configures the MAX TNT 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 MAX TNT SAP table. If the MAX TNT 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 MAX TNT brings up all 20 connections in response to the query.

Note: If the MAX TNT unit has a static IPX route for even one remote server, it chooses to bring up that connection as opposed to the more costly solution of bringing up every connection that has Dial-Query set.

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 this connection. Without this feature, when the client is in a distant location and sends a Get Nearest Server Request query, the client receives responses from servers closer to that location, rather than 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 the home-server proxy, set the IPX-SAP-HS-Proxy parameter to Yes, and configure the IPX-SAP-HS-Proxy-Net parameter with from one to six IPX network numbers. The MAX TNT 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 8-1 shows a MAX TNT providing a connection between an IPX network, which supports NetWare servers and clients, and a remote site that also supports NetWare servers and clients, and an Ascend unit.

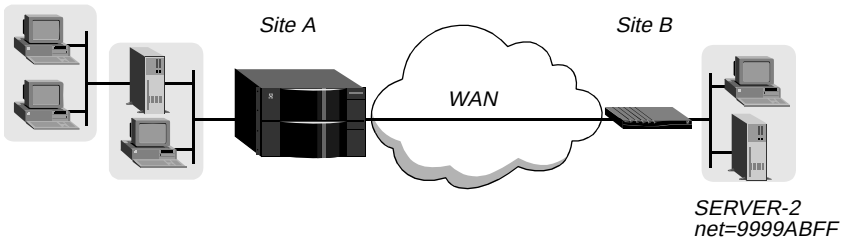


Figure 8-1. IPX connection with NetWare servers on both sides

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 Ascend 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"
    User-Service = 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, to ensure that the MAX TNT 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-SiteA-1 Password = "ascend", User-Service = Dialout-Framed-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 8-12.

Examples of a connection to a dial-in client

Figure 8-2 shows a NetWare client dialing into the MAX TNT to reach a corporate IPX network. The caller is running NetWare client software with PPP software to dial in.

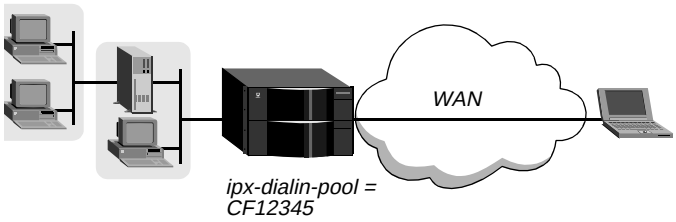


Figure 8-2. Dial-in NetWare client

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 using PPP software, and the Connection profile must set Peer-Mode to Dialin-Peer. In addition, the MAX TNT 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 8-4.

Following is an example of input that configures an IPX routing connection for the client shown in Figure 8-2:

```
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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-Route-IPX = Route-IPX-Yes,
    Ascend-IPX-Peer-Mode = IPX-Peer-Dialin
```

Configuring static IPX routes

When the MAX TNT is reset or power cycled, it clears its 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 MAX TNT to reach a NetWare server and download more complete tables from there.

In the case where a MAX TNT is connecting to another Ascend 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 MAX TNT downloads the RIP table from the other Ascend 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 an address change. Their advantages are that they ensure that the

MAX TNT can bring up the connection in response to clients' SAP requests, and 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.

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 use the following parameters, which are 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 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	The server's node address on the internal network. Servers typically use the default node address of 000000000001 on the internal network.
Server-Socket	A well-known socket number in the server. For details, see "Socket numbers in static routes" on page 8-15.
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.
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 these value for very distant servers.

Parameter	Specifies
Profile-Name	Name of the Connection or RADIUS dialout profile used to reach the server. The default value is null. When the MAX TNT 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	Enables/disables 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 this format:

```
ipxroute-name-N Password="ascend", User-Service = Dialout-Framed-User
```

The *name* argument is the MAX TNT 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 MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

Note: To specify routes that may 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 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 dialout user profile that uses the route. When the MAX TNT 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 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	The server's node address on the internal network. Servers typically use the default node address of 000000000001 on the internal network.
socket	A well-known socket number in the server. For details, see "Socket numbers in static routes" on page 8-15.
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.
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.

Syntax element	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 these 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 may use a different socket each time they load, and 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-SiteA-1 Password = "ascend", User-Service = Dialout-Framed-User
   Ascend-IPX-Route = "sitebgw cc1234ff 000000000001 0451 0004 Server-1"
```

Defining and applying IPX SAP filters

IPX SAP filters contain a set of rules that determine which remote NetWare services will be excluded from or included in the MAX TNT 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 MAX TNT 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, which are 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 = ""

[inIPX-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	Effect
IPX-SAP-Filter-Name	You must assign each SAP filter a name, so that it 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)	Each SAP filter can contain up to 8 Input-Filter specifications, which are defined individually and applied in order (1–8) to SAP packets the MAX TNT receives. Input filters determine which remote services are accessible to local NetWare users.
Output-IPX-SAP-Filters (1–8)	Each SAP filter can contain up to 8 Output-Filter specifications, which are defined individually and applied in order (1–8) to SAP response packets. The MAX TNT transmits SAP responses in reply to a SAP request packet. Output filters determine which local NetWare services are available to remote users.
Valid-Filter	Enables or disables the Input or Output filter. When it is set to No (the default), that filter is skipped when filtering the SAP data. Set it to Yes for each defined filter you intend to use.
Type-Filter	Specifies whether to include or exclude the service defined by the Server-Name or Server-Type parameters (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	Specifies a NetWare service type. Service types are hexadecimal numbers representing a type of NetWare service. You can use the FFFF type to indicate all types. The number for File Service is 0004. For complete information about SAP service types, refer to your NetWare documentation.
Server-Name	Specifies the name of a local or remote NetWare server. You can use the wildcard characters * and ? 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 MAX TNT SAP table will be inaccessible to clients on other MAX TNT interfaces. Following are the commands that define the SAP filter:

```
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 MAX TNT 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. Following are the commands that define the SAP filter:

```
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 MAX TNT SAP table and its responses to SAP queries on the interface. If the directory services feature is not supported, servers or services that are not in the MAX TNT 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 MAX TNT unit's SAP table and its 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 9

Configuring the Atalk-Global profile 9-1

Configuring LAN AppleTalk interfaces. 9-2

Configuring WAN AppleTalk interfaces 9-4

Introduction

A MAX TNT configured for AppleTalk routing enables dial-in connections from AppleTalk Remote Access (ARA) client software, PPP dial-in software that supports AppleTalk, and AppleTalk-enabled Ascend 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 is required for any kind of AppleTalk connection, even if the individual Connection profile to a remote device does not use routing.

Configuring the Atalk-Global profile

When an ARA or AppleTalk PPP client dials in, the MAX TNT 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, which are shown with sample settings:

```
[in ATALK-GLOBAL]
atalk-dialin-pool-start = 100
atalk-dialin-pool-end = 200
```

AppleTalk networks are assigned a network range, which is a contiguous range of integers between 1 and 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 a range 1000-1002 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 1000–1002:

```
admin> read atalk-global
ATALK-GLOBAL read

admin> set atalk-dialin-pool-start = 1000

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 MAX TNT will operate as a seed or nonseed router on the interface. In this release, only the built-in Ethernet interface on the shelf-controller can be configured an AppleTalk interface. The Atalk-Interface profile contains the following parameters, which are shown with default settings:

```
[in ATALK-INTERFACE/{ { any-shelf any-slot 0 } 0 } (new)]
interface-address* = { { any-shelf any-slot 0 } 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	Enables/disables AppleTalk routing on the shelf-controller Ethernet interface. If set to No, none of the other parameters applies.
Hint-Zone	Name of the zone in which the MAX TNT resides. Applies only when the MAX TNT is a nonseed router.
Atalk-Router	Specifies a routing mode. If set to Atlk-Router-Off, none of the remaining parameters applies. If set to Atlk-Router-Seed, 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. If set to Atlk-Router-Nonseed, 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 9-2.)
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 MAX TNT 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 between 1 and 65,199. Each range must be unique. No two interfaces may use the same range, and no two network ranges may 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 1005-1010 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 1005–1010, 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 = 1005
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 MAX TNT is configured in nonseed mode, a seed router must be available at start-up time, or the MAX TNT cannot come up in AppleTalk routing mode. (If the MAX TNT 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 MAX TNT resides, the system can include the specified zone name in the ZipGetNetInfo packet, and the router can return a valid network range for that zone. This is recommended.

The following commands configure the MAX TNT 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 dialin on the MAX TNT. 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 sync-PPP when the calling unit is an Ascend router (Pipeline or MAX series).

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 dialin connection (AppleTalk PPP)
- Synchronous PPP connection with an Ascend router (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). These 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, which are 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	Enables/disables 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 MAX TNT initiates an ARA disconnect when that time is up. The ARA link goes down cleanly, 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	Enables/disables 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 MAX TNT uses when routing packets to a remote site for a dialout AppleTalk connection. Note that currently only dial-in AppleTalk is supported.
Atalk-Static-Netstart Atalk-Static-Netend	Network range for packets that the MAX TNT routes to a remote site for a dialout AppleTalk connection. Note that currently only dial-in AppleTalk is supported.
Atalk-Peer-Mode	Type of dial-in client (router or dialin-peer). When set to Dialin-Peer, the MAX TNT 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)	Enables/disables 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). When set to Appletalk-Peer-Dialin , the MAX TNT 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 9-1, 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.

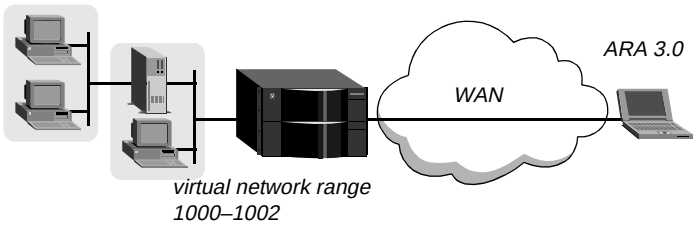


Figure 9-1. ARA Client dial-in

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"
    User-Service = 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 9-2, the dial-in client is running ARA 3.0, and has selected 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.

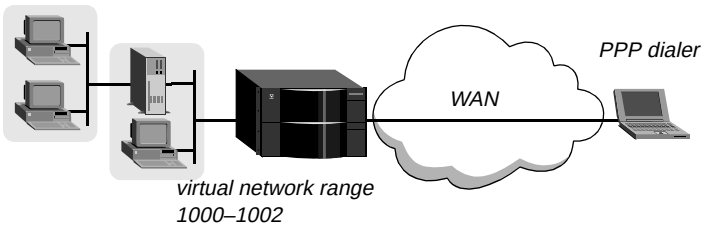


Figure 9-2. AppleTalk connection using a PPP dialer

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"
    User-Service = 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 9-3, the remote Pipeline unit is configured as an AppleTalk router on the extended AppleTalk network 2000-2001, in the Branch zone.

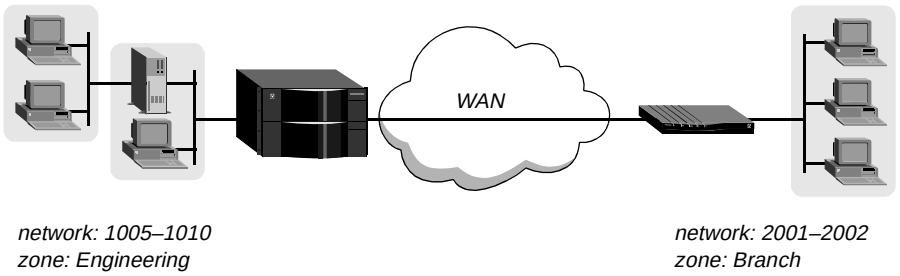


Figure 9-3. AppleTalk routing connection

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"
    User-Service = 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 MAX TNT must be configured both as an IP router as well as an AppleTalk router. For details about configuring the IP router and individual IP connections, see Chapter 4, “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 9-1 describes Macintosh TCP/IP configurations for a PPP connection:

Table 9-1. 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 MAX TNT handles IP packets by encapsulating them in DDP. Table 9-2 describes Macintosh TCP/IP configurations for a PPP connection:

Table 9-2. 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.

Table 9-2. Macintosh TCP/IP settings for ARA connections (continued)

Macintosh software	IP settings for an ARA connection
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 9-4, 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 MAX TNT local interface. The client has a hard-coded IP address.

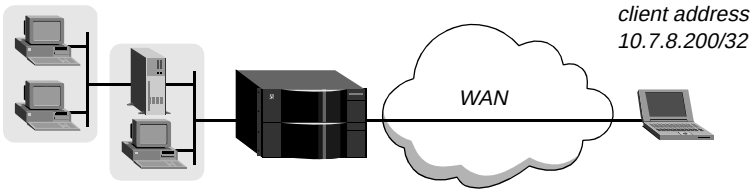


Figure 9-4. ARA connection that encapsulates IP packets in DDP

The following commands configure a profile that enables the client to dial in using ARA client 3.0 and then initiate a Telnet connection to a host on the MAX TNT 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"
    User-Service = Framed-User,
    Framed-Protocol = ARA,
    Framed-Address = 10.7.8.200,
    Framed-Netmask = 255.255.255.255,
    Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Dialin
```

Ascend Packet Filters

10

Filter overview 10-1
Defining generic filters 10-6
Defining IP filters. 10-11
Defining Type-of-Service filters 10-17
Defining IPX filters 10-21
Defining route filters 10-24
Applying a filter to an interface 10-26

Filter overview

A filter contains specifications describing packets and what to do when those packets are encountered. When a filter is applied to an interface, the MAX TNT monitors the data stream on that interface and takes a specified action when packet contents match the filter.

Depending on how a filter is defined, it can apply to inbound or 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 (which are applied to inbound packets) and 12 Output-Filters (which are applied to outbound packets). Each of those 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. They specify a forwarding action based on a comparison between certain bytes or bits in a packet and a value defined in the filter. 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 based on higher-level fields in IP packets, such as source or destination address, protocol number, and so forth. 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 based on 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 get.

Route filters apply only to RIP update packets. They specify whether matching routes in a RIP packet will be accepted into the routing table or denied, or accepted with an increased metric. They can also specify a source address, to 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 MAX TNT to drop or forward specific packets. The focus is typically to keep out traffic that you don't 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, 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.

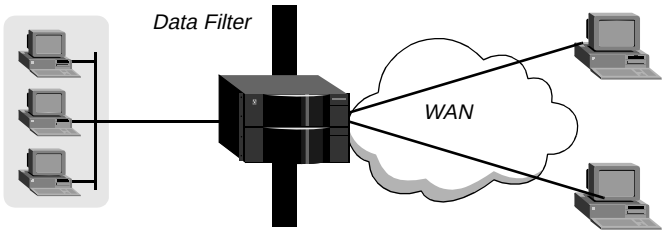


Figure 10-1. Data filters drop or forward certain packets

Call filters prevent unnecessary connections and help the MAX TNT 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.

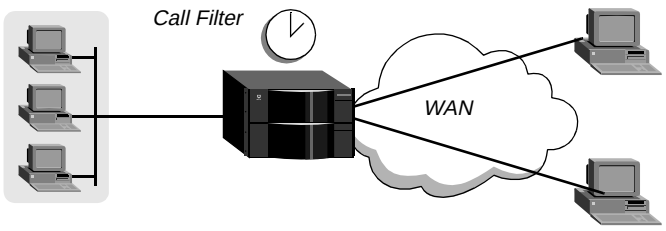


Figure 10-2. Call filters prevent certain packets from resetting the timer

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. The Idle-Timer is set to 120 seconds by default, so if a connection is inactive for two minutes, the MAX TNT terminates the connection.

