MAX E1/PRI 4.6C Release Note

Number 3 **August 23, 1996**

This release note describes the features in the Ascend MAX system software version 4.6C. It is intended for MAX owners who have system software version 4.6B or earlier.

How to use this Release Note

Use this release note in conjunction with your MAX documentation. To use this release note, follow these steps:

1. Read through the next section "What's new in software version 4.6C?," to determine which new features apply to your environment.
2. Obtain the version 4.6C binary file from Ascend anonymous FTP server (ftp.ascend.com). If you need Technical Assistance, contact Ascend in one of the following ways:
   - In the United States, call (800) 272-3643
   - Outside the United States, call (510) 769-6001
   - Customer Support BBS by modem, dial (510) 814-2302
3. Upgrade to the new software by following the instructions in the section, "Upgrading system software," on page 128. Then configure the features that apply to you by reading the appropriate sections in this release note.

What's new in software version 4.6C?

The following new features are described in this release note:

With interface-based routing, each physical or logical interface on the box has its own IP address.

As a frame relay concentrator, the MAX can support a large number of low-speed frame relay connections and concentrate them into one or more high-speed connections to a frame relay switch using either the serial WAN interface or E1 lines. To support this, Ascend has implemented the NNI (Network to Network Interface) version of the frame relay protocols.

Interface-Based Routing

All of the Ascend products implement what is referred to as system-based or box-based routing. With system-based routing, the entire box is addressed with a single IP address. For systems that have a single backbone connection, system-based routing is by far the simplest form of routing from both a configuration and trouble-shooting perspective.

The alternative form of routing is referred to as interface-based routing. With interface-based routing, each physical or logical interface on the box has its own IP address. For a product such

as a MAX E1, it would potentially be required to assign over one hundred IP addresses to a single box. It is for this reason that Ascend implemented system-based routing for the MAX.

However, there are now some applications that the MAX is used for in which it might be useful to "number" some of the interfaces— in other words, to have the MAX operate as a partially system-based router and partially interface-based router. Reasons for using numbered inter- faces include trouble-shooting leased point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing allows the Ascend product to operate more nearly the way a multi-homed Internet host behaves, should that be desired.

This feature allows the user to configure each link as "numbered" (interface-based) or "unnumbered" (system-based). If no interfaces are specified as numbered, then the box will operate exactly as has previously. Interface numbering is accomplished via the Connection profile.

System Behavior With a Numbered Interface

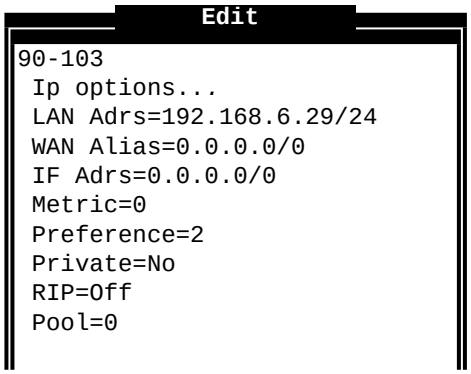
If a MAX is using a numbered interface, the following differences in operation should be noted, compared to unnumbered (system-based) routing:

- IP packets generated in the MAX and sent to the remote address will have an IP source address corresponding to the numbered interface, not to the default (Ethernet) address of the MAX.
- During authentication of a call placed from a MAX using a numbered interface, the MAX will report the address of the interface as its IP address.
- The MAX will add to its routing table host routes all numbered interfaces listed in Connection Profiles.
- The MAX will accept IP packets whose destination is a numbered interface listed in a Connection profile, considering them to be destined for the MAX itself. (The packet may actually arrive over any interface, and the numbered interface corresponding to the packet's destination address need not be in the active state.)

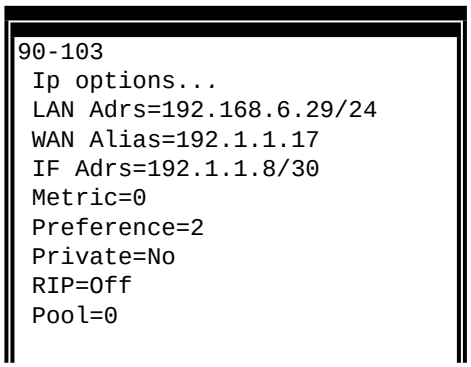
New IF Adrs parameter

Configuration of a numbered link takes place in the Connection profile, under the IP Options submenu. A new parameter, IF Adrs, specifies the IP address of the interface. If the field is left at its default value (0.0.0.0/0), then the interface will be treated as unnumbered.

The screen below shows a typical screen for an unnumbered interface. The new IF Adrs field is not used for an unnumbered interface.



The screen below shows settings for a numbered interface. The WAN Alias parameters has been filled in with the address of the remote end of the link, and the new IF Adrs parameter contains the number of the interface at the near end of the link.



IF Adrs

Description: This parameter specifies the IP address of the interface at the near end of a link.

Usage: Press Enter to open a text field. Then, type the IP address of the numbered interface.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate the netmask from the IP address with a slash. The default is 0.0.0.0/0.

Press Enter again to close the text field.

`Usage: 200.207.23.7/24`

Dependencies: The IF Adrs parameter does not apply if the MAX does not support IP (Route IP=No).

Parameter Location: Connection Profile: Ethernet > Connections > IP options

See Also: WAN Alias, Route IP

Specifying the remote interface address

This section provides some guidelines on using interface-based routing.

If both the system and interface addresses are known

If interface-based routing is being added to a system which has already been set up using system-based routing, the easiest way to specify the remote interface address is by using the WAN Alias parameter in the Connection profile. WAN Alias is used to identify the remote end of the link. If a WAN Alias is set, the following will take place:

- Host routes will be created to both the Lan Adrs and the WAN Alias; the WAN Alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs.
- A route will be created to the remote system's subnet, showing the WAN Alias as the next hop.
- Incoming PPP/MPP calls must report their IP addresses as the WAN Alias (rather than the Lan Adrs). That is, the caller must be using a numbered interface, and its interface address must agree with the WAN Alias on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the WAN Alias address as the “next hop” (gateway) field. (The Lan Adrs address will also work, as would be used for system-based routing.)

If only the interface address is known

It is also permissible to omit the remote side’s system address from the profile and use interface-based routing exclusively. This is an appropriate mechanism if, for example, the remote system is on a backbone net which may be periodically reconfigured by its administrators, and you want to refer to the remote system only by its mutually agreed-upon interface address.

In this case, the remote interface address is entered in the Lan Adrs parameter, and the WAN Alias is left as default (0.0.0.0). Note that Lan Adrs must always be filled in, so if the only known address is the interface address, it must be placed in the Lan Adrs parameter rather than the WAN Alias parameter.

If the remote interface address is placed in the Lan Adrs parameter, the following will take place:

- A host route will be created to the Lan Adrs (interface) address.
- A net route will be created to the subnet of the remote interface.
- Incoming PPP/MPP calls must report their IP addresses as the Lan Adrs (interface) address.

If the remote interface address is not specified

If interface-based routing is in use and the local interface is numbered, the remote address will usually be known (in practice, the subnet must be agreed upon by administrators of both sites.) It is possible, but not recommended, to number the local interface, omitting the interface address of the remote site and using only its system or LAN address. In that case, do not use the (supposedly unknown) remote interface address in any static routes.

The fallback behavior when a local interface is numbered but no corresponding remote interface address is set, is the following:

- The remote interface must have an address on the same subnet as the local, numbered interface. Incoming PPP will be rejected if the Connection Profile numbers the local interface and the (remote) caller supplies an address not on the same subnet.

New RADIUS attributes

If the connection profile is stored in a RADIUS database, two new RADIUS attributes (and the existing Ascend-PPP-Address) are used to support interface-based routing:

Attribute Name	Value	Type	Explanation
Ascend-PPP-Address	253	ipaddr	Local interface address
Ascend-IF-Netmask	154	ipaddr	Local interface netmask
Ascend-Remote-Addr	155	ipaddr	Remote interface (WAN Alias)

NNI support (Frame Relay Concentrator)

In a frame-relay backbone, every access line must connect directly to a frame relay switch. In the past, most connections to the frame relay network were relatively high speed (full E1 lines at 1.5Mbps). Frame relay switches such as those from Cascade and Stratacom are designed around high performance E1 speed or higher interface connections.

With the change in frame relay pricing offered by RBOCs, it may now be lower cost to run low speed 56K or 64K leased frame relay connections in place of analog or even ISDN dial-up connections. However, the problem on the network-side is that the same frame relay port that is designed for the high speed connections must be consumed for the 56K or 64K connection. Because of this, the network infrastructure costs for the low speed ports is very high.

Ascend’s position

Ascend’s greatest strength in network infrastructure has been the ability to concentrate a large number of low-speed individual connections into a small number of high-speed connections to the backbone. Traditionally, Ascend has done this with dial-up connections concentrated into a high-speed router port, running the standard routing protocols.

However, a MAX 4000 is architecturally equally capable of supporting a large number of 56K or 64K leased frame relay connections and concentrating them into one or more high-speed connections to a frame relay switch using either the 8Mbps serial interface or the E1 lines.

In this model, each DS0 (or B-channel) on the E1 lines can be a separate frame relay connection from a low-speed frame relay user. Up to 96 low-speed connections in North America/Japan or 120 low-speed connections in Europe could be concentrated into a single MAX 4000. If all of the frame relay connections are concentrated onto the single 8-Mbps serial

interface, the MAX 4000 turns a single high-cost frame relay port on a traditional frame relay switch into approximately 100 ports operationally.

NNI protocol solution

For the MAX to operate as a frame relay concentrator, it must appear as a “frame relay switch” to the low-speed network access connections and as another “frame relay switch” to the network infrastructure connections to switches such as those from Cascade or Stratacom. Ascend does this through implementing the NNI (Network to Network Interface) version of the frame relay protocols in addition to the UNI (User to Network Interface) protocols that were already implemented.

Ascend’s frame relay concentrator implementation

The Ascend frame relay implementation now supports the following functionality:

- FR (UNI-DTE) connection

  A DTE (data terminal equipment) is the end-point for data. A DTE sends enquiries to a DCE. For this type of connection, the MAX performs the FR DTE functions specified for link management and can connect to a FR DCE unit (frame relay switch).

- FR (UNI-DCE) switch connection

  A DCE (data communications equipment) is the UNI side of a frame relay switch. A DCE responds to enquiries from a DTE. For this type of connection, the MAX functions as a frame that performs the FR DCE functions specified for link management and can have FR DTE devices connected to it.

- FR NNI connection

  An NNI (Network-to-Network interface) interface allows the MAX to function as a frame relay switch connecting to another frame relay switch. For this type of connection, the MAX performs both FR DTE and DCE link management functions. The NNI connection may be between two Ascend units in NNI mode or between the MAX and another FR switch in NNI mode, such as those from Cascade and Stratacom.

Configuring the frame relay concentrator

In addition to the basic NNI protocol development, extensive configuration and status information has been added to the MAX to allow mapping between an individual DLCI on a network access connection and other DLCIs on the network infrastructure connection.

Note: To configure a frame relay circuit, you must set up the access lines. For example, if you are using E1 lines to accommodate a separate frame relay connection on each B-channel, you must configure each channel appropriately. See the *ISP & Telecommuting Configuration Guide* for information about configuring E1 lines.

You must also configure the following aspects of the frame relay network:

- connections out to the frame relay network from the MAX (Frame Relay Profiles)
- logical data circuits between users and end-points on the frame relay network (Connection Profiles)

Frame Relay Profiles (resident in NVRAM)

Table 1 shows Frame Relay Profile parameters related to the new types of connections. New parameters and parameters that have new values are shown in bold type.

Table 1. Frame Relay Profile parameters

Location	Parameters with example values
Ethernet→Frame Relay→*any profile* (Frame Relay Profile)	Name=PacBell Active=Yes Call Type=Nailed **FR Type=NNI** **LinkUp=Yes** Nailed Grp=1 Data Svc=64k ... **Link Mgmt=Q.933A** N391=6 **DTE N392=3** **DTE N393=4** **DCE N392=3** **DCE N393=4** T391=10 T392=15 MRU=1532

To define a Frame Relay Profile:

1 Open a Frame Relay Profile.

2 Assign a name to the profile.

For example:

Name=PacBell

The name can contain up to 15 alphanumeric characters. You must use this name in Connection Profiles that access this connection to the switch.

3 Activate the profile.

Active=Yes

4 Specify that this is a nailed connection and the group number of the nailed channels (or serial WAN port) to use.

For example:

Call Type=Nailed
Nailed Grp=1

Nailed is the default for frame relay connections. When the call type is nailed, dial numbers and other telephone company parameters are N/A. You can specify switched if the frame relay switch allows dial-in; however, frame relay networks currently have no dial-out connection capability.

5 Specify the FR type.

For example:

FR Type=DCE

FR Type is the type of FR datalink. The default is DTE. The types are:

- DCE (for a UNI-DCE interface)
- DTE (for a UNI-DTE interface)
- NNI (for an NNI interface)

See “Connection profiles for frame relay circuits (resident in NVRAM)” on page 17 and “Data flow” on page 20 for related information.

6 Specify whether the link comes up automatically.

For example:

LinkUp=Yes

This indicates that the datalink comes up automatically and stays up even when the last DLCI has been removed. If this parameter is set to No, the datalink does not come up unless a Connection Profile (DLCI) brings it up, and it shuts down after the last DLCI has been removed.

Note: You can start and drop frame relay datalink connections by using the DO DIAL and DO HANGUP commands. DO DIAL brings up a datalink connection. DO HANGUP closes the link and any DLCIs on it. If LinkUp=Yes, DO HANGUP brings the link down, but it will be automatically restarted. A restart will also occur if there is a DLCI profile invoking the datalink.

7 Set the data service.

For example:

Data Svc=64k

The two types that are available are 64K or 56K.

8 Specify the link management protocol used between the MAX and the frame relay switch.

For example:

Link Mgmt=Q.933A

The three link management types that are available are:

- None (no link management)
- T1.617D (for T1.617 Annex D)
- Q.933A (for Q.933 Annex A)

9 Set the frame relay timers and event counts.

- N391

  This parameter specifies the Full Status polling cycle. It is the interval at which the MAX requests a Full Status Report. You can specify a number of seconds between 1 and 255 (default 6). This parameter is N/A if FR Type is DCE.

- DCE N392

  This parameter specifies the number of errors during DCE N393 monitored events which causes the network side to declare the user side procedures inactive. This parameter’s value should be less then DCE N393. You can specify a number between 1 and 10 (default 3). This parameter is N/A when FR Type is DTE.

- DCE N393

  This parameter specifies the DCE monitored event count. You can specify a number between 1 and 10 (default 4). This parameter is N/A when FR Type is DTE.

- DTE N392

  This parameter specifies the number of errors during DTE N393 monitored events which cause the user side to declare the network side procedures inactive. This

parameter's value should be less then DTE N393. You can specify a number between 1 and 10 (default 3). This parameter is N/A when FR Type is DCE.

– DTE N393

This parameter specifies the DTE monitored You can specify a number between 1 and 10 (default 4). This parameter is N/A when FR Type is DCE.

– T391

This parameter specifies the Link Integrity Verification polling timer. You can specify a number of seconds between 5 and 30 (default 10). T391 should be less than T392. This parameter is N/A when FR Type is DCE.

– T392

This parameter specifies the timer for verification of polling cycle. This is the length of time the unit should wait between Status Enquiry messages. You can specify a number of seconds between 5 and 30 (default 10). An error is recorded if no Status Enquiry is received within T392 seconds.This parameter is N/A when FR Type is DTE.

10 Set the maximum data size.

For example:

MRU=1532

11 Close the Frame Relay Profile.

Frame Relay Profiles (RADIUS)

In previous releases of the Ascend software, all Frame Relay Profiles were stored in NVRAM with the maximum number being 16. With the addition of the FR concentrator feature, the MAX must support additional Frame Relay Profiles profiles, so you can now specify these profiles in RADIUS.

RADIUS frame relay profiles are accessed during system startup and when the Upd Rem Cfg is selected in the Sys Diag menu. The Upd Rem Cfg command to a submenu that allows the user to select the type of update from RADIUS. The Upd Rem Cfg submenu now contains these options:

```
Upd Rem Cfg...
   0=ESC
   1=Routes
   2=Pools
   3=Nailed Prof
   4=Termsrv
   5=All
```

- 1 (Routes) updates the static route and bridge entries.
- 2 (Pools) updates the address pools
- 3 (Nailed Prof) updates the Permanent Connection and Frame Relay Profiles
- 4 (Termsrv) updates terminal server related items such as the banner or menu interface
- 5(All) updates all of the above

The MAX uses a well known user-name and password to retrieve frame relay datalink information from RADIUS. The password is always "ascend". The user-name must the following format:

`frdlink-`*unit-id*

- `frdlink` is a literal keyword
- *unit* is system name of the unit accessing the data (the MAX)
- *id* is a unique number identifying this entry.