How filters work

A Filter profile can specify up to 12 Input-Filter and Output-Filter specifications. Each filter has its own forwarding action—forward or drop. The filters are applied in sequence, and a match occurs at the first successful comparison between a filter and the packet being examined. When a comparison succeeds, 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 this filter. However, this does not mean that the packet is forwarded. When no filter is in use, the MAX TNT forwards all packets, but once you apply a filter to an interface, this default is *reversed*. For security purposes, the unit does not automatically forward non-matching packets. It requires a filter that explicitly allows those 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 10-14.

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 is allowed to go on to the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet.

If the 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 it 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 is allowed to go on to 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 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 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 non-zero 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 in 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 in the Dst-Port-Cmp parameter, the comparison fails.

6 If TCP-Estab is Yes and the protocol number is 6, the comparison succeeds.

If the 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 it is applied as a data filter, the forwarding action is either to forward the packet or drop it.

Type of Service 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 is allowed to go on to 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 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 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 non-zero 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 in 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 in 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 is allowed to go on to 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 in 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 in the Dst-Socket-Cmp parameter, the comparison fails.

If the 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 it 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 is allowed to go on to 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 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 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.

Parameter	Specifies
Valid-Entry	Enables/disables the filter specification. When it is set to No (the default), that specification is skipped when filtering the data stream. Set it 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 specification provides the same function as the Input-Filters and Output-Filters structure 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 MAX TNT 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 specification 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.

Settings in a local Filter profile

In a local Filter profile, a generic filter uses the following parameters, which are 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
```

Note: The same parameters are also available below 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 specified in the filter. For details, see “Specifying the offset to the bytes to be examined” on page 10-8.
Len	Number of bytes to test in a packet, starting at the specified offset (see “Specifying the number of bytes to test” on page 10-9).
More	Enables/disables inclusion of the next filter before determining whether the packet matches the specification. If set to Yes, the current specification is linked to the one immediately following it, so the filter can examine multiple noncontiguous bytes within a packet before the forwarding decision is made. The match occurs only if *both* specifications are matched. (The subsequent specification must be enabled, or the MAX TNT ignores the filter specification in which More is set to Yes.
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	A binary mask.The system applies the Mask to the specified Value before comparing it to the bytes in a packet specified by Offset. For details, see “Masking the value before comparison” on page 10-9.
Value	A hexadecimal number to be compared to specific bits contained in packets after the Offset, Length, and Mask calculations have been applied. After you have entered the number, the system enters a colon at the byte boundaries.

Settings in a RADIUS profile

In a RADIUS profile, you define a generic filter as a value to the Ascend-Call-Filter or Ascend-Data-Filter attribute, using the following format:

"generic *dir action offset mask value compare* [more]"

Keyword or Argument	Value
`generic`	Type of filter. Valid filter types for the Ascend-Data-Filter and Ascend-Call-Filter attributes are Generic-Filter (the default) and IP-Filter. See XREF TOS for related information.
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 10-8.
mask	A binary mask. The system applies the *mask* to the specified *value* before comparing it to the bytes in a packet specified by *offset*. For details, see “Masking the value before comparison” on page 10-9.
value	A hexadecimal number to compare to the packet contents at the specified offset in the packet. 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 MAX TNT compares packet contents to the filter value. You can specify `=` (Equal) or `!=` (Not Equal). Equal is the default.
`more`	If the More flag is present, the MAX TNT 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 MAX TNT 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 frame to the data in the packet to be tested against this filter. For example, with the following local definition:

```
[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 comparable RADIUS filter definition:

```
Ascend-Data-Filter = "generic in drop 2 0fffffff000000f 07fe45700000009"
```

And the following packet contents:

```
   2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The first two byes in the packet (2A and 31) are ignored due to the two-byte offset.

Specifying the number of bytes to test

In a RADIUS profile, the length of the mask and value must be equal, and 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 at the specified offset. The mask setting is assumed to be Len number of octets.

For example, 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
```

and the following packet contents:

```
   2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The filter applies the mask only to the eight bytes following the two-byte offset.

Masking the value before comparison

A generic filter can include a mask to apply to the specified value before comparing it to the bytes in a packet starting at the specified offset. You can use the mask to fine-tune exactly which bits you want to compare. The mask is assumed to the same number of octets as the Len parameter.

The MAX TNT applies the mask to the specified value using a logical AND after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. 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, with the following filter specification:

For example, with the following local definition:

```
[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
```

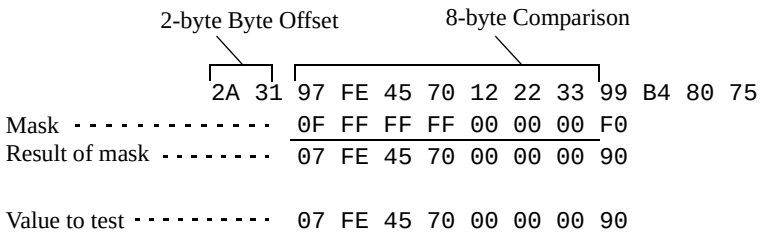
Or comparable RADIUS filter definition:

```
Ascend-Data-Filter = "generic in drop 2 0fffffff000000f 07fe45700000009"
```

And the following packet contents:

```
   2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The mask is applied as shown below, resulting in a Value that matches the Value.



The packet matches this filter. Because the forward parameter is set to No, the packet will be dropped. The byte comparison works as follows:

- 2A and 31 are ignored due to the two-byte offset.
- 9 in the lower half of the third byte is ignored, because the mask has a 0 in its place. The 7 in the third byte matches the Value parameter's 7 in the upper half of that byte.
- F and E in the fourth byte match the fourth byte specified by the Value parameter.
- 4 and 5 in the fifth byte match the fifth byte specified by the Value parameter.
- 7 and 0 in the sixth byte match the sixth byte specified by the Value parameter.
- 12 and 22 and 33 in the seventh, eighth and ninth bytes are ignored because the mask has zeroes in those places.
- 9 in the tenth byte matches the Value parameter's 9 in the lower half of that byte. The second 9 in the upper-half of the packet's tenth byte is ignored because the mask has a 0 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 in the Gen-Filter subprofile, so all packets are matched, and the forwarding action is left at the default No. In the Output-Filter, the default values again match all packets, but the forwarding action is set to Yes. So 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, such as protocol numbers, logical addresses, and TCP or UDP ports.

Settings in a local Filter profile

The IP-Filter subprofile contains the following parameters, which are 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
```

Note: The same parameters are also available below 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	A protocol number. A number of zero matches all protocols. If you specify a non-zero number, the MAX TNT compares it to the Protocol field in packets. For a list of assigned protocol numbers, see RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.
Source-Address-Mask	A mask to be applied to the Source-Address value before comparing that value to the source address of a packet.
Source-Address	An IP address. After applying the Source-Address-Mask, the MAX TNT compares the result to the source address in a packet. For details, see “Filtering by source or destination address” on page 10-13.
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	An IP address. After applying the Dest-Address-Mask, the MAX TNT compares the result to the source address in a packet.For details, see “Filtering by source or destination address” on page 10-13.

Parameter	Specifies
Src-Port-Cmp	Type of comparison to perform when comparing source port numbers. If set to 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 number.
Source-Port	A 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 10-14.
Dst-Port-Cmp	Type of comparison to perform when comparing destination port numbers. If set to 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 number.
Dest-Port	A 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 10-14.
TCP-Estab	Enables/disables application of the filter only to packets in an established TCP session. Applicable only if the protocol number has been set to 6 (TCP).

Settings in a RADIUS profile

In a RADIUS profile, you define an IP filter as a value to the Ascend-Call-Filter or Ascend-Data-Filter attribute, using 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 specification cannot contain newlines. The syntax is shown above on two lines for printing purposes only.

Keyword or Argument	Value
`ip`	Type of filter. Valid filter types for the Ascend-Data-Filter and Ascend-Call-Filter attributes are Generic-Filter (the default) and IP-Filter. See XREF TOS for related information.
`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 MAX TNT 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 address" on page 10-13.

Keyword or Argument	Value
`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 MAX TNT 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 address" on page 10-13.
proto	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX TNT compares it to the Protocol field in packets. For 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), talk (517). For more details, see "Filtering by port numbers" on page 10-14.
`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). 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), talk (517). For more details, see "Filtering by port numbers" on page 10-14.
`est`	If the Est flag is present, it restricts application of the filter only 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 address

When you specify a source or destination address in an IP filter, the MAX TNT applies the filter's forwarding action to packets received from or sent to that address. If you also specify a subnet mask, the MAX TNT 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 MAX TNT 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 portion of the address that falls behind each binary 0 (zero) 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 source address for a single host is matched.

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 that are not required from outside your domain. UDP-based services are 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 (<), Eql (=), Gtr (>), or Neq (!=) the port number specified in the filter.

Examples of an IP filter to prevent local address spoofing

IP-address spoofing 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 "Examples of per-session source address checking" on page 4-21.

The sample filter first defines two Input-Filters that drop packets whose source address is on the local IP network or is the loopback address (127.0.0.0). In effect, these specifications say: "If you see an inbound packet with one of these source addresses, drop the packet." 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.

This example uses a local IP network address of 192.100.50.128, with a subnet mask of 255.255.255.192. These addresses are just examples.

Note: If you apply this filter to the Ethernet interface, the MAX TNT drops IP packets it receives from local LAN, and you will not be able to Telnet to the unit.

The following commands create 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 MAX TNT drops it instead of forwarding it to the Ethernet, 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 commands create 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 MAX TNT drops it instead of forwarding it to the Ethernet, 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 commands create the second Input-Filter, setting the type to IP-Filter and setting Forward to Yes. The third filter uses all default values. Because Forward is set to Yes, the MAX TNT forwards all remaining packets (those with nonlocal source addresses) to the Ethernet.

```
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 commands create the first Input-Filter, setting the type to IP-Filter and Forward to Yes, and configure the first filter to allow packets to reach the Web server's destination address at a destination TCP port which 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 commands create the second Input-Filter, setting the type to IP-Filter and Forward to Yes, and configure the second filter to allow inbound TCP packets that are responding to a local user's outbound Telnet request, you can forward TCP packets whose destination port is greater than the source port. (Telnet requests go out on port 23 and responses come back on some random port greater than 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, setting the type to IP-Filter and Forward to Yes, and configures the third filter to allow inbound RIP updates, you can specify a filter that forwards inbound UDP packets if the destination port is greater than 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 greater than 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 next 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. ICMP does not use ports like TCP and UDP, 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 Type-of-Service 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.) Administrators can also define TOS filters directly in a RADIUS user profile by setting the Ascend-Filter attribute.

Settings in a local Filter profile

Following are the relevant Filter parameters, which are 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	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX TNT compares it to the Protocol field in packets. For list of protocol numbers, see RFC 1700.
Source-Address-Mask	A mask to be applied to the Source-Address value before comparing that value to the source address of a packet.

Parameter	Specifies
Source-Address	An IP address. After applying the Source-Address-Mask, the MAX TNT compares the result to the source address in a packet. For details, see “Filtering by source or destination address” on page 10-13.
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	An IP address. After applying the Dest-Address-Mask, the MAX TNT compares the result to the source address in a packet.For details, see “Filtering by source or destination address” on page 10-13.
Src-Port-Cmp	Type of comparison to perform when comparing source port numbers. If set to 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 number.
Source-Port	A 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 10-14.
Dst-Port-Cmp	Type of comparison to perform when comparing destination port numbers. If set to 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 number.
Dest-Port	A 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 10-14.
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, 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 next four bits of the TOS byte are used to choose a link based on 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.

Settings in a RADIUS profile

In RADIUS, a TOS filter entry is a value of the Ascend-Filter attribute. A TOS filter value is specified in 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 newlines. The syntax is shown here on multiple lines for printing purposes only.

Keyword or argument	Description
`iptos`	Specifies an IP filter.
`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 MAX TNT 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 address” on page 10-13.
`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 MAX TNT 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 address” on page 10-13.
proto	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX TNT compares it to the Protocol field in packets. For 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), > (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), talk (517). For more details, see “Filtering by port numbers” on page 10-14.
`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), > (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), talk (517). For more details, see “Filtering by port numbers” on page 10-14.

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, those bits are set to the specified value (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` *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. Those four bits are used to choose a link based on the type of service. One of the following values can be specified: 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 is a relatively low priority, which means that an upstream router that implements priority queuing may drop these packets when it becomes loaded. The commands also set TOS to prefer a low latency connection. This means that the upstream router will choose a a fast connection is one is available, even if it is higher cost, lower bandwidth, or 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 00:00:00:0+
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={00:00:00:0000:00:00:0000:00:00:00:00:0000:00:00:00:00+
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 specification:

```
jfan-pc Password = "secret"
    User-Service = 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 specifications cannot contain newlines. The above example shows the specification on two lines for printing purposes.

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 subprofile contains the following parameters, which are 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
```

Note: The same parameters are also available below 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 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.

Filtering by source or destination 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 the Src-Net-Address in a filter, you should also specify the 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 may 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 MAX TNT to drop all outbound IPX packets with the destination IPX network 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 MAX TNT to drop all inbound IPX packets from a specific source. In this example, the filter causes the MAX TNT to drop packets from the source IPX network address 00000005:00abcde12345 and the source socket number of 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.

Note: For route filters, the forwarding action has no effect.