  IDs must be assigned in sequence starting with “1” and with no missing numbers. For example, if you have three frame relay datalink profiles, the first one must be ID=1, the next two must be ID=2 and ID=3. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

Table 2 shows the new RADIUS attributes for specifying a frame relay datalink connection.

Table 2. New RADIUS attributes required for FR datalink connections

Attribute	Number	Value
Ascend-FR-LinkUp	157	Indicates if a link comes up automatically: 0 (Ascend-LinkUp-Default) 1 (Ascend-LinkUp-AlwaysUp)
Ascend-FR-Nailed-Grp	158	Indicates the nailed channel number for a FR datalink (an integer).
Ascend-FR-Type	159	Type of frame relay connection: 0 Ascend-FR-DTE (the default) 1 Ascend-FR-DCE 2 Ascend-FR-NNI
Ascend-FR-Link-Mgt	160	The type of FR Link Management: 0 Ascend-FR-No-Link-Mgt (default) 1 Ascend-FR-T1-617D 2 Ascend-FR-Q-933A
Ascend-FR-N391	161	The interval at which the MAX requests a Full Status Report (1–255) default 6.
Ascend-FR-DCE-N392	162	The number of errors during DCE N393 monitored events which causes the network side to declare the user side procedures inactive (1–10). Default 3. This parameter’s value should be less then DCE-N393.
Ascend-FR-DTE-N392	163	The number of errors during DTE N393 monitored events which causes the network side to declare the user side procedures inactive (1–10). Default 3. This parameter’s value should be less then DTE-N393.
Ascend-FR-DCE-N393	164	The DCE monitored event count (1–10). Default 4.
Ascend-FR-DTE-N393	165	The DTE monitored event count (1–10). Default 4.

Table 2. New RADIUS attributes required for FR datalink connections

Attribute	Number	Value
Ascend-FR-T391	166	The Link Integrity Verification polling timer (5–30). Default 10.
Ascend-FR-T392	167	The timer for verification of polling cycle (5–30). Default 15. This is the length of time the unit should wait between Status Enquiry messages. An error is recorded if no Status Enquiry is received within T392 seconds.

Example frame relay datalink profiles in RADIUS:

frdlink-dialgw-1 Password = "ascend" User-Service= Dialout-Framed-User,

Ascend-FR-Profile-Name = "FR Prof 1",

Ascend-FR-Type= Ascend-FR-DTE,

Ascend-FR-Nailed-Grp = 1,

Ascend-FR-Link-Mgt = Ascend-FR-T1-617D,

Ascend-FR-N391 = 20

frdlink-dialgw-2 Password = "ascend" User-Service= Dialout-Framed-User,

Ascend-FR-Profile-Name = "FR Prof 2",

Ascend-FR-Type= Ascend-FR-NNI,

Ascend-FR-Nailed-Grp = 2,

Ascend-FR-LinkUp = Ascend-LinkUp-AlwaysUp,

Ascend-FR-Link-Mgt = Ascend-FR-T1-617D

Connection profiles for frame relay circuits (resident in NVRAM)

Connection profiles can now define the path within the frame relay switch by using a new FR_CIR encapsulation type and circuit configuration parameter, shown in Table 3.

Table 3. Frame Relay Profile parameters

Location	Parameters with example values
Ethernet→Connections→*any profile* (Connection Profile)	Name=DTE-1 Active=Yes Encaps=FR_CIR ... Encaps options... FR Prof=PacBell DLCI=17 Circuit=Circuit1

A circuit specification defines two DLCI endpoints of a permanent virtual circuit (PVC), with one endpoint specified in each Connection Profile. Two Connection Profiles are required for a single PVC.

A DLCI is defined as a DLCI number related to a Frame Relay Profile. The two DLCIs can use the same datalink (Frame Relay Profile) or different ones. When combined as a circuit, the two DLCI endpoints act as a tunnel—data received on one DLCI bypasses the Ascend router and is sent out on the other DLCI. See “Data flow” on page 20 for additional details.

Note: Currently, multicast circuits are not supported, so only two DLCIs can be used to specify a PVC. If more than two DLCIs use the same circuit name, only two are used.

When the FR_CIR type is not specified, the FR type works as it did previously. Data is routed to the DLCI and data from the DLCI is sent to the Ascend routing code. The difference between FR_CIR and FR encapsulation is that FR_CIR builds a circuit by joining two DLCIs, where FR ends a circuit by terminating a DLCI.

- Example DTE connection with one DLCI (FR encapsulation)

  This example shows a DLCI to the Ascend router with a DTE interface:

```
Frame Relay Profile:
  Name=FR Prof 1
  FR Type=DTE
  ...
Connection Profile:
  Station=victorgw
  Encaps=FR
  ...
  Encaps options...
    FR Prof=FR Prof 1
    FR DLCI=16
    Circuit= N/A
```

- Example DCE connection to the Ascend router (FR encapsulation)

  This example shows a DLCI to the Ascend router engine with a DCE interface:

```
Frame Relay Profile:
  Name= FR Prof 1
  FR Type=DCE
  ...
Connection Profile
  Station=tedgw
  Encaps=FR
  ...
  Encaps options...
    FR Prof= FR Prof 1
    FR DLCI= 16
    Circuit= N/A
```

- Example NNI connection with a circuit (FR_CIR encapsulation)

  This example shows how to configure a typical circuit. DLCI 23 from FR Profile #2 and DLCI 16 from FR Profile #1 form a permanent virtual circuit (Circuit1) through the MAX. Also in this example, a DCE interface on the MAX would connect to DLCI 16, which typically would connect some FR device's DTE interface.

  The PVC link between DLCI 16 of EndPoint1 and DLCI 23 EndPoint2 profiles is set up by giving the same name to the Circuit parameters of both Connection Profiles.

```
Frame Relay Profile 1:
  Name= FR Prof 1
  FR Type=DCE
  ...
Frame Relay Profile 2:
  Name=FR Prof 2
  FR Type=NNI
  ...
Connection Profile 1:
  Station=EndPoint1
  Encaps=FR_CIR
  ...
  Encaps options...
    FR Prof= FR Prof 1
    FR DLCI= 16
    Circuit= Circuit1
Connection Profile 2:
  Station=Endpoint2
  Encaps=FR_CIR
  ...
  Encaps options...
    FR Prof= FR Prof 2
    FR DLCI= 23
    Circuit= Circuit1
```

User profiles for frame relay circuits (RADIUS)

You can specify a frame relay circuit in a RADIUS permanent profile. (See the RADIUS permanent profile document for details.) Table 4 shows new RADIUS attributes or attribute values for specifying a frame relay circuit.

Table 4. New RADIUS attributes required for FR circuits

Attribute	Number	Value
Framed-Protocol	263	A new value has been added: FR-CIR for frame relay circuits. The other end of the FR circuit must also be defined.
Ascend-FR-Circuit-Name	156	Indicates the PVC segment name for which this profile is an endpoint. The value is a string, maximum size 15 characters.

The MAX retrieves the profiles that define a circuit using a well known user-name and password. The password is always “ascend”. The user-name must the following format:

`permconn-`*unit-id*

- `permconn` is a literal keyword
- *unit* is system name of the unit accessing the data (the MAX)
- *id* is a unique number identifying this entry.
  IDs must be assigned in sequence starting with “1” and with no missing numbers. For example, if there are two profiles defining a circuit, the first one must be ID=1, the next must be ID=2. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

The following example RADIUS profiles define two endpoints for a PVC (PVC1). The PVC includes DLCI 16 on datalink “FR Prof 1" and DLCI 23 on datalink “FR Prof 2".

```
permconn-dialgw-1 Password = "ascend" User-Service = Dialout-Framed-
User,
    Framed-Protocol = FR-CIR,
    User-Name = "Endpoint1"
    Ascend-FR-Profile-Name = "FR Prof 1"
    Ascend-FR-Dlci = 16,
    Ascend-FR-Circuit-Name = "PVC1"


permconn-dialgw-2 Password = "ascend" User-Service = Dialout-Framed-
User,
    Framed-Protocol = FR-CIR,
    User-Name = "Endpoint2"
    Ascend-FR-Profile-Name = "FR Prof 2",
    Ascend-FR-Dlci = 23
    Ascend-FR-Circuit-Name = "PVC1"
```

Data flow

This section describes how data flows through the Ascend frame relay sub-system for various types of datalink connections (UNI-DTE, UNI-DCE, and NNI).

The DTE interface is designed to connect to a DCE interface. It's relatively uncommon to configure a DTE-to-DTE or DCE-to-DCE link.

The NNI performs both DTE and DCE link management. This type of management is used between frame relay switches to tie frame relay networks together.

There are different ways to determine if a DLCI endpoint is active. The determination is based on the link management type of the datalink. A datalink is always considered active if the N392 and N393 is met or if no link management functions are performed.

- If the datalink is a DCE, then the DLCI endpoints are considered active when the datalink is active.
- A DLCI on a DTE or NNI datalink, is considered active when the datalink is active and when it's remote DLCI counterpart is active.
- Both DLCI endpoints of a circuit must be active for the circuit segment to be considered active.

Below are some example setups and a description of the data flow for each one:

- One endpoint on a DTE datalink

  This is a standard configuration for a frame relay DTE where the datalink is attached to a FR switch. Data entering the Ascend unit will be routed to the appropriate DLCI and sent to the remote FR unit. Incoming data will be sent to the Ascend routing code. The datalink will only do FR DTE link management.

  In this setup, DLCI 23 is defined as a connection with FR encapsulation and only DTE link management is performed:

  ```
  Ascend Routing engine<------> DLCI 23 <------> remote FR unit
  ```

- One endpoint on a DCE datalink

  In this configuration, data entering the Ascend unit will be routed to the DLCI and sent to the remote FR unit. Incoming data from the remote unit will be sent to the Ascend routing code.

  In this setup, DLCI 23 of the DCE is defined as a connection with FR encapsulation. The datalink will do FR DCE link management. If link management is turned on for this datalink and the Monitored events threshold is reached, then the DLCI(s) on that datalink are declared inactive.

  ```
  Ascend Routing engine<------> DLCI 23 <------> remote FR unit
  ```

- A circuit between two DCE datalinks

  In a circuit configuration between two DCEs, data coming from either endpoint of the circuit will be sent to the other and will bypass the Ascend routing engine. The data portion of each packet is sent exactly as received. The FR header will be modified to contain the corresponding DLCI.

  In this setup, the DLCIs of DCEs are defined as connections with FR_CIR encapsulation. Both datalinks will do DCE link management.

  If the any DLCI changes status (becomes active or inactive), this change will be reflected in the response from the other endpoint's DCE to its Full Status Enquiry. Data received on an inactive circuit will be dropped.

- A circuit between a DCE and NNI datalink

  A circuit between a DCE and NNI datalink is similar to a DCE-to-DCE circuit except the NNI endpoint will do both DCE and DTE link management. The DLCI of the NNI and the DLCI of the DCE are defined as connections with FR_CIR encapsulation.

- A circuit between two NNI datalinks

  A circuit between two NNI datalinks (NNI to NNI) is similar to a DCE-to-DCE circuit except the NNI endpoints will do both DCE and DTE link management.

  In this setup, the DLCIs of the NNIs are defined as connections with FR_CIR encapsulation.

Terminal server commands

The terminal server has been modified to support additional frame relay commands. To view them, type:

```
ascend% sh fr ?
```

The output is similar to this:

```
sh fr ?Display help information
sh fr statsDisplay Frame relay information
sh fr lmiDisplay Frame relay LMI information
sh fr dlci[name]Display all DLCI information or just for [name]
sh fr circuitDisplay the FR circuit table
```

Viewing information about configured circuits

To display the status of FR circuits, type:

```
ascend% show fr circuits
```

The output is similar to this:

```
circuit1 User Setting
       frProf116Up
       frProf223Up

circuit2User Setting
       frProf224Down
       frProf518Up
```

The circuit field displays the circuit name. The User Setting field shows the admin state of the circuit. The administrator can stop the data flow of the circuit by using the SET CIRCUIT command (see “Turning off a circuit without affecting its DLCIs” on page 22).

The first profile name (such as frProf1) is the name of the Frame Relay Profile that represents one end-point of the circuit, and the DLCI number is this end of the circuit. The state of the circuit will be UP if the endpoint is active or DOWN if the endpoint is inactive.

Viewing frame relay statistics

To display FR statistics that include the type of connection, type:

```
ascend% show fr stats
```

The output is similar to this:

```
Name  Type Status  Speed  MTU  InFrame   OutFrame
fr1    DTE Up      56000  1532   0      0
fr2    DCE Up      56000  1532   0      0
fr3    NNI Up      56000  1532   0      0
```

The types of connections are:

- DCE (for UNI-DCE)
- DTE (for UNI-DTE)
- NNI (for NNI)

Changing the status of a datalink configured in RADIUS

Because there is not an easy way to start or stop a RADIUS Frame Relay profile, a SET command has been added to allow the user to perform a DO HANGUP on Frame Relay datalinks. The format of this SET command is:

```
set fr [mode] [name]
```

The name is the Frame Relay profile name. The specified mode (optional) may be one of the following:

- To display information about the SET FR command:

  ```
  ascend% set fr ?
  ```

  ```
  set fr ?            Display help information
  set fr do [name]    Do dial on the FR datalink
  set fr hangup [name]Do hangup on the FR datalink
  set fr remove [name]Remove the RADIUS FR datalink
  ```

- To dial the FR datalink, use the DO parameter.

  For example, this command dials a FR datalink named PacBell:

  ```
  ascend% set fr do PacBell
  ```

- To hang up the FR datalink, use the HANGUP parameter.

  For example, this command hangs up the FR datalink named PacBell:

  ```
  ascend% set fr hangup PacBell
  ```

- To remove from cache any FR profiles read in from RADIUS, use REMOVE.

  For example, this command clears the FR profile named PacBell:

  ```
  ascend% set fr remove PacBell
  ```

  This command clears any FR RADIUS profile in the MAX unit's cache:

  ```
  ascend% set fr remove
  ```

Note: Unless the FR profiles are removed from the RADIUS server's database, the FR datalink profile will be restored the next time the MAX reads RADIUS.

Turning off a circuit without affecting its DLCIs

There may be times when the administrator would like to "turn off" traffic going through a FR circuit without disabling the circuit endpoints. The SET CIRCUIT command provides that

functionality. It prevents traffic from going between endpoints without disrupting the state of the DLCI. The format of this command is:

```
set circuit [mode] [name]
```

The specified mode (optional) may be one of the following

- To display information about the SET CIRCUIT command:

  ```
  ascend% set circuit ?

  set circuit ?       Display help information
  set circuit active [name]  Set the CIRCUIT to active
  set circuit inactive [name]  Set the CIRCUIT to inactive
  ```

- To allow data to flow through a circuit, use the ACTIVE parameter.

  For example:

  ```
  ascend% set circuit active Circuit
  ```

- To turn off data flow without disrupting the state of the DLCIs, use the INACTIVE parameter.

  For example:

  ```
  ascend% set circuit inactive Circuit2
  ```

Hanging up a PPP call on a RADIUS timeout

By default, if authentication fails on a PPP connection because of a bad password or an authentication server timeout, the Ascend unit gracefully shuts down the PPP connection by sending an LCP-CLOSE request to the dial-up user. When Windows '95 (MSN) receives the LCP-CLOSE during authentication, it assumes a rejected password, and displays a message telling the user that his or her password is invalid.

If authentication fails because of a RADIUS timeout, this message gives the user incorrect information. Using the new “Disc on Auth Timeout” parameter, you can now specify that the Ascend unit simply hangs up a PPP connection on a RADIUS timeout without closing down cleanly. The resulting message to the user specifies that the network failed.

Disc on Auth Timeout

Description: This parameter enables you to specify whether the Ascend unit gracefully shuts down the PPP connection on a RADIUS timeout.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Ascend unit does not shut down cleanly, but simply hangs up a PPP connection on a RADIUS timeout.
- No specifies that the Ascend unit shuts down a call gracefully on a RADIUS timeout.

  No is the default.

Dependencies: If PPP=No, Disc on Auth Timeout=N/A.

Parameter Location: Answer Profile: Ethernet→Answer→PPP Options

See Also: PPP

R2 signaling support and Group B/Group II selection

The Ascend software now supports R2 signaling on the MAX E1 platform. R2 signaling is widely implemented in international markets where ISDN PRI is not yet available.