In a local Filter profile, the Route-Filter subprofile contains the following parameters, which are 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
```

Note: The same parameters are also available below 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	A mask to be applied to the Source-Address value before comparing that value to the source address of a RIP update packet.
Source-Address	An IP address. After applying the Source-Address-Mask, the MAX TNT compares the result to the source address in a RIP packet. For related information, see “Filtering by source or destination address” on page 10-22.
Route-Mask	A mask to be applied to the destination address of a route.
Route-Address	An IP address. After applying the Route-Mask, the MAX TNT compares the result to routes ina RIP packet. If it finds a route with a matching destination, it takes the specified action.
Add-Metric	A number between 1 and 15, to be added to the metric value for a route that matches the filter specification, if the specified Action 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 set in the add-Metric parameter to the route Metric and accept the route).

Example of a filter that excludes a route

In the following 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
```

Note: 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 the following 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
```

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

Following are the parameters related to applying a filter, 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 10-29. 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 10-28. The setting in the Answer-Defaults profile is used only for RADIUS-authenticated connections that do not include a data filter.
Filter-Persistence	Enables/disables 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 10-30.
TOS-Filter	Name of a Filter profile. For details, see “Examples of applying a TOS filter to a WAN interface” on page 10-29.
Filter-Name	Name of a Filter profile. For details, see “Example of applying a filter to a LAN interface” on page 10-30.

Settings in RADIUS profiles

The following RADIUS attribute-value pairs are used to apply a filter to a WAN connection:

Attribute	Value
Ascend-Call-Filter (243)	An abinary-format filter specification 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 10-6 and "Defining IP filters" on page 10-11.
Ascend-Data-Filter (242)	An abinary-format filter specification 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 10-6 and "Defining IP filters" on page 10-11.
Ascend-Filter (91)	A 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 Type-of-Service filters" on page 10-17.
Filter-ID (11)	Name of a local Filter profile that defines a data filter. The next time the MAX TNT 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), the system creates a baseline 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, so if the caller's profile applies a data filter or call filter (or both), the MAX TNT does not use the filters applied in the Answer-Defaults profile.

Attributes that are not specified in the caller's profile take their value from the Answer-Defaults settings. So if the caller's RADIUS profile does not apply a data filter or call filter, and the Use-Answer-For-All-Defaults parameter is set to Yes, filters applied in the Answer-Defaults profile are applied to the authenticated connection.

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 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 MAX TNT supports the local Filter profiles shown below:

```
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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.10.10.64,
    Framed-Netmask = 255.255.255.0,
    Filter-Id = "ip-spoof"
```

The following RADIUS profile references both local filters:

```
tlynch Password = "secret"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.10.10.64,
    Framed-Netmask = 255.255.255.0,
    Filter-Id = "ip-spoof",
    Filter-Id = "web-access"
```

Note: As is always the case with filters, the order in which they are applied within the user profile is significant. If the MAX TNT supports multiple Filter profiles with similar names, it uses the first Filter profile to match the characters specified in the user profile.

The following example defines an anti-spoofing filter within the user's RADIUS profile:

```
tlynch Password = "secret"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.10.10.64,
    Framed-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 MAX TNT 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"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.10.10.23,
    Framed-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 MAX TNT 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 using Filter-Id:

```
jfan-pc Password = "johnfan"
    User-Service = 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"
    User-Service = 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 specifications cannot contain newlines. The above example shows the specification on two lines for printing purposes.

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 MAX TNT 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 or 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.

Note: Route filters do not stop RIP update packets from being forwarded. Their action determines whether the system adds matching routes to its routing table.

Following is an example of applying a route 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 reach the Ethernet or leave the Ethernet for another interface. A filter applied to an Ethernet interface takes effect immediately. If you change the Filter profile definition, 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 MAX TNT inaccessible from the local LAN.

Following is an example of a procedure that 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
```

Authentication Methods

A

Introduction A-1
RADIUS password handling A-2
Authenticating framed protocol sessions A-6
Authenticating user login sessions A-9
Token card authentication A-13
Tunnel authentication A-21
Pre-authentication (CLID or DNIS) A-23
Callback after authentication A-30

Introduction

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, and tries to use it later to establish what appears to be a valid session.

Authentication of terminal-server logins

For login sessions, when users dial into 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.

Pre-authentication using call information

Calling-Line ID (CLID) and Dial Number Information Service (DNIS) are information that may be provided as part of the call by the telco switch. You can use this information to verify the calling number and dialed number, respectively, before the MAX TNT answers the call.

Using callback for added security

After authentication is complete, the MAX TNT can hang up and call back, ensuring that the connection is made only with a trusted number.

RADIUS password handling

The Ascend RADIUS daemon recognizes RADIUS user entries 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 may also be a phone number (for CLID or DNIS authentication), a special string indicating a pseudo-user profile, or the string `DEFAULT` (for the default user profile). For details about pseudo-user profiles, see the *MAX TNT RADIUS Guide*.

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 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

In addition to the connection-specific password typically assigned to a specific user profile, the Ascend RADIUS daemon recognizes the following reserved values for the Password (2) attribute:

Password values	Description
`UNIX`	Instructs the RADIUS server use the UNIX authentication by means of the /etc/password file. This password does not work with the CHAP protocol.
`SAFEWORD`	Instructs the RADIUS server to request validation from an Enigma Logic SafeWord server (see "Token card authentication" on page A-13).
`ACE`	Instructs the RADIUS server to request validation from a Security Dynamics ACE server (see "Token card authentication" on page A-13).
`ascend`	Used for pseudo-user and other system profiles. When this password is in use, the User-Service attribute should always specify Dialout-Framed-User, to prevent callers from accessing the network using a well-known password. *Although the system does not reject the profile without the Dialout-Framed-User setting, omitting it introduces a serious security risk.*
`Ascend-CLID` or `Ascend-DNIS`	Used for pre-authenticating calls using CLID or DNIS information When these passwords are in use, the User-Service attribute should always specify Dialout-Framed-User, to prevent callers from accessing the network using a well-known password. *Although the system does not reject the profile without the Dialout-Framed-User setting, omitting it introduces a serious security risk.*

Password expiration

The Ascend RADIUS daemon supports password aging and expiration, and provides a method for enabling users who dial into 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 reserved passwords (such as `Ascend`).

Note: If you run the Ascend RADIUS daemon with a flat ASCII file, RADIUS accepts a user's replacement for an expired password only if you start the daemon with the `-p` argument. If you run the daemon in DBM mode, RADIUS accepts a user's replacement for an expired password if you specify the `-p` argument, but does not recognize the new password until you rebuild the users database by running `builddbm` again. For details, see the *MAX TNT RADIUS Guide*.

The Ascend RADIUS daemon uses the following attribute-value pairs to support password aging and expiration.

Attribute	Value
Ascend-PW-Expiration (21)	Expiration date for the user's password (a date consisting of a month, day, and year specification.) Its value can be updated automatically when a user renews a password. Must be a Check-Item.
Ascend-PW-Lifetime (208)	Number of days a password can be valid (an integer from 0 to 65535). The default zero disables password expiration. If it is set to a nonzero value, when the user changes the password, the MAX TNT adds the value to the current date and updates the Ascend-PW-Expiration date. This 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, 1999:

```
brian Password = "localpw", Ascend-PW-Expiration = "Jan 1, 1999"
    Ascend-PW-Lifetime = 30,
    Ascend-PW-Warntime = 2,
    ...
```

When the user dials in on December 30, 1998, he receives a message that his password will expire in two days. If he changes the password at that time (by using the 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, 1999.

If the user dials in on January 1, 1999, he receives a message that his password has expired, and he 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:

- You did not start the RADIUS daemon with the `-p` argument.
- 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.
- The RADIUS daemon is running in DBM mode. When the daemon is running in DBM mode, a user can successfully change an expired password, but cannot gain access to the

network immediately. Access with the new password can take place only after you rebuild the RADIUS database with the modified users file containing the new password.

The DEFAULT user profile

A special user profile named `DEFAULT` can be placed at the end of the user file to specify what to do with users who do not have a profile in the user 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 using their UNIX account name and password:

```
DEFAULT Password = "UNIX"
    User-Service = Login-User,
    Login-Service = Telnet
```

Shared secrets and secure exchanges

A shared secret is used to authenticate packets exchanged between the MAX TNT 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 TNT-01, the following entry in the clients file specifies a shared secret of `nas-secret`:

```
TNT-01 nas-secret
```

The MAX TNT 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:

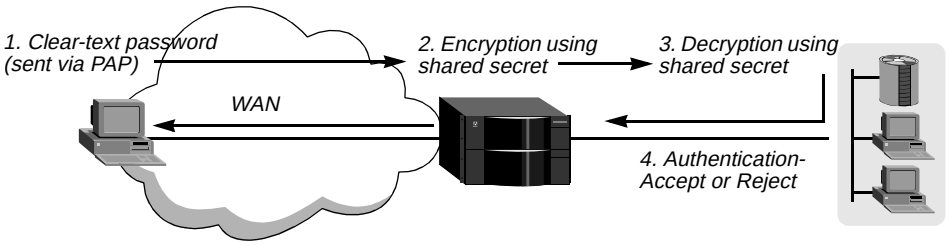


Figure A-1. Shared secret used between the MAX TNT and a RADIUS server

The shared secret is used to encrypt the password from the dial-in call before sending it 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 NAS. The Ascend RADIUS daemon encrypts 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 Ascend-Send-Secret and the RADIUS daemon does not encrypt the password, authentication will fail.

If the dial-out profile uses the Ascend-Send-Passwd (232) attribute to specify the password instead, the RADIUS daemon performs no encryption before sending the password to the NAS. This may be required if you are using a RADIUS server that does not support outbound password encryption.

Unless you are using a RADIUS daemon that does not support Ascend-Send-Secret, its use 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 MAX TNT authenticates the user using the agreed-upon authentication protocol. 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 each end 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 indicate 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 to a value other than the default No-PPP-Auth, the MAX TNT requests certain authentication options using LCP, and the caller must accept one of the options the system offers. With the default setting, the MAX TNT does not request authentication.

PAP-PPP-Auth indicates the Password Authentication Protocol (PAP), which provides a simple method for the MAX TNT to establish its identity in a two-way handshake. The remote device must support PAP.

CHAP-PPP-Auth indicates the Challenge Handshake Authentication Protocol (CHAP), which is more secure than PAP. When the MAX TNT 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 indicates 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 indicates any of the above protocols. The MAX TNT 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.

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 MAX TNT forces the peer to use PAP.

When PAP is used with RADIUS authentication, the MAX TNT 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 decrypts the password using the same shared secret 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 may 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, where an insecure plain text login might be required. 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.

When CHAP or MS-CHAP is used with RADIUS authentication, the following events occur:

1. The MAX TNT 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 MAX TNT. The MAX TNT never has the caller's password.
4. The MAX TNT 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 with the local version of the remote secret, along with the challenge and PPP packet ID received from the MAX TNT.
6. The RADIUS server compares the calculated MD5 digest with the digest it received from the MAX TNT. If the digests are the same, the passwords matched, and the call is accepted.

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 authentication is negotiated. Other values are PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, and Any-PPP-Auth.
Send-Password	Password the MAX TNT 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.

Attribute	Value
Ascend-Authen-Alias (203)	A login name for the MAX TNT 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.

Attribute	Value
Ascend-Send-Auth (231)	Authentication protocol requested for a dial-out call. With the default Send-Auth-None (0) value, no authentication is negotiated. Other values are Send-Auth-PAP (1) and Send-Auth-CHAP (2).
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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.1.2.3,
    Framed-Netmask = 255.255.255.248

route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "10.1.2.3/29 10.1.2.3 1 n hanif-out"

hanif-out Password = "localpw", User-Service = Dialout-Framed-User
    User-Name = "hanif",
    Ascend-Dial-Number = "555-1212",
    Framed-Protocol = PPP,
    Framed-Address = 10.1.2.3
    Framed-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, it may be 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 the authorized level of access to the terminal-server itself or 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 MAX TNT forwards the call to the router software, and establishes a regular PPP session. Except for the initial processing, the MAX TNT 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 MAX TNT 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 MAX TNT authenticates it 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 which come under the heading of *authorization*. For details, see Appendix B, "Authorization Options."

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 15 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 async interface. For example:

```
ATDT961234
CONNECT 115200
** Ascend TNT 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 a system password as well as their own name and password before seeing the terminal-server prompt.

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 into the terminal server:

```
System Password:

Name:
Password:
```

Customizing the login sequence

The following parameters (shown with default settings) define which strings are sent to and expected from a dial-in user during the login process:

```
[in TERMINAL-SERVER:terminal-mode-configuration]
banner = "** Ascend TNT 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 `"** Ascend TNT Terminal Server **"`.
Login-Prompt	Second line sent to the dial-in user, prompting for a user name. 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.

Parameter	Specifies
Third-Prompt-Sequence	Where the third login prompt appears in the login sequence (first or last).
Prompt	String to use as the command-line prompt in the terminal-server interface.
Login-Timeout	Number of seconds the login prompt is displayed before timing out. When a user logs into 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, command-line prompt, and login timeout:

```
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 into 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, defined 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 Ascend (for example, one that includes a menu selection before login). If that is the case at

your site, you should configure the terminal server to display the required prompt and specify that it should be displayed first, to mimic the other terminal server and retain compatibility with client software in use by subscribers.

The following example shows how to configure these 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 configure these parameters to mimic another terminal server that expects users to select a service prior to 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

The MAX TNT supports token-card authentication by using a RADIUS server as the intermediary between the MAX TNT 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.

Token cards are hardware devices, typically shaped liked credit-card calculators, with an LCD display that informs users about 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 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 SafeWord, 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

The MAX TNT supports 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 does not affect the MAX TNT External-Auth profile configuration, which must still specify RADIUS as the external server.

A simple method of authenticating token-card calls

The MAX TNT can support token-card authentication from non-Ascend units by authenticating the calls in the terminal-server software using normal PAP authentication to do the challenge-response token exchanges. For example, the following RADIUS profile specifies authentication from an ACE server:

```
carlos Password = "ACE"
      User-Service = Framed-User,
      Framed-Protocol = PPP,
      Framed-Address = 10.2.3.78,
      Framed-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 with a challenge prompt (typically a Passcode prompt for ACE authentication), and uses the response to that challenge 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:

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 (described in the next section).

When users have a token card that not require a challenge-response exchange (such as ACE), you can use Ascend-Token-Immediate to simply 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 using Ascend-Token-Immediate:

```
robin Password = "ACE", Ascend-Token-Immediate = Tok-Imm-Yes
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.3.4.5,
    Framed-Netmask = 255.255.255.255
```

Authenticating token-card connections from Ascend units

Figure A-2 shows a dial-in connection to a MAX TNT on a secure network. The remote user must use a token card to gain access to the secure network.

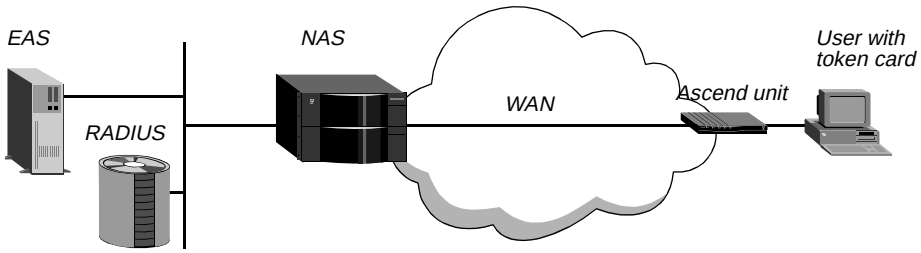


Figure A-2. Token card authentication for dial-in connections

A user with a token card initiates a connection to the MAX TNT (the Network Access Server, or 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 MAX TNT 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, for a total of up to three attempts.

As the last step in authentication, the RADIUS server sends an authentication response to the MAX TNT. If authentication is unsuccessful, the MAX TNT receives an Access-Reject packet and terminates the call. If authentication is successful, the MAX TNT receives an Access-Accept packet containing a list of Attribute-Value pairs from the user profile in the RADIUS server's database. The MAX TNT uses the Attribute-Value pairs to create the connection.

Configuring the MAX TNT as the NAS

To configure the MAX TNT to function as the 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. For details, see the *MAX TNT RADIUS Guide*.

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 Ascend unit in password mode by using 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

The first step in setting up RADIUS for token card authentication is to make sure the server is running the most recent version of the Ascend RADIUS daemon. We strongly recommend that you download and install the latest version of the RADIUS daemon and its dictionary file from `ftp.ascend.com`. The RADIUS archive is located within the Software Releases directory.

The Ascend RADIUS daemon 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 MAX TNT must interrupt the session to challenge the user for another token.

With PAP-TOKEN, the caller's Send-Password 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 (via PAP), but because it is used only once, this may not considered a serious security risk.

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-3 shows a PC user with a SecurID token card dialing into the MAX TNT through a Pipeline unit. The EAS is a UNIX host running RADIUS and Security Dynamics ACE software.

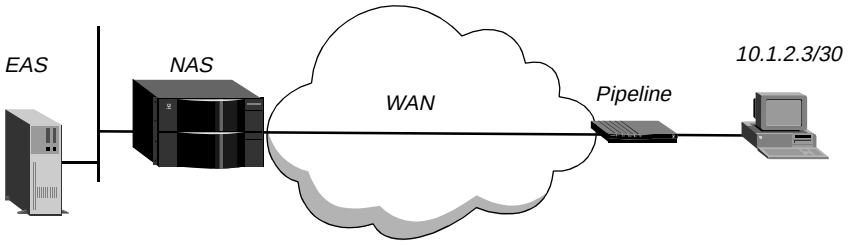


Figure A-3. PAP-TOKEN with an ACE server

When the EAS sends an Access-Challenge packet back through the RADIUS server and the MAX TNT 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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.1.2.3,
    Framed-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. The base channel is authenticated using PAP-TOKEN. If channels are added to the call, they are authenticated using CHAP and the caller's Aux Send PW. The RADIUS server informs the NAS of the Aux Send PW to expect for subsequent channels by sending the value as Ascend-Receive-Secret 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:

Attribute	Value
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the Aux Send PW 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 for the caller, and uses it to create the digest sent to the RADIUS server via CHAP.

Figure A-4 shows a user with a token card dialing into the MAX TNT 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.

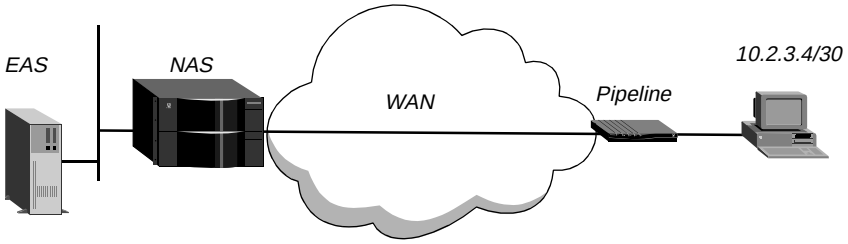


Figure A-4. PAP-TOKEN-CHAP with a Safeword server

Following is a sample user profile:

```
Raoul Password = "SAFEWORD"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.2.3.4,
    Framed-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.

Note: When you start the RADIUS daemon, you must specify the `-c` option to enable cache-token authentication.

In addition to the requirement that the Password attribute must specify ACE or SAFEWORD, CACHE-TOKEN authentication uses the following attribute-value pairs:

Attribute	Value
Ascend-Receive-Secret (215)	Text string of up to 20 characters, which must match the Send PW 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 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. 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 attribute Ascend-Token-Expiry is reached. 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 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-5 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.

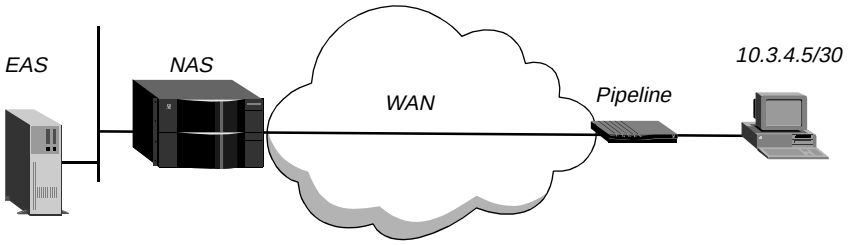


Figure A-5. CACHE-TOKEN with a SafeWord server

Following is a RADIUS user profile for the dial-in user:

```
Aydin Password="SAFEWORD", Ascend-Token-Expiry=30, Ascend-Token-Idle=10,
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 10.3.4.5,
    Framed-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 dial in using a single profile that specifies the remote router name. To dial in, a user must enter the token in this 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-6, multiple remote users are connected to an Ascend unit named Alameda.

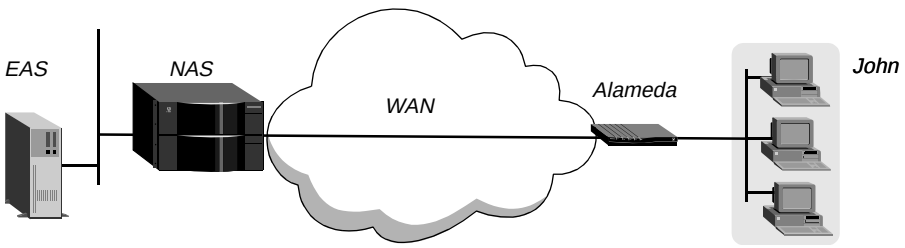


Figure A-6. SACE authentication for remote router users

The user profile specifies the system name of the Pipeline and the password for ACE authentication. For example:

```
Alameda Password = "ACE"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.72.138.1,
    Framed-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 Controller) initiating a tunnel request must supply a password before the Home Agent (or L2TP Network Server) 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 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 mobile-client Connection profile must include the same value in the Password parameter of the Tunnel-Options subprofile. 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",
    User-Service = Framed-User
    Tunnel-Type = ATMP,
    Tunnel-Server-Endpoint = "3.3.3.3:8877",
    Tunnel-Password = "tunnel-password"
```

The Ascend RADIUS daemon encrypts 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 Tunnel-Password and the RADIUS daemon does not encrypt the password, tunnel authentication will fail.

If the mobile-client profile uses the Ascend-Home-Agent-Password (184) attribute to specify

the password instead, the RADIUS daemon performs no encryption before sending the password to the Home Agent. This may be required if you are using a RADIUS server that does not encrypt Tunnel-Password.

Note: Unless you are using a RADIUS daemon 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 using 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 MAX TNT), you can specify a single shared secret for authenticating all locally configured tunnels. The following commands configure a shared-secret once in the 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 mobile clients are authenticated by the LAC using RADIUS, the clients' RADIUS profiles can specify a shared secret by using the Tunnel-Password (69) attribute.

Note: Tunnel-Password must be encrypted by the RADIUS daemon, or tunnel authentication will fail. Both the current Ascend RADIUS daemon and Ascend Access Control encrypt the attribute properly.

The following profile authenticates the tunnel in the calling client's RADIUS profile:

```
l2tp-client Password = "my-password"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.50.1.1,
    Framed-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 Dialout-Framed-User setting for User-Service. For example:

```
lns-sys.domain.org Password = "", User-Service = Dialout-Framed-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 above, it uses the Tunnel-Password value to authenticate the tunnel.

Note: The password in the pseudo-user profile must be null (""). Because this represents a security risk, *the profile must set the Dialout-Framed-User setting.*

Pre-authentication (CLID or DNIS)

Calling Line ID (CLID) is the phone number of a calling device. You can use CLID for authentication only where 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 CLID to protect against the situation where an unauthorized user obtains the name, password, and IP address of an authorized user, and calls in from another location.

Dial Number Information Service (DNIS) is the called-party number, which is an Information Element of the Q.931 ISDN signaling protocol. It is the phone number the remote device calls to connect to the MAX TNT, but without a trunk group or dialing prefix specification. When the profile requires called-number authentication, the number called must match a phone number in a local Connection profile or RADIUS user profile.

CLID or DNIS verification occurs before the MAX TNT accepts a call and begins the process of authenticating a password.

Configuring the MAX TNT to extract and use call information

To enable the MAX TNT to extract and use CLID or DNIS information, set the CLID-Auth-Mode parameter in the Answer-Defaults profile. For example, the following commands specify that the MAX TNT uses CLID information if it is available, but goes on to attempt password authentication of the call if CLID authentication fails for any reason:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set clid-auth-mode = clid-prefer

admin> write
ANSWER-DEFAULTS written
```

When CLID-Auth-Mode is set to 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-25).

If you use a Prefer setting, the system pre-authenticates by means of the CLID or DNIS number if the number present in the call. After pre-authentication, the call can 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 telco switch, the call is not terminated. In effect, if the number is present, the system behaves as if CLID-Auth-Mode were set to Require. If the number is not present, it behaves as if CLID-Auth-Mode were set to Ignore.

If you use a Require setting, the call must be pre-authenticated or it fails. If the CLID or DNIS number matches a profile, the call can 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.

For CLID only, the Fallback setting means that CLID is required, but only if the call is authenticated via 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	Enables/disables sending the User Busy (17) disconnect cause when CLID or DNIS authentication fails. The default No causes the system to send the Normal Call Clearing (decimal 16) cause.
Auth-ID-Timeout-Return-Busy	Enables/disables sending the User Busy (17) disconnect cause when CLID or DNIS authentication times out. The default 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 MAX TNT can compare that number to the one presented by the telco 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	Phone number of the calling device. When a user dials in using MP or MP+, the calling device might have more than one phone number associated with it. In that case, the CLID is the phone 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 phone number the remote device calls to connect to the MAX TNT, 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:

Attribute	Value
Caller-Id (31)	Phone number of the calling device (a string value). When a user dials in using MP or MP+, the calling device might have more than one phone number associated with it. In that case, the CLID is the phone number associated with the channel in use.
Client-Port-DNIS (30)	Called-party number, which is an Information Element of the Q.931 ISDN signaling protocol. It is the phone number the remote device calls to connect to the MAX TNT, but without a trunk group or dialing prefix specification. (A string value.)
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 is known, it is included in the Access-Request to the RADIUS server. If the Caller-Id 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 is rejected if the Caller-Id presented to the server does not match the value of the Caller-Id attribute.

```
emma Password = "test", Caller-Id = "5551213"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

The example immediately above is a normal user profile, but the user is limited to a specific phone number. This 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 phone lines, only one user will be able to connect. It is normally used for security, to prevent a system admin or other important account from be abused.

Examples where 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 MAX TNT sends an Access-Request to the RADIUS server with the Caller-Id number as the User-Name, Ascend-CLID as the password, and a User-Service of Dialout-Framed-User. If it finds a matching RADIUS user entry, such as the one shown below, the call is authenticated and can immediately begin the configured service:

```
5551234 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Not-Require-Auth
```

If no matching entry is found, then the Access-Reject 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", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5551235 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

edgar Password = "test"
    User-Service = 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"
    User-Service = 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 immediately above, or it can be any other kind of valid user profile. For example, it can specify token-card authentication or UNIX password authentication.

Examples where 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 MAX TNT sends an Access-Request to the RADIUS server with the Client-Port-DNIS number as the User-Name, Ascend-DNIS as the password, and a User-Service of Dialout-Framed-User. If it finds a matching RADIUS user entry, such as the one shown below, the call is authenticated and can immediately begin the configured service:

```
1212 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Not-Require-Auth
```

If no matching entry is found, then the Access-Reject 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", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

1217 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

edgar Password = "test"
    User-Service = 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"
    User-Service = 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 immediately above, or it can be any other kind of valid user profile. For example, it can specify token-card authentication or UNIX password authentication.

Examples where CLID is required

When CLID-Auth-Mode is set to CLID-Require, pre-authentication of the phone 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 MAX TNT 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 phone number that does not have an Ascend-CLID entry, the MAX TNT 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 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 clid = 5551212

admin> write
CONNECTION/aydin written
```

The following RADIUS entries identify all acceptable calling line IDs:

```
5551212 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5551213 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5551214 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5551215 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5551216 Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth
```

When CLID is required, a call received from any other number is rejected. Because additional authentication is required, each call also requires its own user profile, which may or may 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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

Examples where DNIS is required

When CLID-Auth-Mode is set to DNIS-Require, pre-authentication of the phone 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 MAX TNT 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 MAX TNT 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 CLID is required:

```
1234 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

2345 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

3456 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

4567 Password = "Ascend-DNIS", User-Service = Dialout-Framed-User
    Ascend-Require-Auth = Require-Auth

5678 Password = "Ascend-DNIS", User-Service = Dialout-Framed-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 may or may not limit that particular user to one caller ID. The following example enables the user to call in on any of the specified DNIS numbers:

```
aydin Password = "test"
    User-Service = 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"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

Callback after authentication

Companies use Callback for a variety of reasons, such as savings on phone charges, but the primary use is for security: to ensure that the connection is made with a known phone number. Hanging up and calling back adds a level of certainty that the connection is with a trusted user, especially because the MAX TNT does so immediately after authentication (or pre-authentication using CLID).

Settings in a Connection profile

Following are the parameters (shown with sample settings) that are used for Callback in a Connection profile:

```
[in CONNECTION/incoming]
dial-number = 95551212
```

```
[in CONNECTION/incoming:ppp-options]
send-password = test
```

```
[in CONNECTION/incoming:telco-options]
answer-originate = ans-and-orig
callback = yes
```

Parameter	Specifies
Dial-Number	Phone number the MAX TNT dials to call back the far end.
Send-Password	Password sent to the far end for authenticating a dial-out call.
Answer-Originate	Enables or restricts the ability to both answer and originate calls using this profile.
Callback	Enables/disables callback. If set to Yes, the system hangs up as soon as authentication is complete and immediately calls back the far end.

Settings in RADIUS

Because the connection is initiated by the caller, the system does not need an explicit dial-out profile or a method of locating the dial-out profile (such as an IP route). All the necessary information for dialing back to the caller is present in the user profile.

Attribute	Value
Ascend-Callback (246)	Enables/disables callback. Callback-No (0) is the default. The other value is Callback-Yes (1).
Ascend-Dial-Number (227)	Phone number the MAX TNT dials to reach the far end.
Ascend-Send-Secret (214)	Password sent to the far end for authenticating a dial-out call. If the RADIUS server does not support Ascend-Send-Secret, use Ascend-Send-Passwd (232). For details, see “Shared secrets and secure exchanges” on page A-5.

Examples of callback after CLID authentication

The following commands define a Connection profile that pre-authenticates using CLID 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",
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.10.11.12,
    Ascend-Dial-Number = "95551212",
    Ascend-Send-Auth = Send-Auth-PAP,
    Ascend-Send-Secret = "test",
    Ascend-Callback = Callback-Yes
```

Examples of 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"
    User-Service = Framed-User,
```

```
Framed-Protocol = PPP,
Framed-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

Introduction B-1

Authorizing immediate mode login service B-2

Authorizing menu mode access B-4

Authorizing terminal-mode logins B-9

Authorizing SNMP management access B-14

Introduction

Authorization procedures define what a user may 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 into 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:

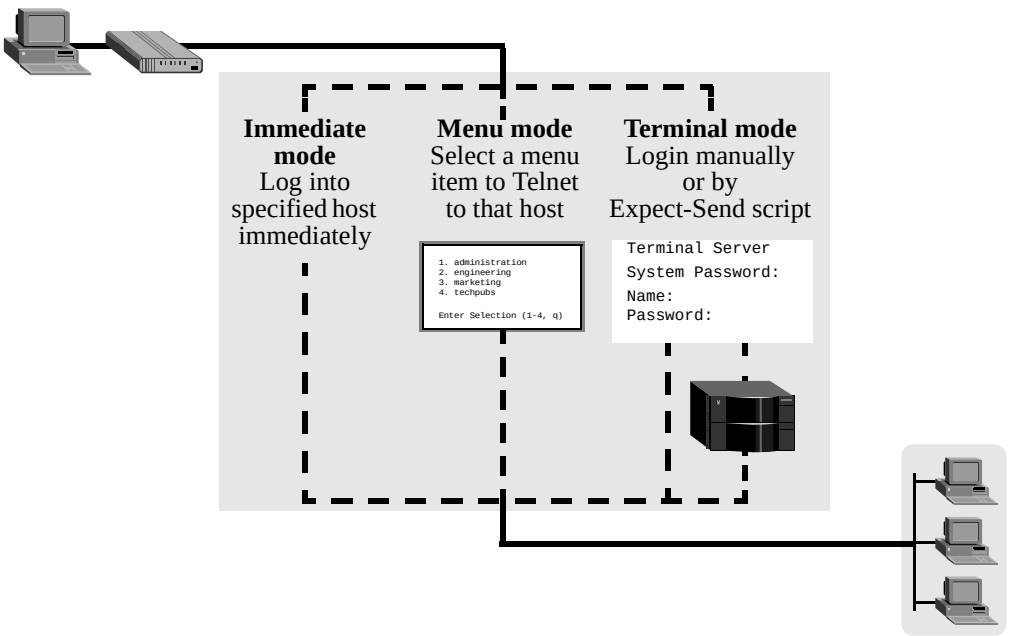


Figure B-1. Terminal-server access modes

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, administrators 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	Enables/disables immediate mode, and specifies the service to use for logging into the specified host. The default None disables immediate mode Other values are Telnet, Raw-TCP, and Rlogin.
Telnet-Host-Auth	Enables/disables handling of async PPP calls in immediate more. If set to No, async PPP calls fail. If set to Yes, the terminal server directs async 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 async 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 on that host.