R2 signaling is a CCITT standardized signaling protocol, which can be used on E1 digital trunks for establishing and clearing 64Kbit/s switched circuits. Signaling is performed through a combination of A/B bit manipulation in channel 16 of the E1 frame (line signaling), and in-band MF tone generation/detection (register signaling).

Note: Refer to the Sys Option Menu to see if R2 signaling is installed. If not, a hash code may be obtained from Ascend Customer Service to enable it.

Configuring R2 signaling in the MAX

In the MAX, you configure R2 signaling in the Net/E1 line profile. In this release, you can explicitly configure Group B/Group II signal codes appropriately for your country. In addition, you can specify a wider range of acceptable address digits in the # Complete parameter.

Table 5 lists the new parameters and parameter values.

Table 5. R2 signaling configuration parameters

Location	Parameters
Net/E1→Line Config→Line N... (Line Profile)	Sig Mode=R2 # Complete Grp B Signal Grp II Signal

Sig Mode

Description: This parameter specifies the signaling that the line uses.

Usage: Press Enter to cycle through the choices.

- None indicates a leased line.
- ISDN specifies that the interface supports ISDN D-channel signaling.
  This setting is valid only if the MAX has the ISDN D-channel signaling option; otherwise, the MAX displays an error message.
  This setting is the default.
- DPNSS indicates that the interface supports DPNSS or DASS 2 signaling.
  DPNSS is another out-of-band signaling mode developed prior to ISDN. Its implementation in terms of channel usage varies from one country to another.
- R2 indicates that the interface supports R2 signaling.
  R2 signaling is a CCITT standardized signaling protocol, which can be used on E1 digital trunks for establishing and clearing 64Kbit/s switched circuits. Signaling is performed through a combination of A/B bit manipulation in channel 16 of the E1 frame (line signaling), and in-band MF tone generation/detection (register signaling).

Parameter Location: Line Profile: Net/E1→Line Config→Any Line Profile→Line *n*

Dependencies: When R2 is selected, the Switch Type parameter is N/A.

See Also: Switch Type, # Complete, Grp B Signal, Grp II Signal

Complete

Description: This parameter specifies how many digits of the incoming call number must be received before answering the call. It applies only to R2 signaling when the Ans *n* # parameter is being used to route incoming calls. The digits received before the call is answered are considered the "called number" for call routing purposes.

Note: This parameter must specify all significant digits of the answer number. If the R2 line supports end-of-pulsing tone, we recommend that setting to ensure that all significant digits are received before the call is answered.

Usage: Press Enter to cycle through the choices.

- 1 digit means that the call is answered when 1 digit of the called number has been received.
- 2 digits means that the call is answered when 2 digits of the called number have been received.
- 3 digits means that the call is answered when 3 digits of the called number have been received.
- 4 digits means that the call is answered when 4 digits of the called number have been received.
- 5 digits means that the call is answered when 5 digits of the called number have been received.
- 10 digits means that the call is answered when 10 digits of the called number have been received.
- end-of-pulsing means that the call is answered when the end-of-pulsing tone has been received.

  If the R2 line supports end-of-pulsing tone, select this option.

Dependencies: This parameter applies only to R2 signaling (Sig Mode=R2), and only when using the Ans *n* # parameters to route incoming calls.

Parameter Location: Line Profile: Net/E1→Line Config→Any Line Profile→Line *n*

See Also: Sig Mode, Ans *n* #

Grp B Signal

Description: When R2 signaling is in use, a Group B signal is sent immediately prior to answering an incoming call, and a Group II signal is sent immediately after an outgoing call is acknowledged by the called end that all necessary digits of the called number have been received.

This parameter specifies one of fifteen codes that can be selected for the Group B signal based on the country in which this signaling is being used. For example, Mexico and Korea use the following combination:

```
B-1
II-2
```

In Argentina it will probably be necessary to select the following combination:

```
B-6
II-1
```

For details about which code to select for your country, contact the telephone company.

Usage: Press Enter to cycle through the choices (B-1 through B-15).

Dependencies: This parameter applies only to R2 signaling (Sig Mode=R2).

Parameter Location: Line Profile: Net/E1→Line Config→Any Line Profile→Line *n*

See Also: Sig Mode, Grp II Signal

Grp II Signal

Description: When R2 signaling is in use, a Group B signal is sent immediately prior to answering an incoming call, and a Group II signal is sent immediately after an outgoing call is acknowledged by the called end that all necessary digits of the called number have been received.

This parameter specifies one of fifteen codes that can be selected for the Group II signal based on the country in which this signaling is being used. For example, Mexico and Korea use the following combination:

```
B-1
II-2
```

In Argentina it will probably be necessary to select the following combination:

```
B-6
II-1
```

For details about which code to select for your country, contact the telephone company.

Usage: Press Enter to cycle through the choices (II-1 through II-15).

Dependencies: This parameter applies only to R2 signaling (Sig Mode=R2).

Parameter Location: Line Profile: Net/E1→Line Config→Any Line Profile→Line *n*

See Also: Sig Mode, Grp B Signal

Interface support for MP call management

PPP connections are single-channel connections that connect to any other device running PPP. MP and MP+ are enhancements to PPP for supporting multi-channel links. In previous releases, if a connection was set up for “MPP,” the MAX first requested MP+. If the other side of the connection didn’t support MP+, the MAX would then request MP. If that protocol was also refused, PPP would be used instead.

In this release of the Ascend software, you can explicitly configure the RFC 1717 MP option. MP supports multi-channel links, but not DBA (dynamic bandwidth allocation). The base channel count is used to determine the number of calls to place, and the number of channels used for that connection does not change. In addition, MP requires that all channels in the connection share the same phone number (that is, the channels on the answering side of the connection must be in a hunt group).

These are the new parameters for configuring MP connections:

Location	Parameters
Ethernet→Connection→*any profile* (Connection Profile)	Encaps=MP
Ethernet→Answer→Encaps... (Answer Profile)	MP=Yes

Additions to SNMP support for RADIUS servers

Prior to this feature, if the MAX was using a secondary RADIUS authentication or accounting server, there was no command that forced the MAX to use its primary servers. Such a need might arise if the primary server had been shut down for service and was back up and available again.

These changes have been made to SNMP support for RADIUS to help network administrators control and monitor the current RADIUS accounting and authentication servers:

- You can now designate the primary RADIUS server through SNMP
- An SNMP trap is now sent whenever a different RADIUS accounting server or the RADIUS authentication server is designated as the primary server
- The Systems Options status screen now displays the IP address of the current RADIUS accounting server and authentication server

All Ascend Products that support SNMP in conjunction with RADIUS support these features.

Primary RADIUS servers now SNMP settable

You can now issue an SNMP set command to force the RADIUS server to be the primary server for the MAX. The first entry, Auth Host #1, in the Ethernet, Mod Config, Auth submenu is considered the primary RADIUS Authentication server. Similarly, the first entry, Acct Host #1, in the Ethernet, Mod Config, Accounting submenu is considered the primary RADIUS Accounting server.

An SNMP set command may be used to reset the primary RADIUS server being used for accounting or authentication. Each service can be independently reset.

The Object IDs for the SET command are as follows:

- radAuthCurrentServerFlag -> .1.3.6.1.4.1.529.13.3.1.12.0
- radAcctCurrentServerFlag -> .1.3.6.1.4.1.529.13.4.1.7.0

Every time the server is reset by this SET command, the MAX now generates an SNMP trap. The MAX also generates a trap if it changes to the next server because the current server failed to respond.

New MIB objects

These new MIB objects have been added to support changing the current RADIUS accounting server:

```
radAcctHostIPAddress OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The IP address of the Accounting server. The
             value 0.0.0.0 is returned if entry is invalid."
    ::= { radiusAcctStatsEntry 6 }


radAcctCurrentServerFlag OBJECT-TYPE
    SYNTAX      INTEGER {
                    invalid(1),
                    current(2)
                }
    ACCESS      read-write
    STATUS      mandatory
    DESCRIPTION"Value indicates whether this entry is the current
                 accounting server or not. Writing any value
                 will cause the current server to be reset to
                 the primary server (Host #1)."
    ::= { radiusAcctStatsEntry 7 }
```

These MIB objects have been added to support changing the current RADIUS authentication server:

```
radAuthHostIPAddress OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The IP address of the Authentication server. The
             value 0.0.0.0 is returned if entry is invalid."
    ::= { radiusAuthStatsEntry 11 }

radAuthCurrentServerFlag OBJECT-TYPE
    SYNTAX      INTEGER {
                    standby(1),
                    current(2)
                }
```

```
ACCESS      read-write
STATUS      mandatory
DESCRIPTION"Value indicates whether this entry is the current
             authentication server or not. Writing any value
             will cause the current server to be reset to
             the primary server (Host #1)."
::= { radiusAuthStatsEntry 12 }
```

SNMP trap for RADIUS server changes

The MAX now generates an SNMP trap whenever the a different RADIUS server is designated as the primary RADIUS server. This trap applies to the either the RADIUS authentication or the RADIUS accounting server.

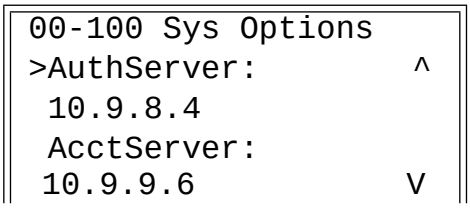
The trap is an “Enterprise Specific Trap (18)” and will be accompanied by the Object ID and IP address for the new server.

- The Object ID for Authentication Server is 1.3.6.1.4.1.529.13.3.1.11.x
- The Object ID for Accounting Server is 1.3.6.1.4.1.529.13.4.1.6.x

where x is the index of the current server (1-3).

System Options screen changes

The IP addresses of the current RADIUS authentication server and RADIUS accounting server are now displayed in the System Options screen, as shown below:



Transparent Telnet mode support

The terminal server interface now supports Transparent Telnet mode. In this mode, a user can send and receive files without having to be in Binary mode.

The Binary Mode parameter in the TServ Options submenu of the Ethernet Profile is now the Telnet Mode parameter. In addition, the telnet command in the terminal server interface includes a new -t option. These new features are described in the sections that follow.

New Telnet Mode parameter

Telnet Mode

Description: This parameter sets the default mode for a Telnet session that you start from the MAX.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Usage: Press Enter to cycle through the choices.

- ASCII specifies that the MAX uses standard 7-bit mode.

  In 7-bit mode, bit 8 is set to 0 (zero); 7-bit Telnet is also known as NVT (Network Virtual Terminal) ASCII.

  ASCII is the default.
- Binary specifies that the MAX attempts to negotiate the Telnet 8-bit binary option with the server at the remote end.

  The user can run X-Modem and other 8-bit file transfer protocols using this mode.
- Transparent specifies that the user can send and receive binary files without having to be in Binary mode.

  The user can run the same file transfer protocols available in Binary mode.

Dependencies: Keep this additional information in mind:

- Telnet Mode applies only if the MAX allows terminal server sessions (TS Enabled=Yes) and enables the user to establish a Telnet connection from a terminal server session (Telnet=Yes).

  A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. A terminal server session is an end-to-end connection between a terminal and a terminal server. Usually, the terminal server session begins when the call goes online and ends when the call disconnects.

  A terminal server session can be either local or remote:

  - A local terminal server session takes place when a terminal (or a computer emulating a terminal) is connected to the MAX unit's Control port, or when you open a Telnet connection to the MAX from a local IP host.

    In either case, you select the Term Serv command from the Sys Diag menu and press Enter to begin the terminal server session. A local terminal server session has access to only a subset of the commands available to a remote terminal server session.
  - A remote terminal server session takes place through a digital modem or through a V.110 or V.120 connection to the MAX.

    A digital modem is a device that can communicate over a digital line (such as a E1 PRI line) with a station that uses a modem connected to an analog line. V.110 and V.120 are both protocols for sending serial data over WAN lines.

    When you make a V.110 connection, the data is encapsulated in V.110 packets; when you make a V.120 connection, the data is encapsulated in V.120 packets. At the other end of the call, the MAX removes the encapsulation and the data appears as a serial data stream.

When you access a terminal server through a digital modem, V.110, or V.120 connection, the remote terminal server session begins immediately; you need not enter the Term Serv command.

- A user can override the Telnet Mode setting and choose ASCII mode, Binary mode, or Transparent mode by using the telnet command in the terminal server menu.
- In Binary and Transparent mode, the Telnet escape sequence does not operate.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→TServ Options

New -t option for the telnet command

You can now specify -a, -b, or -t in the telnet command line.

- -a specifies ASCII mode.
  This option indicates that the MAX uses standard 7-bit mode.
- -b specifies Binary mode.
  This option indicates that the MAX tries to negotiate 8-bit Binary mode with the server at the remote end of the connection.
- -t specifies Transparent mode.
  This option indicates that the user can send and receive binary files, and use 8-bit file transfer protocols, without having to be in Binary mode.

Each of these options overrides the setting of the Telnet Mode parameter.

Unit-specific control of dialout routes and addresses

This release enables you to create pseudo users for Ascend unit-specific configuration control of IP and IPX dialout routes, and for MAC addresses. The unit-specific dialout routes are loaded in addition to the global dialout routes. The MAC address configurations are added to the RADIUS database.

IP dialout routes

For a unit-specific IP dialout route, create a pseudo-user entry in this format:

```
route-<unit_name>-<number> Password="ascend", User-Service=Dialout-Framed-User
Framed-Route=<host ipaddr>[/<subnet mask>] <gateway ipaddr> <metric> [<private>] [<name>]
```

The global entry has this format:

```
route-<number> Password="ascend", User-Service=Dialout-Framed-User
Framed-Route=<host ipaddr>[/<subnet mask>] <gateway ipaddr> <metric> [<private>] [<name>]
```

Note: You should limit each entry to about 25 routes—that is, you should specify up to 25 settings for the Framed-Route attribute.

Table 6 describes each variable.

Table 6. IP dialout variables

Syntax element	Description
route-<unit_name>-<number> or route-<number>	Specifies the name of the unit-specific or global route. <unit_name> is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System Profile. <number> is a number in a sequential series, starting at 1.
<host ipaddr>[/<subnet mask>]	Indicates the IP address of a host or subnet reached by this route.
<gateway ipaddr>	Specifies the IP address of the gateway at the remote end of the connection.
<metric>	Indicates the metric for this route.
<private>	Specifies “y” if this route is private, or “n” if it is not private.
<name>	Indicates the outgoing RADIUS Connection Profile that the route uses.

Example

The first entry contains specifications for a unit-specific route; the second entry contains specifications for global routes.

```
route-alpha-1 Password = "ascend", User-Service = Dialout-Framed-User
        Framed-Route = "10.0.200.0/24 10.0.200.1 1 n inu-out"
route-1 Password = "ascend", User-Service = Dialout-Framed-User
        Framed-Route = "10.0.100.0/24 10.0.100.1 1 n homer-out"
        Framed-Route = "10.0.200.0/24 10.0.200.1 1 n inu-out"
```

How RADIUS adds IP dialout routes to the routing table

For IP dialout routes, these events take place:

1. RADIUS looks for entries having the format route-<unit_name>-1, where <unit_name> is the system name.
2. If at least one entry exists, RADIUS loads all entries having the format route-<unit_name>-<number> to initialize the IP routing table.
   The variable <number> is a number in a sequential series, starting with 1.
3. The Ascend unit queries route-<unit_name>-1, then route-<unit_name>-2, and so on, until it receives an authentication reject from RADIUS.
4. Once the host-specific routes are loaded, RADIUS loads the global configuration entries; these configurations have the form route-<number>.

5 The Ascend unit queries route-1, then route-2, and so on, until it receives an authentication reject from RADIUS.

IPX dialout routes

For a unit-specific IPX dialout route, create a pseudo-user entry in this format:

```
ipxroute-<unit_name>-<number> Password="ascend", User-Service=Dialout-Framed-User
Ascend-IPX-Route="<profile_name> <network#> [<node#>] [<socket#>] [<server_type>] [<hop_count>] [<tick_count>] [<name>]"
```

A global entry has this format:

```
ipxroute-<number> Password="ascend", User-Service=Dialout-Framed-User
Ascend-IPX-Route="<profile_name> <network#> [<node#>] [<socket#>] [<server_type>] [<hop_count>] [<tick_count>] [<name>]"
```

Note: You should limit each entry to about 25 routes—that is, you should specify up to 25 settings for the Ascend-IPX-Route attribute.

Table 7 describes each variable.