If the incoming call uses PPP encapsulation, the normal course of events is for the MAX TNT is to authenticate the call by means of PAP or CHAP and then use the router software to establish an async 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 2-21.

Using RADIUS profiles

RADIUS uses the following attribute-value pairs to specify an immediate-mode login:

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.
User-Service (6)	Specifies whether the link can use framed or unframed services. Valid values are Login-User (1), Framed-User (2), and Dialout-Framed-User (5).

If you set the Login-Service to Telnet or TCP-Clear, and you do not specify a value for the Login-Host attribute, the MAX TNT 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 MAX TNT drops the call. If Auth-TS-Secure is set to No, the MAX TNT allows the caller access to the terminal-server interface. For detailed information about the Auth-TS-Secure parameter, see the *MAX TNT Reference Guide*.

Following is a RADIUS profile that specifies an immediate Telnet session for the user:

```
joel Password = "localpw"
    User-Service = 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	Enables/disables menu mode after authentication. The Menu command in terminal-mode can invoke menu mode regardless of this setting.
Toggle-Screen	Enables/disables toggling from menu mode to terminal-mode. If 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	Enables/disables retrieving 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 of up to 4 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 this format:

`initial-banner-`*`name-N`* `Password = "ascend", User-Service = Dialout-Framed-User`

The optional name argument is the MAX TNT 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 MAX TNT stops retrieving the profiles when it encounters the gap in sequence.

The following attribute-value pairs can be used to define an initial-banner pseudo-user profile:

Attribute	Value
Ascend-Host-Info (252)	IP addresses and text description (up to 31 characters) of up to 10 hosts. The value uses the following format: "*ip-address text*" The RADIUS 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.
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 should be 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:

```
initial-banner-tnt01Password="ascend",User-Service=Dialout-Framed-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 MAX TNT authenticates the user's login name and password, and then displays a text-based menu such as the one shown in Figure B-2:

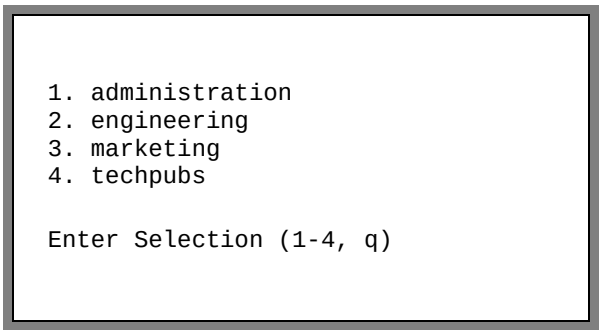


Figure B-2. Terminal-server menu mode

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 to choose, along with an input prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile to give the user a custom menu of items from which to choose. 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:

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, in the following format: "*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 MAX TNT 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", User-Service = 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:"
```

```
1. Display IP Stats     3. Telnet to Ken's unit
2. Ping server          4. Display ARP Table.
                Option:
```

Figure B-3. Customized login screen for RADIUS user

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 further, to display a unique string (a match pattern) instead of a number for each option, add the match pattern Ascend-Menu-Item definitions. For example, the following profile defines the custom login screen shown in Figure B-4:

```
Emma Password = "m2dan", User-Service = 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:"
```

```
ip=Display IP Stats      t=Telnet to Ken's unit
p=Ping server            dsp=Display ARP Table.
                Option:
```

Figure B-4. A customize login screen with match patterns

Note: Do not combine numeric menu selections with pattern matching. The first Ascend-Menu-Item attribute determines whether the screen displays numbered selections or patterns.

Extended example of RADIUS and menu mode

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.

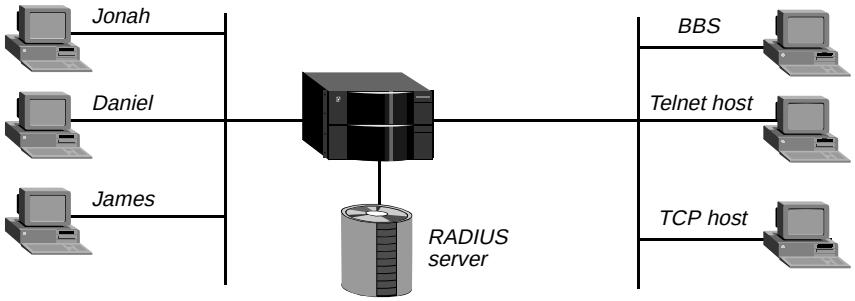


Figure B-5. An extended terminal-server example

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 each line 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:

```
Welcome to ABCNet's Terminal Server
1. BBS          3. Start SLIP
2. Start PPP    4. Start CSLIP
Press q to Quit>>
```

Figure B-6. Menu displayed when DEFAULT profile is used

Instead of using the Default profile, you can configure individual profiles to restrict users from 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"
    User-Service = 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"
    User-Service = 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 those commands are provided in immediate mode 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, see “Authorizing immediate mode login service” on page B-2.

Authorizing use of the commands

The following parameters (shown with default settings) enable 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	Enables/disables the TCP command, which initiates a TCP session to a specified host. The command is disabled by default.
Rlogin	Enables/disables the Rlogin command, which initiates a remote login session to a specified host. The command is disabled by default.
Telnet	Enables/disables 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	The highest Rlogin source port. Its value must be between 128 and 1023, and should be greater than or equal to the value of Min-Source-Port. The default value is 1023.
Min-Source-Port	The lowest Rlogin source port. Its value must be between 128 and 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 between 512 and 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 when no ports are available or when the configured range is incorrect. 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. Users can modify some of the default values on a per-session basis when they invoke 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 for the Telnet session, such as the vt100.
Clear-Call	Enables/disables termination of the connection when a user terminates a Telnet session.
Buffer-Chars	Enables/disables holding 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	Enables/disables 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 unknown command strings as the name of a host for a Telnet session.
Local-Echo	Enables/disables echoing of characters locally. Users can change the echo setting within an individual Telnet session.

Following is an example that 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 MAX TNT does not support a direct SLIP dial-in, because SLIP doesn't 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	Enables/disables the PPP command, which initiates a PPP session. The command is disabled by default.
SLIP	Enables/disables 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	Enables/disables direct PPP negotiation after using the PPP command. By default, the terminal server waits to receive a PPP packet before beginning PPP negotiation.
Info	Enables/disables display of an informational message when the user enters PPP mode. If set to Session-PPP, the system displays PPP Session. If set to 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	Enables/disables response to BOOTP within SLIP sessions. If set to Yes, a user who initiates a SLIP session can get an IP address from the designated IP address pool via BOOTP. If set to No, 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	Enables/disables display of an informational message when the user enters SLIP mode. If set to Basic-SLIP, a default startup message is displayed. If set to Advanced-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 into 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-9.

Authorizing SNMP management access

SNMP management software that uses the Ascend Enterprise MIB and has IP connectivity with the MAX TNT can perform administrative tasks, including reconfiguring the MAX TNT. It is important to restrict this type of access to trusted management stations. Following are the relevant 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	Enables/disables SNMP access. The default 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	Enables/disables 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 MAX TNT 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 MAX TNT 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 specifies 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

A

accounting options for sessions, 2-10
ACE authentication, A-20
address pool definitions, example, 4-54
Address Resolution Protocol (ARP). See ARP
addresses
  AppleTalk, 9-1
  broadcast, and RIP, 4-7
  broadcast, and subnets, 4-6
  DNS, and, 4-45
  dynamic, requiring acceptance, 4-31
  Ethernet ports, 4-6
  filtering on, 10-13, 10-22
  interface-independent, 4-9
  IP-in-IP, 7-11
  NetBIOS servers, 4-44
  numbered interfaces, for, 4-18
  source address checking, 4-21
  system IP, 4-30
  TCP-Clear connections, and, 2-22
  VRouters, effect on, 4-67
  see also IP addresses, IPX addresses
  see also pools
adjacencies, OSPF, 5-4
ADSL. See *MAX TNT Hardware Installation Guide*
algorithms
  line utilization, calculating, 2-18
  link-state routing, 5-7
  shortest-path tree (Dijkstra), 5-8
analog calls, MP and, 2-16
analog modems. See modems
Answer-Defaults profile
  ARA guest access, and, 9-4
  default settings, 2-4
  filters, RADIUS, 10-27
  how system answers calls, 2-3
  incoming calls, and, 2-2, 2-3
  IPX Peer-Mode, 8-9
  PPP authentication, requiring, 2-4
  RADIUS defaults, 2-4
  V.120, 2-4
AppleTalk
  addresses, 9-1
  dial-in pool for clients, 9-1
  IP, and, 9-8
  network ranges, 9-1
  nonseed router, defined, 9-3
  seed router, defined, 9-2
  shelf controller, requirement, 9-1
  zone list, explained, 9-3
AppleTalk Remote Access (ARA). See ARA
AppleTalk, configuration examples, 9-7
ARA
  addresses, AppleTalk, 9-1
  example configuration, 9-6
  guest access, allowing, 9-4
  IP, and, 9-8
  maximum connect time, 9-5
  shelf controller, requirement, 9-1
Area Border Router (ABR) capability, 5-2
areas, OSPF, 5-6
ARP
  proxy mode on LAN, 4-8
  virtual interfaces, with, 4-9
ARP, proxy on Ethernet, 4-8
Ascend extensions to IPX, 8-3
Ascend Signaling Gateway (ASG). See *MAX TNT Hardware Installation Guide*
Ascend subnet notation, 4-5
Ascend Tunnel Management Protocol (ATMP). See ATMP
asynchronous connections
  described, 2-1
  expect-send login scripts, A-10
  framed sessions, A-10
  multichannel connect speeds, 2-16
  terminal server and, 2-5
Atalk-Global profile, 9-1
Atalk-Interface profile, 9-2
ATM. See also *MAX TNT Hardware Installation Guide*
ATM-Frame Relay circuit, example, 3-36
ATM-Frame Relay circuits, 3-32
ATMP
  FA-to-HA connection, 6-11
  Gateway Home Agent, 6-22
  Home Agent
    Gateway and Router, compared, 6-17
    password, A-21

ATMP *continued*
timer for idle tunnels, 6-18
home network name, 6-11
Home Router, 6-20
IPX, 6-29
link to home network, 6-19
local tunnel, 6-25
related RFC, 6-1
resets required, 6-2
resiliency, Primary and Secondary Home Agents, 6-20
RIP responses for mobile clients, 6-20
Router Home Agent, 6-23
routes between agents, 6-3
tunnel components, 6-1
tunnel requests, 6-10
tunnel retry limits, 6-4
ATMP examples, 6-12
ATMP profile
Foreign Agent, 6-7
Home Agent, 6-16, A-21
Home-and-Foreign Agent, 6-26
ATMP tunnel to GRF switch, 6-15
authentication
CACHE-TOKEN, A-19
callback, A-30
called number, A-24
CHAP, A-7
choosing method, A-1
CLID, A-23
encryption on RADIUS server, A-6
expect-send scripts from modems, A-10
external, A-13
external, related RFCs, 1-5
global mode for direct-access, 2-39
L2TP tunnels, 7-4
LAN Manager, for, 2-12
MS-CHAP, A-7
OSPF, MD5 (RFC 2178), 5-3
PAP, A-7
PAP-TOKEN, A-16
PAP-TOKEN-CHAP, A-17
password for dial-in PPP, 2-11
password for PPP dial-out, 2-36
PPP connections, of, A-6
PPTP tunnels, 7-9
RADIUS, 2-6, 2-7, A-2
receive mode, A-6
requiring from callers, 2-4
settings in Connection profile, 2-7
system password, A-11
terminal-server security mode, B-14
third prompt, A-12
token card, A-2, A-13
tokens, how to configure, A-13
tunnel, A-21
tunnels, A-21
user security for dial-out, 2-40
using call information, A-23
Windows NT, for, 2-12
authorization
immediate mode, B-2
interactive terminal-server logins, B-9
logins to hosts, B-9
menu mode, B-2, B-4
PPP sessions, B-12
restricting access to terminal server, B-1
SLIP sessions, B-13
SNMP access to system, B-14
Telnet defaults, B-11
terminal mode, B-9
Autonomous System (AS)
Boundary Router (ASBR) capability, 5-2
defined, 5-3
Average Line Utilization (ALU). See line utilization

B

Backup Designated Router (BDR), 5-4
Backup interfaces, 2-31, 3-16
bandwidth
adding, 2-19
algorithm for calculating line utilization, 2-18
increments, 2-19
line utilization spikes and, 2-18
monitoring usage, 2-19
nailed, for Frame Relay, 3-4
RADIUS attributes for, 2-19
target utilization, 2-19
telco charges, and, 2-18
bandwidth-addition-lockout mode, 2-17
banner, A-11
base channels, 2-14
blackhole (bh0) interface, 4-3
BOOTP
enabling, 4-40
enabling BOOT-Relay, 4-42
server addresses, 4-43
SLIP sessions, for, B-13
BOOTP-Relay Agent, 4-42
Bootstrap Protocol (BOOTP). See BOOTP
broadcast address, ignoring echo requests, 4-33
buffering, TCP-Clear data, 2-21
bundling MP+ channels, 2-3

C

cacheing. See route cacheing
CACHE-TOKEN authentication, A-19
call filters, applying, 10-2, 10-29
call information, configuring security, A-23
call type for connections, 2-26
callback, A-30
called-number authentication, A-23, A-24
calls
  Answer-Defaults profile, and, 2-2
  authenticating, 2-2
  configured profiles, and, 2-2
  dial-out, configuring, 2-35
  dialout, initiating, 2-2
  multichannel, 2-3
  routing, 2-2
cards, spanning, 2-3
CCITT. See ITU-T
Challenge Handshake Authentication Protocol (CHAP). See authentication
Changes in interface-independent IP address, 4-9
channel usage
  bandwidth, 2-19
  base number of, 2-14
  maximum allowed, 2-15
  minimum for establishing session, 2-15
  multilink calls, for, 2-14
  nailed, 2-26
checksums, UDP, 4-41
circuits
  ATM-Frame Relay, 3-33
  NNI-NNI, 3-27
  UNI-NNI, 3-29
  UNI-UNI, 3-25
CLID
  defined, A-23
  L2TP tunnels, opening, 7-4
  PPTP tunnels, opening, 7-9
CLID authentication, A-23
clients
  ARA, 9-4
  Ascend units, dial-in, 2-17
  ATMP mobile clients, 6-8
  ISDN, 2-5, 2-14
  LAN Manager, 2-12, 2-37
  login, terminal server, 2-5
  Macintosh, IP software, 9-8
  Netmanage Pacer, 9-4
  NetWare, 8-3
  outdated software, and fragmentation, 6-5
  TCP applications, 2-24
  Telnet connections and, 2-38
  UNIX, 4-42
  Windows 95, 2-12
  Windows NT, 2-12, 2-37
clock, setting via SNTP, 4-43
community strings, B-14
  read-community, B-14
  read-write-community, B-14
  setting, B-15
compression
  link, in tunnels, 6-4
  link, PPP, 2-11
  MTU, and, 6-4
  PPP links, on, 2-11
  VJ headers, 4-12
Configurable dial-out timer, 2-35
Configurable Rlogin source port range, B-10
Connection profile, 2-7
  AppleTalk routing, 9-5
  ARA, 9-4
  ATM-Frame Relay circuit, 3-33
  ATMP mobile client settings, 6-8
  client DNS options, 4-50
  dial-out, 2-35
  dynamic address assignment, 4-57
  filters, applying, 10-26
  Frame Relay circuits, 3-24
  Frame Relay Direct, 3-21
  Frame Relay DLCI, 3-14
  gateway DLCI, 3-18
  IP options, 4-12
  IP-in-IP tunnel, 7-11
  IPX options, 8-7
  L2TP Network Server, to, 7-3
  modem dial-out, 2-40
  MP settings, 2-14
  MP+ settings, 2-18
  multicast forwarding, 4-63
  nailed, 2-26
  OSPF settings, 5-10
  PPP settings, 2-10
  PPTP Network Server, to, 7-8
  session management, 2-8
  TCP-Clear, 2-21
  X.75, 2-25
  see also RADIUS
connection types
  Frame Relay datalink, 3-6
conventions, documentation, 1-6
costs, OSPF, 5-5

D

data filters, applying, 10-2
datalink. See link operations, Frame Relay

DBA, 2-17
  algorithm for calculating line utilization, 2-18
  decrements, 2-19
  increments, 2-19
  monitoring bandwidth usage, 2-19
  persistence of utilization rate, 2-19
  RADIUS attributes, 2-19
  target utilization, 2-19
  time period for calculating line utilization, 2-19
DDP-IP tunneling, 9-9
default RADIUS profile, 2-4
default route
  client-specific, defining, 4-21
  example configuration, 4-26
  example of, 4-26
  how used, 4-23
  interface table, in, 4-2
  multipath, 4-28
  protecting from updates, 4-37
default zone, AppleTalk, 9-3
denial-of-service attacks, 4-10
Designated Router (DR), 5-4
dial query, IPX, 8-3, 8-9
dial-in calls, 2-5
  Answer-Defaults profile, and, 2-3
  authenticating, 2-4
  MP+, 2-26, 2-29
  passwords, 2-36
  PPP, 2-36
  TCP-Clear, B-3
dial-in connections, examples, 2-10
dial-out calls, how initiated, 2-2
dial-out profiles, RADIUS, 2-34
dial-out timer, 2-35
dial-out, example, 2-34
Dijkstra algorithm, OSPF, 5-8
direct routes, 4-2
direct-access dialout
  configuring, 2-38
  example with global password, 2-39
  example with user password, 2-40
  passwords for, 2-39
  security, 2-39
directed broadcasts, disabling, 4-10
DLCI 1023, LMI, 3-8
DLCI interface, 3-14
DNIS
  defined, A-23
  L2TP tunnels, opening, 7-4
  PPTP tunnels, authentication, 7-10
  PPTP tunnels, opening, 7-9
DNIS authentication
  described, A-23, A-24
DNS
  auto-update, 4-48
  client servers, 4-49
  client servers, connection-specific, 4-51
  client servers, system-wide, 4-50
  list attempt, 4-45
  local servers, 4-44
  local table in RAM, configuring, 4-46
  local table, example of, 4-47
  TCP-Clear connections, and, 2-22
DNS list, 4-45
DNS local table, example, 4-46
DNS servers, example configuration, 4-50
documentation conventions, 1-6
Domain Name System (DNS). See DNS
Dynamic Bandwidth Allocation (DBA). See DBA

E

E1, E3. See *MAX TNT Hardware Installation Guide*
Echo requests, ignoring broadcast, 4-33
encapsulation protocols, 2-1
  ARA, 9-4
  ATM-Frame-Relay-Circuit, 3-33
  Framed-Protocol in RADIUS, 2-11
  Frame-Relay-Circuit, 3-25
  GRE, 6-1
  IP-in-IP, 7-11
  MP, 2-14
  MP+, 2-17
  PPP, 2-11
encryption, password, A-2
End-of-Packet pattern, 2-22
Ethernet interface
  destination address, soft, 4-9
  disabling directed broadcasts, 4-10
  filters, applying, 10-30
  interface table, in, 4-3
  IP configuration, 4-7
  management-only, 4-11
  multiple IP addresses for, 4-9
  RIP, and, 4-8
  see also *MAX TNT Hardware Installation Guide*
  shelf-controller, IPX on, 8-5
  virtual IP interfaces, 4-9
  see also LAN IP interfaces
  see also IPX interfaces
expect-send login scripts, A-10
external authentication
  methods, 2-6
  servers, 2-6, A-13
External-Auth profile, 2-6

F

filter example, 10-10
Filter profile
  direction, A-8, A-24, A-25, B-13
  forwarding action, 10-6
  generic, 10-7
  IP, 10-11
  IPX, 10-21
  route, 10-24
  TOS, 10-17
  traffic, direction filtered, 10-5
  type-of-service, 10-17
Filter-ID, RADIUS, 10-27
filters
  call filter, applying, 10-2, 10-29
  comparison success, defined, 10-3
  data filter, applying, 10-2
  forwarding action (IP, IPX, generic), 10-6
  how packets are processed, 10-3
  IPX SAP, 8-15
  persistence, 10-26
  related RFCs, 1-5
  session management, applying for, 10-29
  specifications in Connection profile, 2-7
  TOS filter, applying, 10-29
  traffic direction to monitor, 10-5
  types of, 10-1
  see also generic, IP, TOS, IPX, route filters
finger queries, 4-42
Foreign Agent, ATMP, 6-10
Foreign agent. See ATMP
fragmentation
  ATMP, preventing between agents, 6-5
  forcing clients to perform, 6-5
  outdated client software, and, 6-5
  prefragmentation in client software, 6-6
  tunnels, and, 6-5
Frame Relay
  ATM-FR circuits, 3-32
  backup interfaces, 3-16
  circuit between NNI interfaces, 3-27
  circuit between UNI interfaces, 3-26
  circuit between UNI/NNI interfaces, 3-29
  circuit-switching options, 3-24