Table 7. IPX dialout variables

Argument	Description
ipxroute-<unit_name>-<number> or ipxroute-<number>	Indicates the unit-specific or global route. <unit_name> is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System Profile. <number> is a number in a sequential series, starting at 1.
<profile_name>	Specifies the RADIUS Connection Profile used to reach the network.
<network#>	Indicates the unique internal network number assigned to the NetWare server.
<node#>	Specifies the node number of the NetWare server to be reached through this route.
<socket#>	Indicates the socket number of the NetWare server to be reached through this route.
<server_type>	Specifies the SAP service type of the NetWare server.
<hop_count>	Indicates the distance to the destination network in hops.

Table 7. IPX dialout variables

Argument	Description
<tick_count>	Specifies the distance to the destination network in IBM PC clock ticks (one-eighteenth of a second). This value is for round-trip timer calculation and for determining the nearest server of a given type.
<name>	Indicates the name of an IPX server.

Examples

The first example defines a unit-specific IPX route; the second example defines a global IPX route.

```
ipxroute-CA-1 Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-IPX-Route = "def 6 7 8 9 10"
ipxroute-1 Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-IPX-Route = "abc 1 2 3 4 5 "
```

How RADIUS adds IPX dialout routes to the routing table

For IPX dialout routes, these events take place:

1. RADIUS looks for entries having the format ipxroute-<unit_name>-1, where <unit_name> is the system name.
2. If at least one entry exists, RADIUS loads all entries having the format ipxroute-<unit_name>-<number> to initialize the IPX routing table.

   The variable <number> is a number in a sequential series, starting with 1.
3. The Ascend unit queries ipxroute-<unit_name>-1, then ipxroute-<unit_name>-2, and so on, until it receives an authentication reject from RADIUS.
4. Once the host-specific routes are loaded, RADIUS loads the global configuration entries; these configurations have the form ipxroute-<number>.
5. The Ascend unit queries ipxroute-1, then ipxroute-2, and so on, until it receives an authentication reject from RADIUS.

MAC addresses

For a unit-specific bridging entry, create a pseudo-user entry in this format:

```
bridge-<unit_name>-<number> Password="ascend", User-Service=Dialout-
Framed-User
        Ascend-Bridge-Address="<MAC_address> <IP_address>"
```

Table 8 describes each variable.

Table 8. MAC address variables

Argument	Description
bridge-<unit_name>-<number>	Indicates the unit-specific bridging entry. <unit_name> is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System Profile. <number> is a number in a sequential series, starting at 1.
<MAC_address>	Specifies a MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it; that is, ":y" is the same as ":0y".
<IP_address>	Specifies an IP address in dotted decimal format.

Each Ascend-Bridge-Address setting specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX can form a bridging connection. When your MAX receives an ARP request for one of the IP devices you specify, the MAX replies with the corresponding MAC address. Because the MAX replies to these ARP requests as if the IP devices were local, you must have Connection Profiles that bridge IP packets to each device. Furthermore, if the links are not nailed up, they must be configured to dial out upon receipt of the ARP request.

Note: You can also specify entries for inclusion in the bridging table using the Bridging Profile in the MAX unit's menu-driven interface.

Example

This example creates two bridging table entries.

```
bridge-Ascend-1 Password="ascend", User-Service=Dialout-Framed-User
        Ascend-Bridge-Address="2:2:3:10:11:12 1.2.3.4 1"
        Ascend-Bridge-Address="2:2:3:13:14:15 5.6.7.8 2"
```

How RADIUS adds entries to the bridging table

For a MAC address configuration, these events take place:

1. RADIUS looks for entries having the format bridge-<unit_name>-<number>, where <unit_name> is the system name and <number> is a number in a sequential series, starting with 1.
2. RADIUS loads the data to create the bridging tables.

Terminal server idle timer

You can now set an idle timer for terminal server users. If a connection is idle for a period longer than the value you specify, the MAX disconnects the session. This feature applies to all MAX products.

Two parameters enables you to configure the idle timer—TS Idle Mode and TS Idle Limit. The RADIUS attribute analogous to TS Idle Mode is Ascend-TS-Idle-Mode (170). The RADIUS attribute analogous to TS Idle Limit is Ascend-TS-Idle-Limit (169). These parameters and attributes are described in the sections that follow.

New parameters

This section describes the parameters that enable you to set the terminal server idle timer.

TS Idle Mode

Description: This parameter specifies whether the MAX uses the terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.

Usage: Press Enter to cycle through the choices.

- None specifies that the MAX does not disconnect the session no matter how long the line is idle.

  This setting disables the idle timer.
- Input specifies that the MAX disconnects the session if the user is idle for a length of time greater than the value of the TS Idle Limit parameter.

  Input is the default.
- Input/Output specifies that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the TS Idle Limit parameter.

Dependencies: Keep this additional information in mind:

- The TS Idle Mode parameter does not apply (TS Idle Mode=N/A) if Encaps=FR or Encaps=TCP-CLEAR.
- The TS Idle Mode parameter in the Answer Profile does not apply (TS Idle Mode=N/A) if Use Answer as Default=No.
- TS Idle Mode in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its TS Idle Mode parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, TS Idle Mode does not apply (TS Idle Mode=N/A) in the Answer Profile.
- The RADIUS attribute analogous to the TS Idle Mode parameter is Ascend-TS-Idle-Mode (170).

Parameter Location: Answer Profile: Ethernet→Answer→Session Options
Connection Profile: Ethernet→Connections→Any Connection Profile→Session Options

See Also: Encaps, TS Idle Limit

TS Idle Limit

Description: This parameter specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.

Usage: Press Enter to open a text field. Then, enter a value between 0 and 65535. The default is 120. A setting of 0 (zero) means that the line can be idle indefinitely. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The TS Idle Limit parameter does not apply (TS Idle Limit=N/A) if Encaps=FR, Encaps=TCP-CLEAR, or TS Idle Mode=None.
- TS Idle Limit in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its TS Idle Limit parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, TS Idle Limit does not apply (TS Idle Limit=N/A) in the Answer Profile.
- The RADIUS attribute analogous to the TS Idle Limit parameter is Ascend-TS-Idle-Limit (169).

Parameter Location: Answer Profile: Ethernet→Answer→Session Options
Connection Profile: Ethernet→Connections→Any Connection Profile→Session Options

See Also: Encaps, TS Idle Limit

New RADIUS attributes

This section describes the RADIUS attributes that enable you to set the terminal server idle timer.

Ascend-TS-Idle-Limit (Attribute 169)

Description: This attribute specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.

Usage: You can specify a value between 0 and 65535.The default is 120. A setting of 0 (zero) means that the line can be idle indefinitely.

Dependencies: Keep this additional information in mind:

- Ascend-TS-Idle-Limit does not apply if you are using a Frame Relay or raw TCP connection, or if Ascend-TS-Idle-Mode=TS-Idle-None.
- The parameter analogous to the Ascend-TS-Idle-Limit attribute is TS Idle Limit.

See Also: Ascend-TS-Idle-Mode (Attribute 170)

Ascend-TS-Idle-Mode (Attribute 170)

Description: This attribute specifies whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.

Usage: You can specify one of these settings:

- TS-Idle-None (0)

  This setting specifies that the MAX does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.

- TS-Idle-Input (1)

  This setting specifies that the MAX disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute (169).

  TS-Idle-Input is the default.

- TS-Idle-Input-Output (2)

  This setting specifies that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute (169).

Dependencies: Keep this additional information in mind:

- Ascend-TS-Idle-Mode does not apply if you are using a Frame Relay or raw TCP connection.
- The parameter analogous to the Ascend-TS-Idle-Mode attribute is TS Idle Mode.

Example: This entry specifies that the user must be idle for 90 seconds before the MAX disconnects the session.

```
DEFAULT Password="UNIX"
        User-Service=Login-User,
        Ascend-TS-Idle-Limit=90,
        Ascend-TS-Idle-Mode=TS-Idle-Input
```

See Also: Ascend-TS-Idle-Limit (Attribute 169)

Support for IPXWAN negotiation

The Ascend software now supports the IPXWAN protocol, which is essential for communicating with Novell software that supports dialup connections, such as NetWare Connect2, and the Multi-Protocol Router.

For full specifications of the IPXWAN protocol, see RFC 1634 and *NetWare Link Services Protocol Specification—IPX WAN Version 2*.

IPX routing connections are established after IPX NCP has been negotiated successfully. In this release of the Ascend software, IPXWAN negotiation begins when IPX NCP has reached the OPEN state. The negotiation process differs based on the type of device communicating with the MAX:

- The Multi-Protocol Router or other Novell software that supports dialups

  For these connections, IPXWAN options supersede those negotiated by IPXCP.

- Novell software operating over PPP connections

  These connections do not negotiate options during the IPXCP phase, so all options are negotiated during the IPXWAN phase of link establishment.

- Another Ascend unit

  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.

IPXWAN negotiation consists of these steps:

1. The far-end device sends an IPXWAN Timer_Request packets.
   This triggers IPXWAN negotiation in the MAX.
2. 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 exchange.
3. The slave unit returns an IPXWAN Timer_Response packet.
4. The master unit initiates an exchange of information about the final router configuration.
   The MAX supports the following routing options:
   - Ascend Routing—Unnumbered RIP/SAP without aging.
   - Novell Routing—Unnumbered RIP/SAP with aging.
   - None—Peer is a Dialin Client. (No RIP/SAP except on request and we may assign Net and Node Numbers.)

   Header compression is rejected as a routing option.

After these steps are concluded, transmission of IPX packets begins, using the routing protocol negotiated.

New tsave command option: -m

By default, the text configuration file you can create using the tsave command contains the VT-100 interface parameter names. A new option, -m, has been added to the tsave command to allow you to save the configuration file with the MIB field numbers instead of the parameter names.

Note: The files created by tsave and tsave -m can both be restored by trestore.

All Ascend products support this new option.

To use the tsave command, you must first enter debug mode by quickly typing this four-character sequence

```
Esc [ Esc =
```

Then, to save the configuration of the Ascend unit with the MIB field numbers instead of parameter names, enter this command line:

```
tsave -m <ipaddr> <filename>
```

Consider this example:

```
tsave -m 200.253.164.100 all
```

This command line saves the entire configuration of the Ascend unit with an IP address of 200.253.164.100 to a file called “all”.

Values are saved in the format:

OOOO:MMMM.FFFF

where

- OOOO represents the Occurrence number (if > 0),
- MMMM represents MIB Type (if > 0),

- FFFF represents the MIB field number (if MMMM > 0).

Example

For example, the following text file results from performing a tsave on a MAX 200Plus:

```
START=FILT=900=0
Name=IP Call
In filter 01...Valid=Yes
Out filter 01...Valid=Yes
Out filter 01...Generic...Forward=Yes
Out filter 01...Ip...Forward=Yes
END=FILT=900=0
```

If you perform a tsave -m command, this file is output:

```
START=FILT=900=0
54.1=IP Call
1:54.2,55.1=Yes
1:54.3,55.1=Yes
1:54.3,1:55.4,55.2=Yes
1:54.3,1:55.5,55.2=Yes
END=FILT=900=0
```

Consider this line:

```
1:54.3,1:55.5,55.2=Yes (Out filter 01...Ip...Forward=Yes)
```

[Out Filter] This is the 1st Occurrence of the Out Filter array; “Out filter 01..." belongs to the 54th MIB type; and it is the 3rd field in that MIB type. Thus the MIB tag generated is 1:54.3.

[IP] This is the first occurrence of an IP filter; the “IP...” belongs to the 55th MIB type; and it is the 5th field in that MIB. Thus the MIB tag generated is 1:55.5.

[Forward] There are not multiple occurrences of this field so the occurrence number is 0; “Forward” belongs to the 55th MIB type; and it is the 2nd field of that MIB. Thus the MIB tag generated here is 55.2.

All three MIB tags are now assembled (comma separated) into a single MIB tag: 1:55.3,1:55.5,55.2.

BOOTP Relay

The Bootstrap Protocol (BOOTP) defines how a computer on a TCP/IP network can get from another computer its Internet Protocol (IP) address and other information it needs to start up. The computer that requests startup information is called the BOOTP client, and the computer that supplies the startup information is called the BOOTP server. A request for startup information sent from a BOOTP client to a BOOTP server is called a BOOTP request, and the BOOTP server’s response is called a BOOTP reply.

When the BOOTP client and BOOTP server are not on the same local-area network, the BOOTP request must be relayed from one network to another. This task, known as BOOTP relay, can be performed by a MAX.

A device that relays BOOTP requests to another network is known as a BOOTP relay agent. In addition to delivering BOOTP requests to servers, a BOOTP relay agent is responsible for delivering BOOTP replies to clients. In most cases, the agent is a router that connects the networks, such as a MAX.

Using BOOTP relay

By default, a MAX does not relay BOOTP requests to other networks. To enable the BOOTP relay feature for BOOTP clients connected to your MAX, follow these steps:

1 Get the IP addresses the BOOTP server or servers to be used.
You can specify up to two BOOTP servers, as described later in this section.

2 Open the configuration windows if they are not already open.

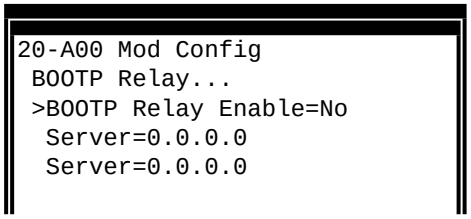
3 Open the Ethernet-->Mod Config menu.
For the location of this menu, see the manual.

4 Make sure SLIP BOOTP support is disabled by following these steps:

- Move the marker to TServ Options and then press the Return key.
- Move the marker to SLIP BOOTP.
- If the value of SLIP BOOTP is Yes, press the Return key to change it to No.

SLIP BOOTP makes it possible for a computer connecting to the MAX over a SLIP connection to use the Bootstrap Protocol. A MAX can support BOOTP on only one connection. If both SLIP BOOTP and BOOTP relay are enabled, you will receive an error message.

5 Move the marker to BOOTP Relay and then press the Return key.
The BOOTP Relay menu appears.



6 Move the marker to BOOTP Relay Enable.

7 Press the Return key repeatedly until the value Yes appears.

8 Move the marker to the first menu item named Server and then press the Return key.

9 In the text box that appears, enter the IP address of a BOOTP server.

10 Press Return to close the text box.

11 If there is another BOOTP server available, move the marker to the second menu item named Server and then press the Return key.
You are not required to specify a second BOOTP server.

Note: If you specify two BOOTP servers, the MAX that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

12 In the text box that appears, enter the IP address of the second BOOTP server.

13 Press Return to close the text box.

Parameter reference

BOOTP Relay Enable

Description: This parameter controls whether Bootstrap Protocol (BOOTP) requests are relayed to other networks.

Usage: Press Enter to cycle through the choices.

- Yes specifies that BOOTP requests are relayed.
- No specifies that BOOTP requests are not relayed.
  No is the default.

Dependencies: You must use the Server parameter to specify the address of at least one BOOTP server. The BOOTP Relay menu also includes a second Server parameter for specifying a second BOOTP server. If you specify two BOOTP servers, the MAX that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

For the BOOTP relay feature to work, DHCP Spoofing must be disabled.

Parameter Location: Mod Config, BOOTP Relay

See Also: Server

Server

Description: This parameter specifies a Bootstrap Protocol (BOOTP) server for handling BOOTP requests. If a server is on the same local-area network as the MAX, BOOTP requests from other networks are relayed to the server. If a server is on another network, BOOTP requests from clients on the same local-area network as the MAX are relayed to the remote server.

Note: This parameter appears twice. Each copy can be used to specify a different BOOTP server.

Usage: Press Enter to open a text field and then type the IP address of the BOOTP server. When you're done, press Enter to close the text field.

Dependencies: If you specify two BOOTP servers, the MAX that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Parameter Location: Mod Config, BOOTP Relay

See Also: BOOTP Relay Enable

Point-to-Point Tunneling Protocol (PPTP)

PPTP (Point-to-Point Tunneling Protocol) is supported in this release of the Ascend software, enabling the MAX to concentrate up to 96 incoming calls from Windows 95 or Windows NT clients and route them directly to up to four Windows NT servers. The MAX acts as a front-end processor, off-loading the overhead of communications processing from the Windows NT servers.

A PPTP session occurs between the MAX and a Windows NT server over a special TCP control channel. Either end may initiate a PPTP session and open the TCP control channel. Note that opening a PPTP session does not mean that a call is active, it simply means that a call can now be placed and received.

Figure 1 shows a MAX acting as a PAC (PPTP Access Controller), which answers the incoming calls and routes the call and incoming user data packets to the appropriate server. The PAC is one end of a PPTP tunnel.

The other end of the PPTP tunnel is the PNS (PPTP Network Server)—a Windows NT server.

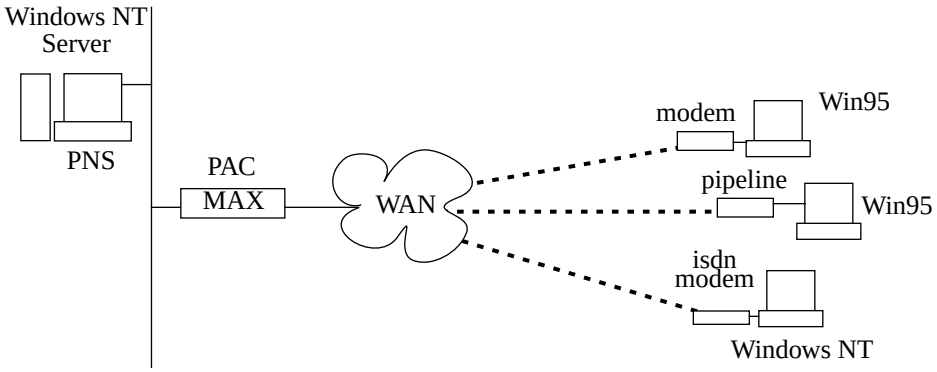


Figure 1. PPTP tunnel on Ethernet

Please note that the MAX and the NT Server do not need to be on the same subnet. Typically, the MAX will be located at an ISP Point of Presence with the NT Server on the customers premise, as shown in Figure 2.

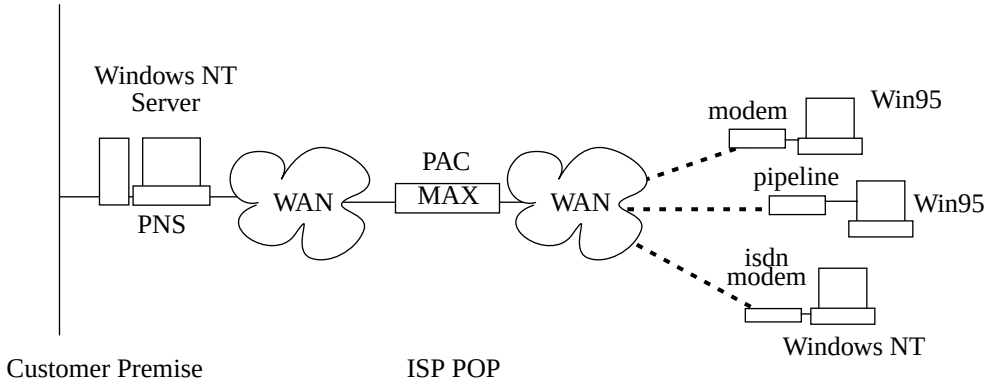


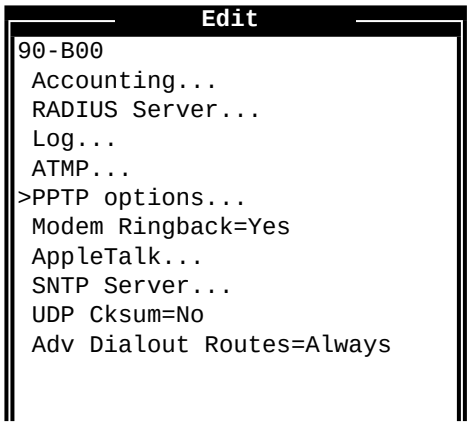
Figure 2. PPTP tunnel across the WAN

The configuration shown in Figure 2 enables Virtual Private Networks (VPN) over a public network such as the Internet.

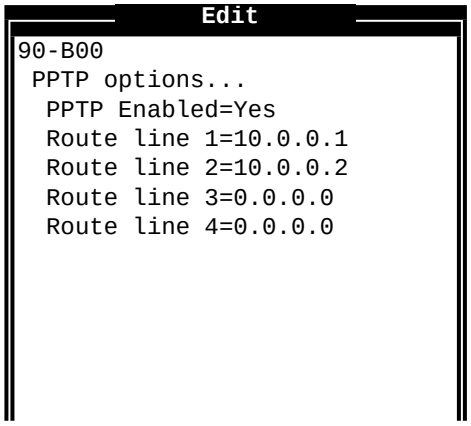
Configuring the MAX as a PAC

To configure the MAX to communicate with an NT server (a PNS) through a PPTP tunnel:

1 Open the Ethernet Profile and scroll down to select the PPTP Options submenu.



2 Open the PPTP options submenu.



3 Turn on PPTP.

```
PPTP Enabled=Yes
```

4 Specify the IP address of at least one (and up to four) NT servers.

For example:

```
Route line 1=10.0.0.1
Route line 2=10.0.0.2
```

5 Close the Ethernet Profile.

See “PPTP parameters,” next, for more details.

PPTP parameters

This section describes the PPTP parameters.

PPTP Enabled

Description: This field enables or disables PPTP (Point-to-Point Tunneling Protocol) functionality in the Ascend unit. When PPTP is enabled, the MAX can initiate a PPTP tunnel with a PNS (PPTP Network Server) by opening the TCP control channel to that device. It can also respond to a request for a PPTP tunnel from a PNS.

Note: If PPTP Enabled is set to Yes and the four Route Line parameters are left with their default values (0.0.0.0), the MAX assumes that all incoming calls are PPTP calls. The MAX will no longer be a router. If there is no established PPTP session between the MAX and a server, then the call will be dropped.

Usage: Press Enter to toggle between Yes and No.

- Yes enables PPTP.
- No disables PPTP.
  No is the default.

See Also: Route Line N

Parameter Location: Ethernet Profile, PPTP Options submenu

Route Line N (N=1–4)

Description: These four parameters define the IP address of the PNS (PPTP Network Server) to which calls received on the given line will be routed. A PNS is a Windows NT server that communicates with the MAX on a TCP control channel.

“Line 1" represents the first WAN line (such as an ISDN BRI or E1 PRI line). “Line 2" is the second WAN line, and so forth. For example, if a call comes in on Line 1 and the Route Line 1 parameter has a valid IP address, the MAX forwards the call to that address. If necessary, the MAX first requests a PPTP session with the PNS at that address and then forwards the call.

Note: When a call comes in on a WAN line whose Route Line parameter has the default zero address (0.0.0.0), the MAX handles the call like a normal (non-PPTP) call and routes it internally. However, if PPTP Enabled is set to Yes and *all* of the Route Line parameters have the default zero address, *all* calls are assumed to be PPTP calls. The MAX will no longer be a router. If there is no established PPTP session between the MAX and a server, then the call will be dropped.

Usage: Press Enter to open a text field. Then specify a valid IP address. For example:

```
10.1.2.3
```

Press Enter again to close the text field.

Dependencies: If PPTP Enabled is set to No, these fields are N/A.

See Also: PPTP Enabled

Parameter Location: Ethernet Profile, PPTP Options submenu

Unique session IDs

Previously, if a customer is using Call accounting via RADIUS, it was possible that the MAX will reset and reuse a session ID that was previously in use. Now, for every session, a unique session ID will be generated to prevent the possibility that session IDs will be used for more than one session.

There is a slight change to the output file created by RADIUS Accounting. Instead of the session IDs starting at 2, when the MAX powers up the session IDs will start at a random decimal number, usually 7 digits long.

Overriding the Answer Profile default

Previously, when validating an incoming call using RADIUS or TACACS, the Ascend unit did not use the Answer Profile, but the factory default Internet Profile. A new parameter, Use Answer as Default, enables you to govern which profile is used. You can also set the IP routing metric for the call with the Metric parameter, now found in the Ethernet→Answer→IP Options menu.

Use Answer as Default

Description: This parameter indicates whether the Answer Profile should override the factory default Internet Profile when the Ascend unit validates an incoming call using RADIUS or TACACS.

Usage: Press Enter to toggle between Yes and No.

- Yes indicates that the Ascend unit uses the Answer Profile.
- No indicates that the Ascend unit uses the factory default.
  No is the default.

Parameter Location: Answer Profile: Ethernet→Answer

Metric

Description: This parameter appears in an Answer Profile, a Connection Profile, and a Route Profile. Its functionality differs depending on the profile:

- In an Answer Profile, the Metric parameter determines the virtual hop count of the IP link when the MAX validates an incoming call using RADIUS or TACACS and Use Answer as Default=Yes.
- In a Connection Profile, the Metric parameter determines the virtual hop count of the link.
- In a Route Profile, the Metric parameter determines the virtual hop count of the route.

If there are two routes available to a single destination network, you can ensure that the MAX uses any available nailed-up channel before using a switched channel by setting the Metric parameter to a value higher than the metric of any nailed-up route. The higher the value entered, the less likely that the MAX will bring the link or route online. The MAX uses the lowest metric.

Usage: Press Enter to open a text field, Then, type a number between 1 and 15. This value is the virtual hop count. The default setting is 7. Press Enter again to close the text field.

Example: If a route to a station takes three hops over nailed-up lines, and Metric=4 in a Connection Profile that reaches the same station, the MAX does not bring the Connection Profile's link online.

Dependencies: Keep this additional information in mind:

- The Metric parameter in an Answer Profile or a Connection Profile does not apply to bridged connections, such as Combinet links (for which Encaps=COMB).
- In the Answer Profile, the Metric parameter does not apply (Metric=N/A) if Route IP=No or Use Answer as Default=No.
- If you enable RIP (Routing Information Protocol) across the WAN in a Connection Profile or an Answer Profile (RIP=Recv or RIP=Both), the hop count for the route can differ from the value of the Metric parameter in the Route Profile because the MAX always uses the lower hop count.
- The hop count includes the metric of each switched link in the route.

Parameter Location: Answer Profile: Ethernet→Answer→IP Options menu
Connection Profile: Ethernet→Connections→Any Connection Profile→IP Options
Route Profile: Ethernet→Static Rtes→Any Route Profile

See Also: Private, RIP

PPP direct negotiation in the terminal server

The Ascend software now supports a PPP Direct parameter that instructs the terminal server to begin negotiating a PPP session immediately when a user enters this command at the terminal server prompt:

```
ascend% ppp
```

The default behavior of the MAX is to enter a receive mode in which it waits to receive PPP packets from the user's workstation. However, some client software expects to receive packets from the MAX before returning PPP packets. If PPP Direct is set to Yes, the MAX begins PPP negotiation immediately, enabling those clients to connect successfully..

Table 9. New PPP Direct parameter

Location	Parameter
Ethernet→Mod Config→TServ options... (Ethernet Profile)	PPP Direct=No

PPP Direct

Description: This parameter instructs the MAX to begin PPP negotiation as soon as a user enters the PPP terminal server command.

Usage: Press Enter to toggle between Yes and No.

- Yes indicates that PPP/LCP negotiation will begin immediately.
- No indicates that the MAX will wait to receive PPP packets from the remote peer. No is the default.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→TServ Options

See Also: PPP, PPP Delay

Cellular modem support

The MAX now supports cellular modem calls. The user can also set the gain level of the modem for cellular communication.

This feature is available on Ascend products with programmable digital modem V.34 slot cards.

New parameters

The following parameters have been added to the Ethernet, Mod Config/TServ options submenu to support cellular modems.

Cell First

Description: This parameter specifies whether the MAX first attempts cellular modem or conventional modem negotiation when answering incoming calls. If the first negotiation fails, the MAX attempts the other negotiation.

Usage: Press Enter to cycle through the choices:

- Yes specifies that the MAX will first attempt cellular modem negotiation.
- No specifies that the MAX will first attempt conventional modem negotiation.

No is the default.

Dependencies: This parameter is never N/A.

Parameter Location: Ethernet, Mod Config, TServ options

See Also: Cell Level

Cell Level

Description: This parameter determines the gain level of the cellular modem.

Usage: Press Enter to cycle through the choices:

- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18

18 is the default.

Dependencies: This parameter is never N/A.

Parameter Location: Ethernet, Mod Config, TServ options

See Also: Cell First

How it works

When an incoming call is routed by the MAX to one of its digital modems, the modem answers the call by issuing an AT command string to the selected modem. This answer string has been modified with the following command for support of cellular modems:

sec=X,Y

where X is the parameter that selects whether the modem negotiates land-based or cellular first, and Y is the modem gain used for cellular communication. For example, if Cell First=No and Cell Level=18 is set in the TServ options menu, the command would be:

-sec=0,18

Command strings reported through SNMP

Note that the modem command string is broken into two discrete command strings with the addition of the cellular command because the command buffer on the V.34 modems is only 58 characters long. This change is transparent except when accessing the modem strings through SNMP. In this case, what is returned to the Modem MIB has changed and looks like the following:

```
Name:.iso.org.dod.internet.mgmt.mib.38.1.8.1.2.1.1
OCTET STRING- (ascii): AT&F0-sec=0,18&C1V0W1X4.AT%C3
N3S2=255S95=44+MS=11,1,300,28800A.
```

This example is for the first string on the first modem, with Cell First=No and Cell Level=18. The “.” in the middle and end of the AT command string are carriage returns.

Changing passwords in a terminal server session

The Ascend software now supports a PASSWORD command that enables RADIUS-authenticated terminal server users to change their passwords.

Note: To use this feature, you must download the latest RADIUS daemon and dictionary file from the Ascend FTP server.

The PASSWORD command uses the same mechanism that enables users to enter a new password when an older one has expired. For that reason, password expiration must be enabled in the user’s profile for the new PASSWORD terminal server command to work. To enable password expiration, include the Ascend-PW-Expiration attribute on the line defining the user and password; for example:

```
balsup Password = "test", Ascend-PW-Expiration ='May 15, 1996'
```

If users have password expiration enabled in their RADIUS profiles, the HELP command in the terminal server interface displays the new PASSWORD command. When executing the PASSWORD command, users are prompted to enter the current (old) password, the new password, and to re-enter the new password:

```
ascend% password
Enter old password:
Enter new password:
Re-type new password:
```

New password cannot be NULL, and must differ from the old password. If the password change is successful, the user will see:

```
Password Updated
```

If the update fails for any reason, the user will see:

```
Password NOT Changed
```

There is no other indication of why the password change failed. Typical problems may be that the old password entered was incorrect, or that the password is not being stored in the RADIUS database (for example, if the user's password is a UNIX password).

Immediate modem service

In Ascend units that support the modem dialout feature, this release of the Ascend software supports a new "immediate modem" feature that enables users on the local network to access a modem without entering the terminal server interface. Previously, the modem dialout feature could be accessed only from the terminal server interface—a user would Telnet to the MAX and then issue the command "open <modem number>" at the terminal server command-line.

Immediate modem service enables users to access a modem by specifying a reserved port number on the Telnet command line. For example, a PC user can access a digital modem in a MAX unit named "max1" by issuing this command in the PC Telnet software:

```
telnet> open max1 5000
```

The user can then begin entering AT commands to dial out.

The TCP port number configured for immediate modem tells the MAX that all Telnet sessions initiated with that port number want immediate modem service. Unlike the modem dialout feature invoked from the terminal server interface, the user cannot escape out of an immediate modem session by entering the ^C^C^C code. If the user enters that code, the Telnet session is terminated.

To support the immediate modem feature, two new parameters have been added:

Table 10. Immediate modem configuration parameters

Location	Parameters with example values
Ethernet/Mod Config/TServ options.... (Ethernet Profile)	Immediate Modem=Yes Imm. Modem port=5000

Immediate Modem

Description: This parameter enables or disables the immediate modem feature.

Usage: Press Enter to toggle between Yes and No.

- Yes enables immediate modem dialout service for users who Telnet to the MAX and specify the Imm. Modem port number on the Telnet command line.

- No (the default) turns off the immediate modem feature.

Parameter Location: Ethernet/Mod Config/TServ Options (Ethernet Profile)

Dependencies: This parameter is N/A if TServ Enabled is No.

See Also: Imm. Modem port

Imm. Modem port

Description: This parameter specifies a TCP port number associated with immediate modem service. When a user on the local network initiates a Telnet session with this port number on the Telnet command line, the MAX invokes immediate modem service. Unlike the modem dialout feature invoked from the terminal server interface, the user cannot escape out of an immediate modem session by entering the ^C^C^C code. If the user enters that code, the Telnet session is terminated.

Usage: Press Enter to open a text field, and then type a number from 5000–65535 (default 5000). Press Enter again to close the text field.

Parameter Location: Ethernet/Mod Config/TServ Options (Ethernet Profile)

Dependencies: This parameter is N/A if TServ Enabled is No.

See Also: Immediate Modem

MP/MP+ calls across multiple MAX units

This feature allows incoming Multilink PPP (MP) or MP+ calls to span multiple MAX units on a single LAN. This is done by allowing multiple MAX units to act a single, logical unit, or "stack." MP/MP+ call spanning is protocol independent and therefore works with all protocols supported by the MAX.