  DLCI interface, 3-14
  link management protocols, 3-7
  link operation settings, 3-7
  nailed bandwidth requirement, 3-4
  NNI interface, 3-13
  RADIUS attributes, 3-8
  UNI-DCE link interface, 3-11
  UNI-DTE link interface, 3-10
Frame Relay circuits, examples, 3-25
Frame Relay concentrator, described, 3-2
Frame Relay Direct, example, 3-22
Frame Relay DLCI interface, example, 3-15
Frame Relay gateway, example, 3-20
Frame Relay link interface, examples, 3-10
Frame Relay profile, 3-6
Frame Relay switch operations, 3-3
Framed-Protocol sessions, 2-3
Frameline. See *MAX TNT Hardware Installation Guide*
frames, IPX types, 8-6
frdlink, RADIUS, 3-8

G

Gateway Home Agent, ATMP, 6-22
generic filters
  action (forward or drop), 10-3
  applying to interfaces, 10-26
  bytes to test, 10-9
  example of, 10-10
  masking value before comparison, 10-9
  offset to packet contents, 10-8
  packet contents, how compared to, 10-3
Generic Routing Encapsulation (GRE), 6-1
Global mode authentication for modem dialouts, 2-39
global-pools, RADIUS, 4-53
Greenwich Mean Time (GMT)., 4-43
GRF switch, connectivity via ATMP, 6-15
GRF switch, fragmentation issues, 6-5
groups
  IGMP, 4-59, 4-64
  nailed channels, of, 2-27
guest access, ARA connections, 9-4

H

heartbeat monitoring, example, 4-61
hello packets, OSPF, 5-5, 5-10
hint zone, 9-3
Home Agent Router, 6-23
Home Agent. See ATMP
home servers, IPX proxy, 8-10
host
  directing inbound async calls to, B-2
  IP-Direct connection to local, 4-19
  matching, DNS, 4-47
  names in Terminal-Server menu, B-6
  TCP-Clear connection to local, 2-24
host route, example, 4-17

host routes
described, 4-6
summarized in advertisements, 4-55
suppressing advertisement, 4-38

I

ICMP
ignoring broadcast echo, 4-33
ignoring redirects, 4-33
idle timers
ATMP tunnels, 6-18
how used, 2-8
RADIUS, in, 2-9
IDSL. See *MAX TNT Hardware Installation Guide*
IGMP
delay for clearing groups, 4-64
multicast heartbeat monitoring, 4-60
multicast trace packets, 4-58
version-1 or version-2, 4-58
immediate mode, B-2
authorizing access, B-2
PPP and, B-2
incoming calls
Answer-Defaults profile, and, 2-3
answering, 2-26, 2-29
authenticating, 2-4
MP+, 2-26, 2-29
passwords, 2-36
PPP, 2-36
interface-independent IP address, setting, 4-9
interfaces
backups for nailed connections, 3-16
blackhole (bh0), 4-3
DLCI, 3-14
Frame Relay circuits, 3-24
IPX, LAN, 8-5
IPX, WAN, 8-7
local, 4-2
loopback (lo0), 4-3
mcast, 4-2
multicast client, 4-64
numbered, example of, 4-18
reject (rj0), 4-3
soft IP (sip0), 4-4
table of, 4-3
tunnel, 4-4
vr0_main, 4-4
VRouter, belonging to, 4-73
WAN, active, 4-4
wanabe, 4-4
Internet Control Management Protocol (ICMP). See ICMP
Internet Group Membership Protocol (IGMP). see IGMP, multicast forwarding
Internetwork Packet Exchange (IPX). See IPX
IP addresses
Ascend subnet notation, 4-5
dynamic assignment, example, 4-57
far end routers, of, 4-16
filtering on, 10-13
interface-independent, 4-9
LAN interface, for, 4-7
network isolation, and, 6-6
numbered interfaces, 4-18
soft interface, 4-9
source address checking, 4-21
spoofing local, preventing, 10-14
system address, 4-30
virtual interfaces, and, 4-9
IP direct, example, 4-19
IP filters
action (forward or drop), 10-4
applying to interface, 10-28
applying to interfaces, 10-26
destination address filtering, 10-13
example, preventing address spoofing, 10-14
example, security, 10-15
packet contents, how compared to, 10-3
port number filtering, 10-14
security uses, 10-15
source address filtering, 10-13
IP interface table, displaying, 4-3, 4-70
IP routing table
convergence, RIP, 5-2
creation of, 4-1
default route, 4-2
direct routes, 4-2
display of, 4-2
fields, explained, 4-2
OSPF inter-router communications, 4-3
preferences, 4-34
route to local interface, 4-2
route to mcast interface, 4-2
routes, dynamic, 4-2
routes, static, 4-1
VRouter, for, 4-70
VRouters, addresses, and, 4-67
see also link state database
IP routing, example, 4-16
IP-Global profile, 4-30
address pools, 4-51
DNS client options, 4-49
DNS options, 4-44
multicast forwarding, 4-58
OSPF, 5-14
protocol options, 4-39
RIP options, 4-35
route cache options, 4-38

router security options, 4-31
system address, 4-30
system routing options, 4-33
IP-in-IP
current implementation, 7-11
MTU size, 7-11
IP-in-IP, example, 7-12
IP-Interface profile, 4-6
examples, 4-7
multicast forwarding, 4-63
OSPF, 5-10
route filters, 10-26
settings, 4-7
slot addresses, 4-6
IP-Route profile
examples, 4-26
multipath routes, 4-28
OSPF, 5-16
settings, 4-23
IPX
Ascend extensions for WAN routing, 8-2
dialing connections for SAP queries, 8-3
NetWare client software, 8-3
over ATMP, 6-29
socket numbers, 8-15
static routes, 8-12
virtual network for dial-in clients, 8-3, 8-4
see also LAN IPX interfaces, WAN IPX interfaces
IPX addresses
filtering on, 10-22
for dial-in NetWare clients, 8-4
LAN interface, for, 8-6
NetWare servers, of, 8-14
IPX filters
action (forward or drop), 10-5
applying to interfaces, 10-26
destination address filtering, 10-22
examples of, 10-23
packet contents, how compared to, 10-4
socket number filtering, 10-23
source address filtering, 10-22
IPX over ATMP, 6-29
IPX RIP
between Ascend units, 8-1
static IPX routes, 8-13
WAN interfaces, on, 8-9
IPX routing, example, 8-10
IPX SAP
dial query, 8-3
filter, examples, 8-17
response packets, filtering services, 8-15
SAP table, filtering services, 8-15
SAP table, how used, 8-1
IPX static routes, example, 8-15
IPX, shelf-controller requirement, 8-5
IPX-Global profile, 8-4
IPX-Interface profile, 8-5
IPX-Route profile, 8-13
ipxroute, RADIUS, 8-11
IPX-SAP-Filter profile, 8-16
IPXWAN, support for negotiation, 8-2
ISDN modems
described, 2-4
terminal server and, 2-5
ITU-T recommendations, 1-5

L

L2TP
Access Concentrator (LAC) capabililty, 7-1
links, control and data, 7-1
Network Server (LNS), connection to, 7-3
tunnel authentication
CLID or DNIS, 7-4
PPP, 7-5
tunnel to LNS, 7-2
L2TP, example, 7-3
L2-Tunnel-Global profile
L2TP, 7-2
PPTP, 7-7
LAN AppleTalk interfaces
default zone, 9-3
hint zone, 9-3
nonseed router, configuring, 9-3
seed router, configuring, 9-2
ZipGetNetInfo request for configuration, 9-3
LAN IP interfaces
directed broadcasts, disabling, 4-10
filtering RIP packets, 10-30
IP-Interface settings, 4-6
management-only, 4-11
MBONE, 4-61
multicast clients, 4-65
OSPF options, 5-9
physical address, 4-6
proxy ARP, enabling, 4-8
RIP, enabling, 4-8
route filters, 10-30
virtual, 4-9
OSPF, and, 4-9, 5-2
proxy ARP, and, 4-9
VRouter, assigning to, 4-73
LAN IPX interfaces
frame type, 8-6
IPX-Interface settings, 8-5
overview, 8-5
routing, spoofing, and, 8-6
shelf-controller Ethernet requirement, 8-5

LAN IPX interfaces *continued*
Type 20 packets, 8-6
LAN OSPF interfaces
area number and type, 5-6, 5-10
ASE handling, 5-11
authentication, 5-3, 5-11
costs, 5-5, 5-11
designated router priority, 5-4, 5-11
intervals for hello packets, 5-10
LSA handling, 5-11
Layer 2 Tunneling Protocol (L2TP). See L2TP
leased lines, connections on, 2-26
line utilization
dynamic algorithm for calculating, 2-18
RADIUS attributes, 2-19
spikes, 2-18
target utilization, and, 2-19
time period for calculating, 2-19
link compression, 2-11
Link management on DLCI 1023, 3-8
link management protocols, 3-7
link operations, Frame Relay, 3-6
Link State Advertisements (LSAs). See link-state database
link-quality monitoring
described, 2-11
magic number support, 2-12
PPP connections, for, 2-12
link-state database
adjacencies, and, 5-4
areas, and, 5-6
ASEs, 5-2
building, 5-7
commands for displaying, 5-3
creating, 5-7
described, 5-2
example, 5-8
updates, 5-7
local address, numbered interface, 4-18
local interface, 4-4
login prompt, A-11
login scripts, A-10
logins
authorizing interactive, B-9
Telnet, 4-32
terminal server, B-1, B-9
timeout, A-12
Login-Service sessions, 2-3, 2-5
loopback (lo0) interface, 4-3
LQM magic number support, 2-12
LSA retransmit interval, 5-11
LSA transit delay, 5-11

M

Management-only Ethernet interface, 4-11
maximum call duration, 2-8
maximum channels, 2-15
Maximum Receive Unit (MRU), 2-11, 6-5
Maximum Transmission Unit (MTU), 6-4, 7-11
MBONE interfaces
examples, 4-62
see also multicast forwarding
MD5 authentication for OSPF (RFC 2178), 5-3
menu mode
authorizing access, B-4
configuring menu text, B-5
described, B-2
metrics, 4-12, 5-1, 5-5
Microsoft extension of CHAP (MS-CHAP). See authentication
minimum channels, 2-15
modem dial-out connections, 2-38
modems
direct access dialout, 2-39
expect-send scripts and authentication, A-10
ISDN, 2-4
PPP calls, and, 2-13
recommended settings, A-10
see also *MAX TNT Hardware Installation Guide*
modes, terminal-server access
immediate, B-2
menu, B-2
security, B-14
terminal, B-9
MP
base channels, 2-14
bundling channels, 2-3
configuring, 2-14
example of, 2-15
maximum channels, 2-15
minimum channels, 2-15
number of channels to use, 2-14
RADIUS attributes, 2-15
See also PPP
MP bonding of analog calls, 2-16
MP+
adding bandwidth, 2-17
bandwidth guidelines, 2-18
bandwidth increments, 2-19
bandwidth-addition-lockout mode, 2-17
bundling channels, 2-3
configuring, 2-17
DBA, 2-18
example of nailed, 2-29
example of switched, 2-20
line utilization rate for adding bandwidth, 2-20

line utilization spikes, 2-18
monitoring bandwidth usage, 2-19
persistence of utilization rate, 2-19
RADIUS, 2-19
telco charges, 2-18
threshold for requesting bandwidth, 2-19
See also MP, PPP
MS-CHAP authentication, A-7
MS-Stac compression, 2-12
multicast backbone (MBONE), 4-58
multicast client interface, example, 4-64
multicast forwarding
global settings, 4-58
heartbeat monitoring, configuring, 4-60
IGMP group membership timeout, 4-59
limitations for VRouters, 4-72
MBONE interface, LAN, 4-61
MBONE interface, specifying, 4-61
MBONE interface, WAN, 4-61
multicast clients, LAN, 4-63
multicast clients, WAN, 4-63
rate limit, specifying for clients, 4-64
related RFCs, 1-4
route to mcast interface, 4-2
multichannel calls, spanning cards and shelves, 2-3
Multilink Protocol (MP) connections. See MP
Multilink Protocol Plus (MP+) connections. See MP+
multipath IP routes, example, 4-29
Multiple destination support for TCP-Clear, 2-21

N

nailed connections
backup interfaces for, 2-32
Connection profiles, and, 2-26
groups, and, 2-27
MP+, 2-29
RADIUS, 2-27
reloading from RADIUS, 2-27
telco settings, and, 2-26
nailed connections, example, 2-28
nailed groups, 2-27
names
DNS, 2-22
host, 2-22
login, 2-3, 2-5, 2-40
remote device, of, 2-11
NAS (Network Access Server) configuration, A-16
neighbors, OSPF, 5-5
NetBIOS
IP host addresses, and, 4-55
IPX Type 20 packets, and, 8-6
servers, specifying, 4-44
netmask. See subnet mask
NetWare, examples, 8-10
NetWare. See IPX
network alignment. see pools
network ranges, AppleTalk, 9-1
Network-to-Network (NNI), defined, 3-2
nonseed router, 9-3
numbered interfaces, 4-18
numbered interfaces, example, 4-18

O

Open Shortest Path First (OSPF). See OSPF
OSPF
ABR capability, 5-2
adjacencies, forming, 5-4
area types, 5-7
areas and ABRs, 5-6
AS defined, 5-3
ASBR calculations, 5-2
ASE options, configuring, 5-15
back designated router, 5-4
costs, configuring, 5-5
designated router, 5-4
IGP, 5-4
importing address pool routes, 5-15
inter-router communications, 4-3
LAN IP interfaces, configuring, 5-11
link-state routing algorithm, 5-7
LSA Type-5, 5-7
LSA Type-7, 5-7
MD5 authentication (RFC 2178), 5-3
neighbors, 5-5
normal areas, 5-7
not-so-stubby areas (NSSA), 5-7
related RFCs, 1-4
RIP, comparison, 5-1
RIP, importing as ASE, 5-14
routing table, how built, 5-8
static route settings, 5-16
stub areas, 5-7
third-party routes, 5-18
Type-7 LSA, configuring, 5-17
variable-length subnet mask (VLSM) support, 5-4
virtual interfaces, limitation, 5-2
OSPF and RIP, example, 5-13
OSPF ASE options, example, 5-15
OSPF costs, example, 5-18
OSPF interfaces, example, 5-12
OSPF NSSA, example, 5-18
outgoing calls
initiating, 2-2, 2-26, 2-29
passwords, 2-11

P

packet buffering
  described, 2-21
  example of, 2-24
packet filters. See filters
packet fragmentation and reassembly, 6-4
PAP authentication, described, A-7
PAP-TOKEN authentication, A-16
PAP-TOKEN-CHAP authentication
  for incoming calls, A-17
password authentication
  L2TP tunnels, opening, 7-5
  PPTP tunnels, opening, 7-10
Password Authentication Protocol (PAP). See authentication
password expiration attributes, A-4
password prompt, A-11
passwords
  ACE, A-16
  changing nonexpired, A-4
  direct-access dialout, for, 2-39
  encryption, A-2
  encryption for dial-out, A-6
  expiration (RADIUS), A-4
  Global mode for direct-access, 2-39
  PPP dial-in connections, for, 2-11
  PPP dialout connections, for, 2-36
  RADIUS, in, A-2
  SAFEWORD, A-16
  shared secrets, A-5
  specifying expiration for, A-3
  system, A-11
  TCP-Clear connections, for, 2-22
  Telnet, A-6
  Tunnel-Password, Ascend-Home-Agent-Password, and, A-21
Permanent Virtual Circuit (PVC), defined, 3-1
permconn, RADIUS, 3-14
Per-session source address checking, 4-21
Ping, ignoring broacast, 4-33
Point-to-Point Protocol (PPP). See PPP
Point-to-Point Tunneling Protocol (PPTP). See PPTP
poison dialout routes, 4-36
poison-reverse RIP policy, 4-35
pools
  addresses, dynamically assigned from, 4-56
  configuring, examples of, 4-54
  global, managed by RADIPAD, 4-52
  network alignment, rules for, 4-55
  OSPF, importing summarized, 5-15
  RADIPAD, specifying host, 4-53
  RADIUS examples, 4-54
  RADIUS, defined in, 4-52
  route to summarized, 4-56
  summarized, 4-55
  VRouter, defined for, 4-69
  VRouter, example of, 4-72
pools, RADIUS, 4-52
port caches, 4-38
ports
  destination for TCP-Clear connections, B-3
  direct-access, for, 2-38
  TCP, for modem access, 2-38
  TCP-Clear destination, 2-22, 2-23
PPP
  authentication of, B-3
  authorizing, B-12
  configuring, 2-10
  example configuration, 2-13, 2-37
  link compression, 2-11
  link-quality monitoring, 2-11, 2-12
  MRU, 2-11
  password authentication, A-6
  RADIUS attributes, 2-11
  receive password (dial-in), 2-11
  related RFCs, 1-3
  requiring authentication, 2-4
  send password (dial-out), 2-36
  synchronous, example of, 2-13
PPTP
  Access Concentrator (PAC) capability, 7-6
  data link, GRE, 7-6
  links, control and data, 7-6
  Network Server (PNS), connection to, 7-6
  tunnel authentication
    CLID or DNIS, 7-9
    PPP, 7-10
  tunnel to PNS, 7-7
precedence, type-of-service, 4-13, 4-16
preferences, 4-34
  default settings, 4-34
  RIP, 4-36
  static routes, 4-34
priority for designated routers, 5-11
private routes, 4-20
private routes (RADIUS), example, 4-29
private routes, connection-specific, 4-29
private routes, example, 4-20
private static routes in RADIUS, 4-29
profiles
  Answer-Defaults, 2-3
    authentication, requiring, 2-4
    RADIUS defaults, 2-4
    V.12 configuration, 2-4
  Atalk-Global, 9-1
  Atalk-Interface, 9-2

ATMP
  Foreign Agent, 6-7
  Home Agent, 6-16, A-21
Connection, 2-7
  AppleTalk routing, 9-5
  ARA, 9-4
  ATM-Frame Relay circuit, 3-33
  ATMP mobile clients, 6-8
  client DNS, 4-50
  dial-out, 2-35
  filters, applying, 10-26
  Frame Relay circuits, 3-24
  Frame Relay Direct, 3-21
  Frame Relay DLCI, 3-14
  gateway DLCI, 3-18
  IP options, 4-12
  IP-in-IP tunnel, 7-11
  IPX options, 8-7
  modem dial-out, 2-40
  multicast forwarding, 4-63
  nailed, 2-26
  OSPF, 5-10
  PPP, 2-11
  session management, 2-8
  TCP-Clear, 2-21
  X.75, 2-25
External-Auth, 2-6
Filter
  direction, A-8, A-24, A-25, B-13
  forwarding action, 10-6
  generic, 10-7
  IP, 10-11
  IPX, 10-21
  route, 10-24
  TOS, 10-17
Frame-Relay, 3-6
IP-Global, 4-30
  address pools, 4-51
  DNS client options, 4-49