Note that call spanning works only with incoming calls. If a MAX wants to place another call but has no available lines a stack will not help. A stack is only effective when a MAX running MP+ is asked for another phone number and has no available lines, or when a rotary is used to access multiple MAX units via the same phone number, thus making it impossible to guarantee that a subsequent call is answered by the same MAX as the original call.

Note: A stack currently does not allow for the sharing of Connection Profiles between MAX. This means that all MAX units in a stack must contain all authentication information for every call or all MAX units in a stack must use a centralized authentication server like RADIUS.

A MAX can become a member of exactly one stack, though there is no requirement that a MAX become a member of a stack. Multiple stacks may exist on the same LAN by simply having different stack names.

How call spanning works

A stack is group of MAX units that are assigned a single stack name. There is no "master" MAX unit in a stack. Any MAX can become a member of a single stack or leave a stack at any time. The MAX units that are in the stack find each other by using an Ethernet multicast packet. Since these multicast packets are unlikely to cross a router, and because of the high

traffic demands created by a MP/MP+ call that spans MAX units, all members of a stack must reside on the same physical LAN.

Once a stack is created every MP/MP+ call that comes into a member of the stack will be compared with MP/MP+ calls on other members of the stack. This is done to determine if the call is part of an already existing bundle. If this call is a new MP/MP+ bundle then it will proceed as normal. If the call is part of an already existing bundle then information about the bundle will be exchanged between the two MAX units.

The MAX that has answered the subsequent call will forward all data packets, via the Ethernet, to the MAX that owns the MP/MP+ bundle. Data packets destined for the WAN will be split between the available channels normally. Those packets that are destined for a WAN interface that is not local to the MAX that owns the bundle will be forwarded, via the Ethernet, to the appropriate MAX to be sent across the WAN link.

In the case of an MP+ call that must add a subsequent channel to an existing bundle the MAX must provide a phone number. In the case of a MAX stack the MAX that owns the bundle will attempt to provide a local phone number. If no phone number is available then the MAX will ask other members of the stack for an available phone number to use for the subsequent channel.

New parameters

Three new parameters have been added for the MAX stacks. These parameters are all located in the Stack Options submenu in the Ethernet-> Mod Config Profile.

Stack Enabled

Description: This parameter specifies whether stacks are enabled on this MAX unit. When a MAX belongs to a stack, it can share MP/MP+ calls among all members of a stack.

Usage: Press Enter to cycle through the choices:

- Yes enables Stacks on this MAX unit.
- No disables Stacks on this unit.
  No is the default.

Parameter Location: Ethernet>Mod Config>Stack Options

Dependencies: Keep this additional information in mind:

- Every member of a stack must reside on the same LAN.
- A MAX unit can only belong to a single stack.

See Also: Stack Name, UDP Port

Stack Name

Description: This parameter specifies the name of name that identifies a MAX to the rest of the members of a stack. This name must be identical on all MAX units in a stack.

Usage: Press Enter to open a text field. Then, type the name of the Stack to which this MAX belongs. Because the stack name is used in MP/MP+ for identifying bundles, the stack name must be unique among all MAX stacks that may communicate with each other. A stack name must 16 characters or less.

Press Enter again to close the text field.

Parameter Location: Ethernet>Mod Config>Stack Options

Dependencies: Keep this additional information in mind:

- The stack name must be unique among all MAX stacks that may communicate with each other.
- Multiple stacks can exist on the LAN.
- Stack Name is not applicable (Stack Name=N/A) if Stack Enabled=No.

See Also: Stack Enabled, UDP Port

UDP Port

Description: This parameter specifies the UDP port that members of a stack use for communication. The UDP port must be identical in all members of a stack, but is not required to be unique among all stacks.

Usage: Press Enter to open a text field. Then, type the number of the UDP port used for intrastack communication.

Press Enter again to close the text field.

Parameter Location: Ethernet>Mod Config>Stack Options

Dependencies: Keep this additional information in mind:

- UDP Port is not applicable (UDP Port=N/A) if Stack Enabled=No.

See Also: Stack Enabled, Stack Name

Multicast forwarding and IGMP functionality

In the IP-only release for the MAX 4000, IGMP (Internet Group Membership Protocol) version-1 and version-2 have been implemented, along with configuration options that enable the MAX to communicate with the multicast routers and forward multicast traffic for the groups it maintains. Figure 3 shows the MAX communicating with a multicast router on its Ethernet interface and forwarding multicast traffic to dial-in multicast clients.

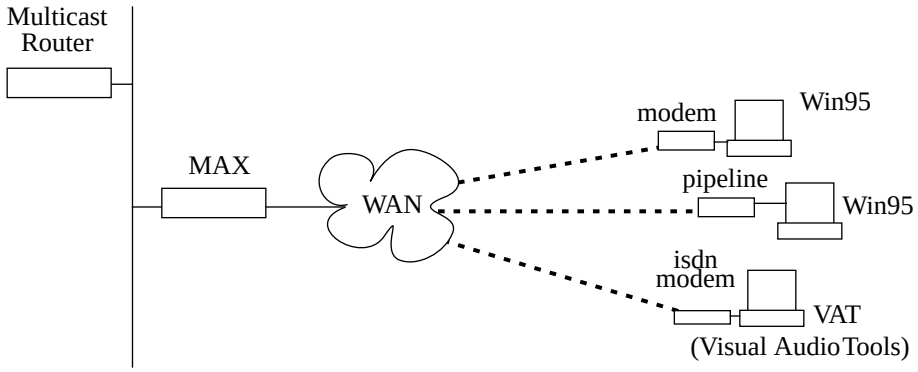


Figure 3. MAX forwarding multicast traffic to dial-in multicast clients

To communicate with an MBONE router, the MAX acts as a multicast client—it receives queries from the router and responds to them using IGMP. The multicast (MBONE) router may reside on its Ethernet interface or across a WAN link. If the router is accessed across the WAN, the MAX may respond to multicast clients on its Ethernet interface as well as across WAN links.

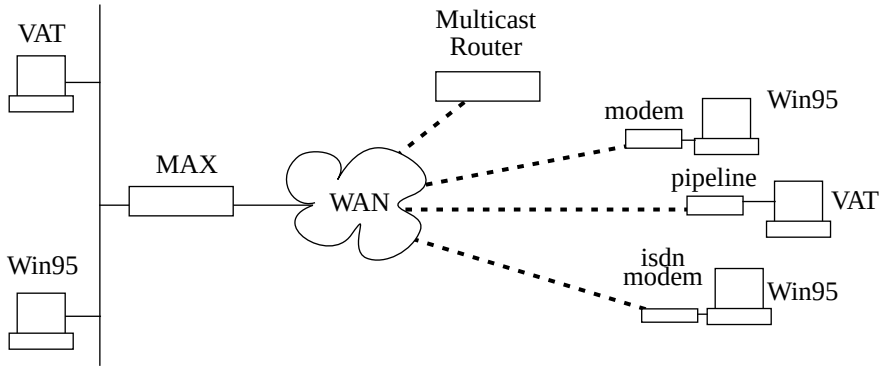


Figure 4. MAX acting as a multicast forwarder on Ethernet and WAN interfaces

To communicate with multicast clients, the MAX sends the clients IGMP queries every 60 seconds, receives responses, and forwards multicast traffic. To the clients it looks like a multicast router, although in fact the MAX is forwarding multicast packets based on group memberships. In this implementation, multicast clients are not allowed to source multicast packets—if they do, the MAX discards the packets.

When multicasting is enabled in the MAX, it builds a multicast forwarding table. Based on IGMP messages it exchanges, the MAX creates new group memberships or refreshes existing ones in its multicast forwarding table. When the MAX receives IP multicast packets from its MBONE interface, it checks its multicast forwarding table and forwards the packets to its multicast clients according to group membership.

When it creates a new group membership, it sends a JOIN message on its MBONE interface. When the last member of a group is no longer active, if the MBONE interface supports a multicast router running IGMP, the MAX sends a LEAVE message.

Configuring the MAX for multicast forwarding

Table 11 lists the MAX 4000 parameters related to MBONE functionality:

Table 11. MAX 4000 multicast configuration parameters

Location	Parameters with example values
Ethernet/Mod Config (Ethernet Profile)	Multicast Forwarding=Yes Mbone Profile=boomer Multicast Client=Yes
Ethernet/Connection/any profile (Connection Profile)	Multicast Client=Yes

Multicast Forwarding

Description: This parameter turns on the multicast forwarding functionality in the MAX. By default, it is set to No.

Usage: Press Enter to toggle between Yes and No.

- Yes turns on multicast forwarding functionality.
  When set to Yes, the MAX appears to an MBONE router as a multicast client, which receives IGMP (Internet Group Membership Protocol) queries from the router and responds to them using IGMP. To dial-in clients, it appears as a multicast router, which sends IGMP queries and forwards multicast traffic.
- No (the default) turns off multicast forwarding.

Parameter Location: Ethernet/Mod Config (Ethernet Profile)

Dependencies: This parameter is available only in the IP-only release for the MAX 4000.

See Also: Mbone Profile, Multicast Client

Mbone Profile

Description: This parameter can specify the name of a Connection Profile for a WAN link to a multicast router. If no profile name is specified and Multicast Forwarding is turned on, the MAX assumes that its Ethernet is the MBONE interface.

In this release, the specified Connection Profile must be resident. (It cannot be accessed via a RADIUS or TACACS server.)

Usage: Press Enter to open a text field. Then, type the name of the Connection Profile to the MBONE interface. If no name is specified, the MAX assumes the presence of a multicast router on its Ethernet interface. Press Enter again to close the text field.

Parameter Location: Ethernet/Mod Config (Ethernet Profile)

Dependencies: This parameter is available only in the IP-only release for the MAX 4000. This parameter is N/A if Multicast Forwarding is set to No.

See Also: Multicast Forwarding, Multicast Client

Multicast Client

Description: This parameter specifies that multicast clients are supported on this interface. In the Ethernet Profile, this parameter takes effect only when the MBONE interface is a WAN link.

Usage: Press Enter to toggle between Yes and No.

- Yes turns on multicast client functionality.
  When set to Yes, the MAX sends IGMP (Internet Gateway Membership Protocol) queries across this interface every 60 seconds and receives responses from or forwards messages for multicast clients.
- No (the default) instructs the MAX not to support multicast clients on this interface.

Parameter Location: Ethernet/Mod Config (Ethernet Profile)
Ethernet/Connection/any profile (Connection Profile)

Dependencies: This parameter is available only in the IP-only release for the MAX 4000. In the Ethernet Profile, this parameter is N/A unless a Connection Profile name has been specified in the Mbone Profile parameter.

See Also: Multicast Forwarding, Mbone Profile

Description:

Terminal server commands for multicast forwarding and IGMP

The SHOW commands described in this section have been added to the terminal server command-line to support multicast functionality. To use them, first invoke the terminal server interface (System/Sys Diag/Term Serv).

To display all the active multicast group addresses and the clients(interfaces) registered for that group, type:

```
ascend% show igmp groups
```

The output is similar to this:

```
IGMP Group address Routing Table Up Time: 0::0:22:17
 Hash      Group Address    Members    Expire time   Counts
  10       224.0.2.250
                             2           0:3:24       3211 :: 0 S5
                             1           0:3:21       145 :: 0 S5
                            0(Mbone)    ......       31901 :: 0 S5
```

- Hash is an index to a hash table (displayed for debugging purposes only).
- Group address is the IP multicast address used in this packet.
- Members is the interface ID on which the membership resides. 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled "Mbone" is the interface on which the multicast router resides.
- Expire time indicates when this membership expires. The MAX sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. When this field contains periods, it means that this membership never expires.
- Counts shows the number of packets forwarded to the client, the number of packets dropped due to lack of resources, and the state of the membership (the state is displayed for debugging purposes).

To list all IGMP multicast clients, type:

```
ascend% show igmp clients
```

The output is similar to this:

```
IGMP Clients

 Client      Version  RecvCount  CLU      ALU
  0(Mbone)      1        0          0       0
  2             1       39         68       67
  1             1    33310         65       65
```

- Client indicates the interface ID on which the client resides. 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they

became active. The interface labeled "Mbone" is the interface on which the multicast router resides.

- Version is the version of IGMP being used.
- RecvCount is the number of IGMP messages received on that interface.
- CLU (current line utilization) and ALU (average line utilization) show the percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

To display IGMP activity statistics, type:

```
ascend% show igmp stats
```

The output shows the number of IGMP packet types sent and received. It uses this format:

```
46 packets received.
 0 bad checksum packets received.
 0 bad version packets received.
 0 query packets received.
46 response packets received.
 0 leave packets received.
51 packets transmitted.
47 query packets sent.
 4 response packets sent.
 0 leave packets sent.
```

To display statistics about multicast traffic, such as how many multicast packets have been forwarded or dropped, type:

```
ascend% show mrouting stats
```

The output shows the number of multicast packets received and forwarded. In many cases, the number of packets forwarded will be greater than the number of packets received, because packets may be duplicated and forwarded across multiple links. The output uses this format:

```
34988 packets received.
57040 packets forwarded.
    0 packets in error.
   91 packets dropped.
    0 packets transmitted.
```

Ascend-Multicast-Client (Attribute 152)

Description: This RADIUS multicast attribute determines when the user is a multicast client. That is, setting this attribute to Multicast - Yes(1), instructs the NAS (which is the MAX) to send IGMP queries to this client every 60 seconds. Based on the responses it receives, it creates new group memberships or refreshes existing ones in its multicast forwarding table. When the MAX receives IP multicast packets from its MBONE interface, it checks its multicast forwarding table and forwards the packets to its clients according to group membership. In effect, it acts as a proxy host for its multicast clients.

X.25 support

The sections that follow describe X.25 support on the MAX. Full technical specifications for X.25, X.3, X.28, X.29, and LAPB (Link Access Protocol–Balanced) can be found in the IETF RFC series and in the CCITT Blue Book Recommendation X series 1988.

What is X.25?

X.25 is an international standard protocol established by the Consultative Committee on International Telephony and Telegraphy (CCITT) to transmit information between users over a WAN. It handles both high-volume data transfers and interactive use of host machines. As a full-duplex, connection-oriented protocol, X.25 uses virtual circuits and provides services such as multiplexing, in-sequence delivery, transfer of addressing information, segmenting and reassembly, flow control, transfer of expedited data, error control, reset, and restart. Allocation of logical channels can be either static (using a PVC or Permanent Virtual Connection) or dynamic (using an SVC or Switched Virtual Connection).

X.25 exchanges packets between a local packet DTE (Data Terminal Equipment) and a remote packet DCE (Data Circuit-Terminating Equipment). The remote DCE is itself attached to a remote DTE.

- A DTE is a device that an operator uses, such as a computer or a terminal.
- A DCE is a device that connects a DTE to a communications channel.

  At the sending end, the DCE converts the data coming from the DTE into a signal suitable to the communications channel. For example, the local DCE might be an analog modem that converts the local DTE's digital signals into analog form for transmission over an analog telephone line.

  At the receiving end, the DCE converts the signal into a form suitable for reception at the DTE. For example, the DCE might be a digital modem that converts analog signals into digital format for reception at the DTE.

Understanding X.25/PAD

A PAD (Packet Assembler/Disassembler) is an asynchronous terminal concentrator that enables several terminals (or other asynchronous devices) to share a single network line. The PAD assembles data from terminals into packets for transmission to an X.25 network, and disassembles incoming packets from the network into a separate data stream for each terminal. In addition to this multiplexing function, the PAD also provides a nearly error-free connection.

PAD-generated packets are transported using the X.25 protocol. The MAX unit's X.25/PAD implementation allows users to access a public or private packet-switched (PSPDN) network over a leased line or a nailed-up ISDN connection.

When a user calls X.25/PAD through a modem, the terminal server performs the authentication, and selects a Connection Profile. The user is authenticated using a local Connection Profile or a RADIUS user profile.

Authentication using a local Connection Profile

If the local Connection Profile indicates that the user is an X.25/PAD user (using the setting Encaps=X.25/PAD), the MAX directs the call to the PAD. The MAX also obtains the name of an X.25 Profile from the Connection Profile. This profile determines the physical interface at which to establish the X.25 connection, and sets the parameters for the call.

Note: The current implementation supports only a single physical interface.

No authentication

1. If the user is not authenticated and TS Enabled=Yes, the terminal server prompt appears and the MAX assigns the first active X.25 Profile to the user. From the regular terminal server prompt, the user enters this command:

   ascend% **pad**

2. If the user is not authenticated and the terminal server has been configured for immediate PAD (that is, the parameter Immed Service=X.25/PAD), the MAX directs incoming calls to the X.25 host immediately.

X.25 protocol stack

The X.25 protocol stack contains these elements:

- Physical layer
- Frame layer (LAPB)
- Packet layer (X.25)
- Application layer (PAD)

The sections that follow briefly describe each layer.

Physical layer

From the perspective of the physical layer, X.25 is a protocol similar to the physical layer protocol RS-232C, and establishes a standard communication link between two hosts. The MAX supports nailed-up connections over Leased 56, ISDN BRI, E1 PRI B or H channels, and channelized fractional E1. Unchannelized E1 is not supported.

Frame layer (LAPB)

The frame layer implements LAPB (Link Access Protocol–Balanced), an HDLC-like protocol that facilitates the exchange of information packets. X.25 enables a sending device to transmit a specified number of frames before requiring an acknowledgment of the first frame. The protocol continuously increments a sequence number and puts the value into each outgoing frame.

The frame layer makes use of the types of frames listed in Table 12.

Table 12. Frame types

Frame type	Description
I-frames (Information frames)	The I-field (Information field) of an I-frame contains the address of the local DTE and the remote DCE, the type of frame in use, and the data itself. The data is passed to the packet layer.
S-frames (Supervisory frames)	S-frames control the flow of I-frames. Each S-frame contains a frame sequence number acknowledging the receipt of an I-frame.

Table 12. Frame types

Frame type	Description
U-frames (Unnumbered frames)	U-frames both establish and discontinue communications at the frame layer.

Packet layer (X.25)

The packet layer defines the packet format as well as the procedures for the exchange of packets containing control information and user data.

At the packet level, a number of logical channels are set up between a local DTE and a remote DCE. Each logical channel is identified by an LCN (Logical Channel Number). Every packet exchange occurs on one of these logical channels. When a connection takes place, X.25 uses a logical channel to establish a virtual connection, or PVC (Permanent Virtual Connection). The DCE maintains the correspondence between the logical channel and the PVC while the call takes place, and clears the PVC when the data exchange is over.

The packet layer makes use of the kinds of packets listed in Table 13.

Table 13. Packet types

Packet type	Description
Call-Connected/Call-Accepted	If the local DTE accepts an incoming call, it sends a Call-Connected packet; if the remote DTE has accepted a call, the remote DCE sends a Call-Accepted packet.
Call-Request/Incoming-Call	When a local DTE makes an outgoing call, it sends a Call-Request packet; if the remote DTE initiates the call, the remote DCE sends as Incoming-Call packet.
Clear-Confirmation	The local DTE or remote DCE sends a Clear-Confirmation packet to confirm that it received a Clear-Request or Clear-Indication packet.
Clear-Request/Clear-Indication	The local DTE sends a Clear-Request packet to initiate the clearing procedure for a call. The remote DCE can initiate the same procedure by sending a Clear-Indication packet. **Note:** The MAX includes support for FF FF cause/diag clearing codes in a Clear-Request packet.
Data	Sending and receiving devices can send and receive packets in either half-duplex or full-duplex mode.

Table 13. Packet types

Packet type	Description
Interrupt	An Interrupt packet can transmit between 1 and 32 bytes of data to the remote DTE without being subject to flow control. The exchange of Interrupt packets does not affect the exchange of data packets and flow-control packets.
Interrupt-Confirmation	The remote DTE sends an Interrupt-Confirmation packet to signal receipt of an Interrupt packet. Two parties in any exchange can send Interrupt packets in half-duplex or full-duplex mode.
Receiver Ready (RR)	An RR packet is a flow control packet that acknowledges the receipt of data and indicates that it can receive more data on the logical channel.
Receiver Not Ready (RNR)	An RNR packet is a flow-control packet that acknowledges the receipt of data and specifies that it cannot not receive any more data on the logical channel.
Reset-Confirmation	When the device that sent a Reset-Request or Reset-Indication packet receives a Reset-Confirmation packet, it can send data on the logical channel.
Reset-Request/Reset-Indication	A local DTE can send a Reset-Request packet to reset the packet sequence number for the logical channel to 0 (zero), and to remove any outstanding data and Interrupt packets from the virtual circuit. A Reset-Indication performs the same tasks for a remote DCE.
Restart-Confirmation	When the device that sent a Restart-Request or Restart-Indication packet receives a Restart-Confirmation packet, it can initiate calls to establish virtual circuits. The Restart-Confirmation packet is always transmitted on logical channel 0 (zero).
Restart-Request/Restart-Indication	A local DTE can send a Restart-Request packet to clear all virtual circuits. A Reset-Indication performs the same task for a remote DCE.

Application layer (PAD)

The application layer takes care of the encapsulation requirements as well as the multiplexing between destination and interface number. This layer also controls outgoing call routing, and enables the application to accept or reject incoming calls based on the called address, user data field, and facilities.

User interface changes

The new X.25 Profile enables you to define the parameters for each physical connection. Mapping between a logical X.25 connection to a physical connection occurs through the Connection Profile.

When you select X.25 from the Ethernet menu, the MAX displays a list of 16 X.25 Profile entries. You can assign a name to each entry. When you select an entry, the MAX displays both X.25 and LAPB (Link Access Protocol–Balanced) parameters:

```
00-601 Ascend X.25...
  Name=Ascend X.25
  Active=No
  Call Type=Nailed
  Nailed Grp=1
  Data Svc=64K
  PRI # Type=N/A
  Dial #=N/A
  Bill #=N/A
  Call-by-Call=N/A
  Transit #=N/A
  LAPB T1=3
  LAPB T2=0
  LAPB N2=20
  LAPB k=7
  X.25 Seq Number Mode=Normal
  X.25 Link Setup Mode=Active
  X.25 Node Type=DTE
  X.25 Window Size=2  v
```

In addition, when you set Encaps=X.25/PAD in a Connection Profile under the Ethernet/ Connections menu, the Encaps Options submenu contains these parameters:

```
00-601 Ascend X.25...
  Encaps options...
    X.25 Prof=
    LCN=3
    Recv Password=
    X.3 Param Prof=CRT
    Immed X.121 Addr=
    Max Unsucc. calls=10
    VC Timer=Disable
```

Finally, the Immed Service and Immed Host parameters in the Ethernet/ Mod Config/ TServ Options submenu now contain X.25 options.

Setting up an X.25 configuration

Table 14 provides a list of all X.25 parameters, along with their default values. Each parameter is described in detail in “X.25 parameter descriptions” on page 65.

Table 14. X.25 Profile parameters

Location	Parameter with default value
Ethernet/Mod Config/TServ Options	Immed Host=[ ] Immed Service=None
Ethernet/X.25/Any X.25 Profile	Name=[ ] Active=No Call Type=Nailed Nailed Grp=1 Data Svc=64K PRI # Type=N/A Dial #=N/A Bill #=N/A Call-by-Call=N/A Transit #=N/A LAPB T1=3 LAPB T2=0 LAPB N2=20 LAPB k=7 X.25 Seq Number Mode=Normal X.25 Link Setup Mode=Active X.25 Node Type=DTE X.25 Window Size=2 X.25 Default Packet Size=128 X.25 Min Packet Size=64 X.25 Max Packet Size=4096 X.25 Lowest PVC=0 X.25 Highest PVC=0 X.25 Lowest SVC=1 X.25 Highest SVC=255 X.25 Clear/Diag=Yes X.25 Reset/Diag=Yes X.25 Restart/Diag=Yes X.25 Options=NPWS X.25 Network Type=CCITT X.25 T20=18 X.25 R20=1 X.25 T21=20 X.25 T22=18 X.25 R22=1 X.25 T23=18 X.25 R23=1 X.121 Source Address=[ ] VC Timer Val=300

Table 14. X.25 Profile parameters

Location	Parameter with default value
Ethernet/Connections/Any Connection Profile	Encaps=X25/PAD
Ethernet/Connections/Any Connection Profile/Encaps Options (when Encaps=X.25/PAD)	X.25 Prof=[ ] LCN=0 Recv Password=[ ] X.3 Param Prof=CRT Immed X.121 Addr=[ ] Max Unsucc. calls=10 VC Timer=Disable

To set up an X.25 configuration, follow these steps:

1 Set the parameters in the X.25 Profile, or accept the default values.

The parameter values provided by default in the X.25 Profile should match the most common values provisioned into public switches. You must obtain a copy of the network's subscription form containing the values as provisioned in the switch.The MAX parameter settings must match these values.

For a discussion of the subscription form values and matching MAX parameters, see “X.25 subscription form values” on page 65.

2 If you want terminal server users to immediately begin an X.25/PAD session, set these parameters in the Ethernet/Mod Config/TServ Options menu:

- Set Immed Service=X.25/PAD.
- Set the Immed Host parameter to the X.121 address of the remote device.

3 In the Connection Profile, set Encaps=X.25/PAD.

4 In the Encaps Options submenu of the Connection Profile, set the X.25 Prof parameter to the name of the X.25 Profile you configured in Step 1.

5 Set the LCN parameter to the channel number of the Permanent Virtual Connection (PVC).

6 Set the Recv Password parameter to the password the remote user must enter.

7 Set the Max Unsucc. Calls parameter to the maximum number of unsuccessful X.25 calls the MAX should try to place before dropping the modem connection.

8 Set the X.3 Param Prof parameter to specify the X.3 parameter profile in use.

For information about the parameters available in each X.3 parameter profile, see “X.3 parameters” on page 91 and “X. 3 parameter profiles” on page 94.

9 Set the Immed X.121 Address parameter to specify the value you indicated for the Immed Host parameter in Step 2.

10 Set the VC Timer parameter to specify whether the MAX should activate or deactivate the Virtual Call Establishment timer.

11 Save your changes.

X.25 subscription form values

Table 15 provides a list of subscription form values and matching MAX parameters.

Table 15. X.25 subscription form values and matching MAX parameters

Subscription form value	MAX parameter
Maximum time the transmitter should wait for an acknowledgment before initiating a recovery procedure (T1)	LAPB T1
Maximum number of times to resend a frame after the T1 timer expires (N2)	LAPB N2
Maximum number of sequentially numbered frames that a given DTE/DCE link may have unacknowledged at any given time (k)	LAPB k
Is the X.25 node a DTE (Data Terminal Equipment) or DCE (Data Circuit-Terminating Equipment)?	X.25 Node Type
Is the link a Switched Virtual Connection (SVC) or a Permanent Virtual Connection (PVC)?	LCN X.25 Lowest PVC X.25 Lowest SVC
Maximum packet size	X.25 Max Packet Size
Window size—the maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required (W)	X.25 Window Size
Number of PVCs	X.25 Highest PVC
Highest PVC channel number	X.25 Highest PVC
Flow control	X.25 Default Packet Size X.25 Max Packet Size X.25 Min Packet Size X.25 Window Size

X.25 parameter descriptions

The sections that follow describe each X.25 parameter.

Active

Description: This parameter activates or deactivates an X.25 Profile.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the profile.
- No deactivates the profile.
  When you choose this setting, the MAX deletes the profile. No is the default.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

Bill #

Description: This parameter specifies a billing number for charges incurred on the X.25 connection. If you do not enter a billing number, the telephone company bills charges to the telephone number assigned to the line.

Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Bill #, your carrier can separate and tally each department's usage.

Usage: Press Enter to open a text field. Then, type a telephone number. You can specify up to ten characters, and you must limit those characters to the following:

```
1234567890()[]!z-*# |
```

The MAX uses the Bill # parameter differently depending on the type of line you use:

- For a E1 line, the MAX appends the value specified in the Bill # parameter to the end of each phone number it dials for the call.
- Bill # for outgoing calls on an ISDN BRI line applies only to installations in Australia.
- For a E1 PRI line, the MAX uses the Bill # parameter rather than the phone number ID to identify itself to the answering party.

  The Clid Auth parameter enables you to require a device to authenticate incoming calls by checking the calling party's phone number. The device performs CLID (Calling Line ID) authentication before answering an incoming call. The calling party's phone number must match the Calling # parameter (or the equivalent value in a RADIUS entry). If the device cannot authenticate the call when CLID authentication is required, the call is rejected.

  If the calling party uses the Bill # parameter instead of its phone number as its ID, the CLID used by the answering side is not the true phone number of the caller. This situation presents a security breach if you use Clid Auth.

  Further, be aware that if you specify a value for the Bill # parameter, there is no guarantee that the phone company will send it to the answering device.

Press Enter to close the text field.

Dependencies: The Bill # parameter does not apply when Call Type=Nailed.

Example: These specifications are valid for Bill #:

```
5105551972
510-555-1972
```

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: Calling #, Call Type, Clid Auth

Call-by-Call

Description: This parameter specifies the E1 PRI service that the MAX uses when placing an X.25 call.

Usage: Press Enter to open a text field. Then, type a number corresponding to the type of service the MAX uses. The default is 6.

Table 16 lists the services available if the service provider is AT&T.

Table 16. AT&T Call-by-Call settings

Number	Service
0	Disable call-by-call service.
1	SDN (including GSDN)
2	Megacom 800
3	Megacom
6	ACCUNET Switched Digital Services
7	Long Distance Service (including AT&T World Connect)
8	International 800 (I800)
16	AT&T MultiQuest

Table 17 lists the VPN and GVPN services available if the service provider is Sprint.

Table 17. Sprint Call-by-Call settings

Number	Service
0	Reserved
1	Private
2	Inwatts
3	Outwatts
4	FX
5	Tie Trunk

Table 18 lists the services available if the service provider is MCI.

Table 18. MCI Call-by-Call settings

Number	Service
1	VNET/Vision
2	800
3	PRISM1, PRISM II, WATS
4	900

Table 18. MCI Call-by-Call settings

Number	Service
5	DAL

Dependencies: Call-by-Call does not apply when Call Type=Nailed.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: Call Type

Call Type

Description: This parameter specifies whether the physical X.25 connection is switched or nailed up.

Usage: Press Enter to toggle between the choices.

- Nailed specifies that the link consists entirely of nailed-up channels.
  You must use the Nailed Grp parameter to specify which channels are associated with the connection.
  Nailed is the default.
- Switched specifies that the link consists entirely of switched channels.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

Data Svc

Description: This parameter specifies the type of data service the link uses.

A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice.

Usage: Press Enter to cycle through the choices. You can specify one of the settings listed in Table 19.

Table 19. Data Svc settings

Setting	Description
56K	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (E1 access lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR. For most E1 PRI lines, select 56K.

Table 19. Data Svc settings

Setting	Description
56KR	The call contains restricted data, guaranteeing that the data the MAX transmits meets the density restrictions of D4-framed TI lines. D4 specifies the D4 format, also known as the Superframe format, for framing data at the physical layer. This format consists of 12 consecutive frames, separated by framing bits. The call connects to the Switched-56 data service. The only services available to lines using inband signaling (E1 access lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.
64K	The call contains any type of data and connects to the Switched-64 data service. This setting is the default.
Voice	This value applies only to calls made over an ISDN BRI or E1 PRI line.The Voice setting enables the MAX to instruct the network to place an end-to-end digital voice call for transporting data when a switched data service is not available. If you choose this setting, the data might become unusable unless you meet these technical requirements: • Use only digital end-to-end connectivity; no analog signals should be present anywhere in the link. • Make sure that the phone company is not using any intervening loss plans to economize on voice calls. • Do not use echo cancellation; analog lines can echo, and the technology to take out the echoes can scramble data in the link. • Do not make any modifications that can change the data in the link.
Modem	This setting places an outgoing call on any available digital modem. If no digital modems are available, the MAX does not place the call. The data rate depends upon the quality of the connections between modems and the types of modems used. The Modem setting requires that your MAX has digital modems installed. Modem applies only when Encaps=MPP, PPP, or X.25/PAD. Currently, multichannel modem calls are not supported even if Encaps=MPP.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

Dial

Description: This parameter specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the X.25 link.

Usage: Press Enter to open a text field. Then, type a telephone number. You can enter up to 37 characters, and you must limit those characters to the following:

```
1234567890()[]!z-*#|
```

The MAX sends only the numeric characters to place a call. The default value is null.

If Sub-Adr=Termsel, include the ISDN subaddress in your specification, separating it from the phone number with a comma. If Sub-Adr=Routing, the subaddress is optional, but you should include it if the MAX uses the subaddress for routing incoming calls. The characters before the comma comprise the phone number; the one or two numeric characters after the comma comprise the subaddress. Consider this example:

```
555-1212,23
```

The MAX dials the phone number 555-1212, and conveys the subaddress 23 to the answering party.

Press Enter to close the text field.