  DNS options, 4-44
  multicast forwarding, 4-58
  OSPF, 5-14
  protocol options, 4-39
  RIP options, 4-35
  route cache options, 4-38
  router security options, 4-31
  system address, 4-30
  system routing options, 4-33
IP-Interface, 4-6, 4-63
  OSPF, 5-10
  route-filters, 10-26
IP-Route, 4-23
  OSPF, 5-16
IPX-Global, 8-4
IPX-Interface, 8-5
IPX-Route, 8-13
IPX-SAP-Filter, 8-16
L2-Tunnel-Global
  L2TP, 7-2
  PPTP, 7-7
RADIUS
  AppleTalk routing, 9-5
  ARA, 9-5
  ATM-Frame Relay circuits, 3-34
  ATMP Gateway Home Agent, to, 6-13
  ATMP IPX, 6-31, 6-33
  ATMP mobile clients, 6-9
  ATMP Router Home Agent, to, 6-13
  client DNS, 4-50
  dial-out, 2-36
  filter action, 10-6
  filter direction, 10-6
  filters, applying, 10-27
  Frame Relay circuits, 3-25
  Frame Relay Direct, 3-21
  gateway DLCI, 3-19
  generic filters, 10-8
  IP filters, 10-12
  IP options, 4-14
  IP-in-IP tunnel, 7-12
  IPX options, 8-8
  LNS, to, 7-3, 7-8
  modem dial-out, 2-40
  nailed, 2-27
  PPP, 2-11
  PPP, multilink, 2-15
  private static routes, 4-25
  session management, 2-9
  TCP-Clear, 2-23, B-3, B-5
  TOS filters, 10-19
RADIUS frdlink, 3-8
RADIUS global-pools, 4-53
RADIUS ipxroute, 8-14
RADIUS permconn, 3-15
RADIUS pools, 4-52
RADIUS routes, 4-24
sharing, 4-32
SNMP, B-14
Terminal-Server, 2-5, A-12, B-1
  authorization, B-2
  PPP-Mode-Configuration, B-12
  security mode, A-10
  Terminal-Mode-Configuration, B-9, B-10, B-11
Tunnel-Server
  L2TP, 7-2
  PPTP, 7-7
VRouter, 4-69
prompts
  login, A-11
  password, A-11
  third, A-12
prority queuing (proxy), 4-22

protocols
AppleTalk, 9-1
ARP, 4-8
ATMP, 6-1
authentication, A-7
BOOTP, 4-40
CCP, 2-12
CHAP, 2-37
GRE, 6-1, 7-6
ICMP, 4-33
IGMP, 4-58
IGP, 5-4
IP-in-IP, 7-11
IPX, 8-2
IPX RIP, 8-2
IPX SAP, 8-1
IPXWAN, 8-2
L2TP, 7-1
link management (Frame Relay), 3-7
Microsoft/STAC, 2-12
MP+, 2-17
MS-CHAP, 2-37
OSPF, 5-1
PAP, 2-37
PPP, 2-11, 2-15
PPTP, 7-6
RIP, 4-8
router options, enabling, 4-39
SLIP, B-13
SNTP, 4-43
Stac LZS, 2-12
statistics for, 4-70
TCP, 4-41
Telnet, B-2
UDP, 4-37
V.120, 2-5
X.75, 2-25
proxy ARP, 4-8
proxy home servers, IPX, 8-10
proxy QOS, examples, 4-22
Proxy-QoS and TOS support, 4-22
pseudo-user profiles. see RADIUS

Q

Quality-of-Service (QOS). See Type-of-Service (TOS)
queues
limiting size of, 4-37
priority queuing (proxy), 4-22

R

RADIPAD for centralized pool management, 4-52
RADIPAD global address pools, 4-52
radipa-hosts, RADIUS, 4-53
RADIUS
AppleTalk routing, 9-5
ARA, 9-5
ATM-FR circuit example, 3-36
ATM-FR circuits, 3-34
ATM-Frame Relay circuits, 3-34
ATMP Gateway Home Agent, 6-13
ATMP IPX, 6-31, 6-33
ATMP mobile client attributes, 6-9
ATMP Router Home Agent, 6-13
client DNS attributes, 4-50
default filters in Answer-Defaults, 10-27
defaults, 2-4
dial-out, 2-36
DLCI permconn profiles, 3-15
dynamic address assignment, 4-57
External-Auth profile, 2-6
filter direction, 10-6
filters, applying, 10-27
forwarding action, 10-6
Frame Relay backup interfaces, 3-16
Frame Relay circuit examples, 3-27, 3-28, 3-31
Frame Relay circuits, 3-25
Frame Relay Direct, 3-21
Frame Relay DLCI interface, 3-15
Frame Relay gateway, 3-15, 3-19
Frame Relay link operations, 3-8
Frame Relay NNI, 3-13
Frame Relay UNI-DCE, 3-12
Frame Relay UNI-DTE, 3-11
frdlink profiles, 3-8
gateway DLCI, 3-19
generic filters, 10-8
global pools profiles, 4-52
idle timer, 2-9
IP connection attributes, 4-14
IP filters, 10-12
IP-in-IP tunnel, 7-12
IPX options, 8-8
IPX peer-mode default, 8-9
ipxroute profiles, 8-14
LNS, connection to, 7-3, 7-8
modem dial-out, 2-40
MP settings, 2-15
MPP settings, 2-19
multicast clients, 4-64
nailed connections, 2-27
overview, 2-8
password handling, A-2
pools profiles, 4-52
pools pseudo-user profiles, 4-52
PPP, 2-11
PPP settings, 2-11
PPP, multilink, 2-15
private static routes, 4-25, 4-29

pseudo-user
frdlink, 3-8
global-pools, 4-53
ipxroute, 8-14
pools, 4-24, 4-52
reloading nailed profiles, 2-27
route profiles, 4-24
routing to PVC endpoint, 3-15, 3-19
session management, 2-9
shared secrets, A-5
summarized pools, 4-56
TCP-Clear, 2-23, B-3, B-5
telco attributes, 2-27
token-card server, and, A-13
TOS filters, 10-19
wanabe interface, 4-4
see also profiles
RADIUS daemon for security card authentication, A-16
RADIUS Filter-ID support, 10-27
RADIUS route pseudo-user profiles, 4-24
RADIUS routes in user profiles, 4-25
reject (rj0) interface, 4-3
remote address, 4-16
resiliency, ATMP, 6-20
Reverse-ARP (RARP). See RARP
RFCs, 1-3
RIP
ATMP Home Agents, in, 6-18
ATMP, between agents, 6-3
ignore default route in updates, 4-37
metrics, 4-12, 4-24
multicast address, 4-7
OSPF ASE, 5-13
OSPF, comparison, 5-1
packets, number queued, 4-37
propagating received routes, 4-35
route filters, defining, 10-24
system address, advertised, 6-3
triggering, 4-36
updating changed routes only (triggering), 4-36
use on LAN interfaces, 4-8
VRouter, defined for, 4-69
see also IPX RIP, 8-1
Rlogin, source port range, B-10
route cacheing
port caches, 4-39
route caches, 4-39
route filters
action taken when match occurs, 10-5
applying to interfaces, 10-26, 10-30
changing a route's metric, 10-25
packet contents, how compared to, 10-5
RIP packets from a specified address, 10-24
specific routes, filtering, 10-25
route, RADIUS, 4-24
Router Home Agent, ATMP, 6-23
Routing Information Protocol (RIP). See RIP
routing policies
cacheing options, 4-38
drop source-routed packets, 4-34
protocol options, enabling, 4-39
quality of service, 4-22
redundant units, 4-36
RIP, 4-34
security, router, 4-31
system IP address, 4-31
system-wide, 4-33
type of service, 4-22
routing table. See IP routing table

S

SDSL. See *MAX TNT Hardware Installation Guide*
security
address, enforcing, B-15
address, source checking, 4-21
authorizing immediate mode, B-2
authorizing interactive terminal-server logins, B-9
authorizing menu mode, B-4
authorizing SLIP sessions, B-13
callback, A-30
called-number authentication, A-24
CLID authentication, A-23
direct-access dialout, for, 2-39
disabling directed broadcasts, 4-10
ignoring broadcast ICMP echo requests, 4-33
immediate mode, B-2
menu mode, B-2
mode for terminal server, B-14
passwords for PPP connections, A-6
PPP sessions, for, B-12
related RFCs, 1-5
restricting access to terminal server, B-1
router policies, 4-31
setting Telnet defaults, B-11
SNMP address, B-14
source address checking, 4-21
system password, A-11
terminal mode, B-9
third prompt, A-12
token-card authentication, A-2, A-13
using call information, A-23
using token cards, A-13
security mode (terminal server), A-10
seed router, AppleTalk, 9-2
Serial Line IP (SLIP). See SLIP (Serial Line IP)
servers
BOOTP, 4-42

servers *continued*
DNS, client, 4-49
DNS, local, 4-45
Enigma Logic SafeWord, A-13
external authentication, 2-6, A-13
NetBIOS, 4-44
NetWare home server proxy, 8-10
NetWare, routes to, 8-13
RADIUS, running RADIPAD, 4-52
Security Dynamics ACE/Server, A-13
SNTP, 4-43
sessions
accounting options, 2-10
framed-protocol, establishing, 2-3
login-service, establishing, 2-3
maximum duration, 2-8
monitoring, 2-3
setting Telnet defaults, B-11
settings in Connection profiles, 2-8
settings in RADIUS, 2-9
timeouts, inactive sessions, 2-8
shared secrets, A-5
shelves, spanning, 2-3
Simple Network Management Protocol (SNMP). See SNMP
Simple Network Management Protocol. See SNMP
Simple Network Time Protocol (SNTP). See SNTP
SLIP (Serial Line IP)
address from BOOTP, B-13
see also authorization
slot cards, spanning for multilink calls, 2-3
slot cards, used for dialins, 2-1
SNMP
address security, B-14
alarm trap for heartbeat monitoring, 4-60
authorization, B-14
community strings, B-14
enabling, B-14
enforcing address security, B-15
limitations for VRouters, 4-68
packets, number queued, 4-37
related books, 1-5
SNMP profile, B-14
SNTP
servers, specifying, 4-43
UTC offset, specifying, 4-43
socket numbers, IPX, 8-15
soft IP interface
route to, 4-10
sip#, creating, 4-10
sip0 interface, 4-4
soft IP interface, example, 4-10
source address checking, 4-21
source-routed packets, dropping, 4-34
split-horizon RIP policy, 4-35
spoofing local address, preventing, 10-14
spoofing, IPX frame types, 8-6
SS7. See *MAX TNT Hardware Installation Guide*
Stac compression, 2-12
Stac-9 compression, 2-12
static routes
ATMP mobile clients. to, 6-20
default route, example, 4-26
IP-Route profile settings, 4-23
IPX, to NetWare server, 8-12
multipath, 4-28
OSPF settings, 5-16
preferences, 4-34
private per-connection (RADIUS), 4-25, 4-29
profiles for defining, 4-1
RADIUS attributes, 4-24
RADIUS user profile, in, 4-25
reasons for defining, 4-23
remote subnet, to, 4-28
soft address, to, 4-10
summarized pools, to, 4-56
third-party, OSPF, 5-18
VRouter, defining for, 4-75
statistics, protocol, 4-70
stub areas, 5-7
subnet masks, explained, 4-4
subnet notation, Ascend, 4-5
subnet route, example, 4-28
summarization. see pools
Suppress host route advertisements, 4-38
switched dial-in connections, examples, 2-10
synchronous connections
described, 2-1
dial-in PPP, 2-13
system IP address, 4-31
ATMP, recommendation, 6-2
VRouter, for, 4-69
system reset
ATMP requirements, 6-2
OSPF, 5-9

T

T1, T3. See *MAX TNT Hardware Installation Guide*
TA (Terminal Adapter) V.120, 2-5
target utilization, requesting bandwidth, and, 2-19
TCP
port for immediate dialout service, 2-38
PPTP tunnel control link, 7-6
timeout value, 4-41

TCP-Clear, 2-21
  authentication of, B-3
  buffering datastream, 2-21
  destination TCP port, 2-22, 2-23, B-3
  DNS name of host, 2-22
  encapsulation protocol, 2-22, 2-23, B-3
  End-of-Packet pattern, 2-22
  IP address of host, 2-22
  multiple destinations, 2-21
  passwords, 2-22
  performance enhancements, 2-21
  RADIUS attributes, 2-23
  required settings, 2-21
TCP/IP, related books, 1-6
TCP-Raw. See TCP-Clear
telco
  call information, A-23
  charges, 2-18
  CLID or DNIS information, 7-4, 7-9
  nailed connections, options, 2-26
  RADIUS attributes, 2-27
  settings in Connection profiles, 2-7
Telnet
  logins, 4-32
  password, A-6
  terminal-mode defaults, B-11
telnet password, 4-31
Terminal Adapter (TA). See TA (Terminal Adapter)
terminal mode
  authorizing, B-9
  described, B-9
terminal server
  asynchronous connections and, 2-5
  authorizing immediate mode, B-2
  authorizing interactive logins, B-9
  authorizing menu mode, B-4
  authorizing SLIP sessions, B-13
  banner, A-11
  expect-send login scripts, A-10
  immediate mode, B-2
  login prompt, A-11
  menu mode, B-2
  password prompt, A-11
  password protecting, A-9
  restricting access, B-1
  security mode, B-14
  setting Telnet defaults, B-11
  system password, A-11
  terminal mode, B-9
  third prompt, A-12
Terminal-Server profile, 2-5, A-10
  authorization, for, B-2
  authorizing interactive logins, B-9, B-10
  authorizing PPP sessions, B-12
  modem dial-out, 2-38
  restricting access, B-1
  setting Telnet sessions defaults, B-11
  setting third prompt, A-12
third prompt, A-12
third-party routes, 5-18
third-party routing, example, 5-19
timeouts, login, A-12
timers
  inactive sessions, for, 2-8
  inactive tunnels, for, 6-18
  PPP sessions, for, 2-8
  RADIUS, in, 2-9
  setting absolute for connections, 2-9
token cards, A-13, A-15
  access challenges, A-15
  example of dial-in, A-15
token-card authentication, A-2, A-13
  RADIUS, and, A-13
  setting up Cache-Token, A-19
  setting up PAP-Token-CHAP, A-17
token-card authentication, example, A-15
tokens, A-15
TOS filters
  action (set precedence bits), 10-17
  action taken when match occurs, 10-4
  applying to interfaces, 10-26, 10-29
  packet contents, how compared to, 10-4
  when to use, 10-17
TOS filters, example, 10-20
Transmission Control Protocol (TCP). See TCP
triggering, RIP, 4-36
triggering, RIP updates, 4-36
tunnel interface, 4-4
tunneling
  ATMP authentication, A-21
  ATMP idle timer, 6-18
  ATMP overview, 6-1
  ATMP retry limits, 6-4
  ATMP tunnel request
    Foreign Agent, 6-10
    Home Agent response, 6-17, 6-19
  DDP-IP, 9-9
  fragmentation issues, 6-5
  GRF switch, to, 6-5, 6-15
  IP-in-IP, 7-11
  IPX over ATMP, 6-30
  L2TP overview, 7-1
  L2TP profiles, 7-2
  L2TP tunnel authentication, 7-4, 7-5
  L2TP, configuring tunnel, 7-2
  link compression, and, 6-4
  mobile client configurations, 6-8
  MTU limit, explicit, 6-4
  PPTP overview, 7-6

tunneling *continued*
PPTP profiles, 7-7
PPTP tunnel authentication, 7-9, 7-10
PPTP, configuring tunnel, 7-7
UDP port for ATMP control information, 6-3
Tunnel-Server profile
L2TP, 7-2
PPTP, 7-7
Type-5 LSAs, 5-7
Type-7 LSAs, 5-7, 5-17
Type-of-Service (TOS)
examples, 4-22
overview, 4-22
priority levels, 4-13, 4-16
settings, 4-14, 4-15
Type-of-Service filters, 10-17
type-of-service policy, 4-22

U

UDP
ATMP, port for tunnel control, 6-3
checksums, enabling, 4-41
packet queues, reducing overhead, 4-37
port for L2TP tunnel control link, 7-1
Universal Time Configuration (UTC), 4-43
UNIX client finger queries, 4-42
User Datagram Protocol (UDP). See UDP
user profiles, RADIUS. see RADIUS
User-to-Network (UNI), defined, 3-1
utilization rate
persistence, 2-19
request for bandwidth, and, 2-19, 2-20

V

V.120 TA (Terminal Adapter), 2-5
authentication, B-3
settings for incoming calls, 2-4
terminal server and, 2-5
variable-length subnet masks (VLSM), 5-3
Virtual Circuits. See Frame Relay
virtual IP interfaces, example, 4-9
virtual IPX network for dial-in clients, 8-3
virtual LAN interfaces, 4-9
Virtual Private Networks. See tunneling, VRouters
virtual router (vr0_main) interface, 4-4
Virtual Routers. see VRouters
VJ header prediction, 4-12
VRouter profile, 4-69
VRouters
address pools, for, 4-69
assigning interfaces to, 4-73
defined, 4-67
defining, example of, 4-69
interfaces, displaying, 4-74
network commands modified, 4-67
protocol statistics, 4-70
RIP policies, 4-69
routing table, 4-70
static routes, defining, 4-75
static routes, displaying, 4-75
system address for, 4-69
VRouters, example, 4-69

W

WAN AppleTalk interfaces
AppleTalk PPP, 9-7
AppleTalk router, to, 9-7
ARA clients, 9-6
ARA Guest access, allowing, 9-4
client software for, 9-4
connection types, 9-4
filters, applying, 10-2, 10-28
IP, and, 9-8
remote device, peer mode, 9-5, 9-6
WAN connections
asynchronous, 2-1
encapsulation protocols, 2-1
idle timer, 2-8
maximum duration of, 2-8
synchronous, 2-1
telco options, 2-26
WAN Frame Relay interfaces
ATM, circuits, 3-33
DLCI, 3-14
filters, applying, 10-2, 10-28
FR Direct, 3-20
gateway, 3-19
paired, circuits, 3-24
WAN IP interfaces
AppleTalk, and, 9-8
ATMP tunnel, 6-7, 6-12
call filters, applying, 10-3
client-specific default route, 4-21
Connection profile settings, 4-12
data filters, applying, 10-2, 10-28
filtering RIP packets, 10-30
host route, 4-17
host-to-host, 4-19
IP Direct, 4-19
L2TP tunnel, 7-3
MBONE, 4-61
multicast clients, 4-65

numbered interface connection, 4-18
OSPF options, 5-9
PPTP tunnel, 7-9
private, 4-20
RADIUS attributes, 4-14
router-to-router, 4-16
VJ compression, 4-12
VRouter, assigning to, 4-73
WAN IPX interfaces
authentication of, 8-7
Connection profile settings, 8-7
dial query, 8-9
filters, applying, 10-2, 10-28
home server proxy, 8-10
IPX RIP,enabling, 8-9
IPX SAP, enabling, 8-9
net-number and net-alias, 8-9
RADIUS profile settings, 8-8
remote device, peer mode, 8-8
SAP query, dialing connection, 8-9
WAN OSPF interfaces
area number and type, 5-6, 5-10
ASE handling, 5-11
authentication, 5-3, 5-11
costs, 5-5, 5-11
designated router priority, 5-4, 5-11
intervals for hello packets, 5-10
LSA handling, 5-11
wanabe interface, 4-4

X

X.75 connections, 2-25

Z

ZipGetNetInfo request, sent to seed router, 9-3
zones
default, 9-3
hint-zone, 9-3
list of, 9-3