Dependencies: Dial # does not apply when Call Type=Nailed.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: Call Type, Sub-Adr

Immed Host

Description: This parameter specifies one of these elements:

- The IP address or hostname of a device with which remote terminal server users establish a Telnet, raw TCP, or Rlogin session immediately after the banner appears.
- The X.121 address (or mnemonic) of a remote X.25 host that the MAX automatically calls when establishing an immediate X.25/PAD session.

Usage: Press Enter to open a text field. Then, type the IP address, X.121 address, or hostname of the device.

The IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0/0. If a domain name server is supported on the local network, you can specify the device's hostname instead.

An X.121 address can contain between 1 and 15 decimal digits. When an outgoing call is placed by a terminal connected to one of the PAD's async ports, it must contain the address of the remote computer or other remote device with which it is attempting to communicate, much as an ordinary telephone call is placed by dialing the correct number.

Press Enter again to close the text field.

Example: Suppose that the device to which users can immediately Telnet has the IP address 200.5.109.3 and the hostname "MyHost". You can enter either of these specifications:

```
Immed Host=200.5.109.3
Immed Host=MyHost
```

Parameter Location: Ethernet Profile: Ethernet/Mod Config/TServ Options

See Also: Immed Port, Immed Service

Immed Service

Description: This parameter specifies whether remote terminal server users establish a Telnet, raw TCP, Rlogin, or X.25/PAD session immediately after the banner appears.

Usage: Press Enter to cycle through the choices.

- Telnet specifies that a Telnet session is established.

  Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

- Raw-TCP specifies that a raw TCP session is established.

  Raw TCP is a TCP/IP connection with no Telnet protocol. When you choose this setting, the MAX establishes a TCP connection between the MAX and the host specified by the Immed Host parameter. The Immed Port parameter specifies the application port that the TCP session plugs into.

- Rlogin specifies that an immediate Rlogin session is established.

  Rlogin is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Rlogin host. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

- X.25/PAD specifies that an immediate X.25 connection is established.

  When you choose this setting, the call is directed to the PAD, and the MAX makes an X.25 call request with the X.121 address specified by the Immed Host parameter.

  X.25 is a connection-oriented protocol that uses virtual circuits and provides services such as multiplexing, in-sequence delivery, transfer of addressing information, segmenting and reassembly, flow control, transfer of expedited data, error control, reset, and restart. Allocation of logical channels can be either static (PVC or Permanent Virtual Connection) or dynamic (SVC or Switched Virtual Connection).

  A PAD (Packet Assembler/Disassembler) is an asynchronous terminal concentrator that enables several terminals (or other asynchronous devices) to share a single network line. The PAD assembles data from terminals into packets for transmission to an X.25 network, and disassembles incoming packets from the network into a separate data stream for each terminal. In addition to this multiplexing function, the PAD also provides a nearly error-free connection. PAD-generated packets are transported using the X.25 protocol.

- None specifies that no immediate connection occurs for remote terminal server users logging into the MAX.

  None is the default.

Dependencies: Keep this additional information in mind:

- You must set the Immed Host parameter to the IP address, X.121 address, or hostname of the host to which you want to connect.
- If you set Immed Service=Rlogin or X.25/PAD, the Immed Port parameter does not apply.

Parameter Location: Ethernet Profile: Ethernet/Mod Config/TServ Options

See Also: Immed Host, Immed Port

Immed X.121 Addr

Description: This parameter specifies the X.121 address the MAX should automatically call as soon as a PAD session starts for this user.

Usage: Press Enter to open a text field. Then, specify an X.121 address.

An X.121 address can contain between 1 and 15 decimal digits. When an outgoing call is placed by a terminal connected to one of the PAD's async ports, it must contain the address of the remote computer or other remote device with which it is attempting to communicate, much as an ordinary telephone call is placed by dialing the correct number.

When a device makes an outgoing call, it sends a Call-Request packet. Each Call-Request packet coming in from the network must contain an address that indicates the call's destination. In practice, the address is most commonly composed of up to 12 digits assigned to the PAD as a whole by the network; the address can also contain digits designated by the PAD administrator as a subaddress to distinguish the various ports within the PAD from one another. By default, the PAD listens on any address matching the subaddress of the asynchronous port.

For example, the network address of the PAD might be 311021755555; one might then choose to append the subaddress 01 to access asynchronous port #1. All incoming calls with the address 31102175555501 can reach asynchronous port #1.This address pattern can be modified using the PAD listen command.

The default is null. This setting indicates that the MAX does not automatically place a call. Press Enter again to close the text field.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

LAPB k

Description: This parameter specifies the maximum number of sequentially numbered frames that a given DTE/DCE link may have unacknowledged at any given time. This specification is also called the Level 2 Window Size or the Frame Window Size.

Usage: Press Enter to open a text field. Then, type a number between 1 and 7. The default is 7. A higher value enables faster throughput. The value you specify must be the same for both ends of the link. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: LAPB N2, LAPB T1, LAPB T2

LAPB N2

Description: This parameter indicates the retry limit—the maximum number of times the MAX can resend a frame when the LAPB T1 timer expires.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 20. A higher value increases the probability of a correct transfer of data. A lower value allows for quicker detection of a permanent error condition. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: LAPB k, LAPB T1, LAPB T2

LAPB T1

Description: This parameter specifies the maximum amount of time in seconds the transmitter should wait for an acknowledgment before initiating a recovery procedure.

On a transmission line between a user and the network, a particular frame or acknowledgment may be incorrectly transmitted or simply discarded. To keep the transmitter from waiting indefinitely for an acknowledgment, you can specify the maximum amount of time the transmitter should wait.

Usage: Press Enter to open a text field. Then, type a number between 1 and 255. The default is 3. When you choose a value for this parameter, you must take into account any frame transmission and processing delays you may encounter. In most cases, you should use the default value suggested by the network. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: LAPB k, LAPB N2, LAPB T2

LAPB T2

Description: This parameter determines the maximum number of milliseconds LAPB (Link Access Protocol–Balanced) waits for outgoing I-frames (Information frames) before sending a Restart-Request packet to the network. An I-frame is a frame that transports data over an access link.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: LAPB k, LAPB N2, LAPB T1

LCN

Description: This parameter specifies the LCN (logical channel number) to use for a PVC (Permanent Virtual Connection).

At the packet level, a number of logical channels are set up between a DTE and a DCE. Every packet exchange occurs on one of these logical channels. When a connection takes place, X.25 uses a logical channel to establish a PVC. The DCE maintains the correspondence between the logical channel and the PVC while the call takes place, and clears the PVC when the data exchange is over.

Usage: Press Enter to open a text field. Then, type a channel number. You can enter a number between 0 and 4095. The default is 0 (zero). If you accept the default, the X.25 link does not use a logical channel or PVC; the link is an SVC (Switched Virtual Connection). Press Enter again to close the text field.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

Max Unsucc. Calls

Description: This parameter specifies the maximum number of unsuccessful X.25 calls the MAX tries to place before dropping the modem connection.

Usage: Press Enter to open a text field. Then, specify a number between 0 and 9999. The default is 10. A value of 0 (zero) indicates that the MAX never drops the modem connection because of unsuccessful X.25 calls. Press Enter again to close the text field.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

Nailed Grp

Description: This parameter specifies the group number of the physical nailed-up circuit the MAX uses to attach to the X.25 switch.

Usage: Press Enter to open a text field. Then, type a group number. You can assign only one X.25 Profile to a group. The default is 1. Press Enter again to close the text field.

Dependencies: The Nailed Grp parameter does not apply when Call Type=Switched.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: Call Type

Name

Description: This parameter specifies the name of an X.25 Profile. The Connection Profile uses this name to refer to a physical X.25 connection.

Usage: Press Enter to open a text. Then, type the name of the profile. You can specify up to 15 characters. The default is null. The name you specify must be unique within the list of X.25 Profiles. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

PRI # Type

Description: This parameter enables an AT&T switch to use your Dial # when you make an E1 PRI call.

A switch is the device that connects the calling party to the answering party. The connection is a switched circuit consisting of one or more channels.

Usage: Press Enter to cycle through the choices.

- National specifies phone numbers within the U.S.
  National is the default.
- Intl specifies phone numbers outside the U.S.
- Local specifies phone numbers within your Centrex group.

Dependencies: Keep this additional information in mind:

- PRI # Type appears only on E1 PRI units.
- PRI # Type does not apply when the line does not support E1 PRI signalling, or when Call Type=Nailed.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: Call Type

Recv Password

Description: This parameter specifies the password for the Connection Profile user of an X.25 link.

Usage: Press Enter to open a text field. Then, type a password. You can enter up to 20 characters. The default is null. Press Enter again to close the text field.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

VC Timer

Description: This parameter enables you to activate or deactivate the Virtual Call Establishment timer on a per-user basis.

Usage: Press Enter to toggle between the choices.

- Enable activates the timer.

  When you specify this value, the MAX maintains a connection to a character-oriented device that has not established a virtual call for the length of time specified by the VC Timer Val parameter, or until it reaches the number of unsuccessful calls specified by the Max Unsucc. Calls parameter.
- Disable disables the timer.

  Disable is the default.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

See Also: Max Unsucc.Calls, VC Timer Val

VC Timer Val

Description: This parameter sets the Virtual Call Establishment timer—the number of seconds the X.25 link maintains a connection to a character-oriented device that has not established a virtual call.

Usage: Press Enter to open a text field. Then, specify a value between 0 and 9999. The default value is 300.

The timer value is link wide. You can set the VC Timer parameter to enable or disable the timer on a per-user basis. A value of 0 (zero) for the VC Timer Val parameter disables the timer for all users, regardless of the value of the VC Timer parameter.

Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: VC Timer

X.121 Source Address

Description: This parameter specifies the source address to use in logical calls.

Usage: Press Enter to open a text field. Then, type an address. An X.121 address can contain between 1 and 15 decimal digits. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

X.25 Clear/ Diag

Description: This parameter specifies whether Clear-Request packets include the diagnostic field.

The DTE sends a Clear-Request packet to initiate clearing procedures for a call. The DCE accomplishes the same task by using a Clear-Indication packet. The DTE can send a Clear-Request packet to refuse an incoming call, or to clear a call once the data exchange is complete. Once the DTE or DCE receives a Clear-Confirmation packet, the call is cleared and the logical channel is available for other calls.

A Clear-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the reset, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the reset, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that Clear-Request packets include the diagnostic field.
- No specifies that Clear-Request packets do not include the diagnostic field. No is the default.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Reset/Diag, X.25 Restart/Diag

X.25 Default Packet Size

Description: This parameter establishes the default number of bytes in the data field of a data packet.

Usage: Press Enter to cycle through the choices:

- 64
- 128
- 256
- 512
- 1024
- 2048
- 4096

The default is 128.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Max Packet Size, X.25 Min Packet Size, X.25 Window Size

X.25 Highest PVC

Description: This parameter specifies the highest PVC (Permanent Virtual Connection) number available.

Usage: Press Enter to open a text field. Then, type a number between 0 and 4095. The default is 0 (zero). The number you specify must be greater than or equal to the value specified by the X.25 Lowest PVC parameter. Press Enter again to close the text field.

Dependencies: If X.25 Lowest PVC=0, the value you specify for X.25 Highest PVC is not meaningful.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Lowest PVC

X.25 Highest SVC

Description: This parameter specifies the highest SVC (Switched Virtual Connection) number available.

Usage: Press Enter to open a text field. Then, type a number between 0 and 4095. The default is 8. The number you specify must be greater than or equal to the value specified by the X.25 Lowest SVC parameter. Press Enter again to close the text field.

Dependencies: If X.25 Lowest SVC=0, the value you specify for X.25 Highest SVC is not meaningful.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Lowest SVC

X.25 Link Setup Mode

Description: This parameter specifies whether the X.25 link comes up in active or passive disconnect mode.

Usage: Press Enter to toggle between the choices.

- Active specifies active disconnect mode.

  When you choose this setting, the frame layer comes up in DM (Disconnect Mode), and the packet layer sends Restart-Request messages upon initialization. A Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can issue a call to establish a virtual circuit.

  Active is the default.

- Passive specifies passive disconnect mode.

  When you choose this setting, the frame layer comes up sending SABM(E) and the packet layer issues a Restart-Request message to the network only upon receipt of a Request-Restart token. SABM(E) stands for Set Asynchronous Balanced Mode (Extended).

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

X.25 Lowest PVC

Description: This parameter specifies the lowest PVC (Permanent Virtual Connection) number available.

Usage: Press Enter to open a text field. Then, type a number between 0 and 4095. The default is 0 (zero). This defaults means that no PVC is available. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Highest PVC

X.25 Lowest SVC

Description: This parameter specifies the lowest SVC (Switched Virtual Connection) number available.

Usage: Press Enter to open a text field. Then, type a number between 0 and 4095. The default is 1. A setting of 0 (zero) indicates that no SVC is available. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Highest SVC

X.25 Max Packet Size

Description: This parameter establishes the maximum number of bytes in the data field of a data packet when negotiating the packet size with a remote X.25 switch.

Usage: Press Enter to cycle through the choices:

- 64
- 128
- 256
- 512
- 1024
- 2048
- 4096

The default is 128. Note that a large packet size improves throughput by reducing the overhead associated with header transmission. However, a large packet size also increases the probability of transmission errors, causes increased transmission delays on the network, and is associated with processing delays at the host.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Default Packet Size, X.25 Min Packet Size, X.25 Window Size

X.25 Min Packet Size

Description: This parameter establishes the minimum number of bytes in the data field of a data packet when negotiating the packet size with a remote X.25 switch.

Usage: Press Enter to cycle through the choices:

- 64

- 128
- 256
- 512
- 1024
- 2048
- 4096

The default is 128.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Default Packet Size, X.25 Max Packet Size, X.25 Window Size

X.25 Network Type

Description: This parameter specifies the type of network used by the link.

Usage: CCITT specifies that the link uses a CCITT network. At present, CCITT is the only value available for this parameter.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

X.25 Node Type

Description: This parameter specifies whether the local X.25 node is DTE (Data Terminal Equipment) or DCE (Data Circuit-Terminating Equipment).

- A DTE is a device that an operator uses, such as a computer or a terminal.
- A DCE is a device that connects the DTE to a communications channel.
  A DCE converts the format of the data coming from the DTE into a signal suitable to the communications channel. An example of a DCE is a modem, which converts digital data to analog signals suitable for sending over a telephone line.

Usage: Press Enter to toggle between the choices.

- DTE specifies that the local X.25 node is Data Terminal Equipment.
  DTE is the default.
- DCE specifies that the local X.25 node is Data Circuit-Terminating Equipment.

Dependencies: For proper X.25 operation, the two ends of a link must be of opposite types.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

X.25 Options

Description: This parameter specifies X.25 packet-level options.

Usage: Press Enter to cycle through the choices.

- None specifies that no packet-level options are enabled.
  None is the default.
- NPWS specifies that the X.25 protocol negotiates packet and window size.
  The window size establishes the maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Default Packet Size, X.25 Max Packet Size, X.25 Min Packet Size, X.25 Window Size

X.25 Prof

Description: This parameter specifies the name of an X.25 Profile that carries X.25 logical connections. If the matching X.25 Profile can not be found, the MAX does not start a session for this Connection Profile. To guard against misconfiguration, the MAX does not allow you to save an active Connection Profile specifying X.25 encapsulation unless the named X.25 Profile is defined and active.

Usage: Press Enter to open a text field. Then, using up to 15 characters, type the name of the X.25 Profile. Press Enter again to close the text field.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

X.25 R20

Description: This parameter determines the limit for Restart Retries—that is, the number of times the MAX transmits a Restart-Request packet before waiting indefinitely for a response.

At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). This default indicates that the MAX always waits indefinitely for a response. Press Enter again to close the text field.

Dependencies: The value you specify is not meaningful if X.25 T20=0.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 R22, X.25 R23, X.25 T20

X.25 R22

Description: This parameter determines the limit for Reset Retries—that is, the number of times the MAX retransmits a Reset-Request packet before clearing a call.

At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). Press Enter again to close the text field.

Dependencies: The value you specify is not meaningful if X.25 T22=0.

Parameter Location: Ethernet Profile: Etherne/X.25/Any X.25 Profile

See Also: X.25 R20, X.25 R23, X.25 T22

X.25 R23

Description: This parameter determines the limit for Clear-Request Retries—that is, the number of times the MAX sends a Clear-Request before waiting indefinitely for a response.

The DTE can send a Clear-Request packet to refuse an incoming call, or to clear a call once the data exchange is complete. The DCE accomplishes the same task by using a Clear-Indication packet. Once the DTE or DCE receives a Clear-Confirmation packet, the call is cleared and the logical channel is available for other calls.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). Press Enter again to close the text field.

Dependencies: The value you specify is not meaningful if X.25 T23=0.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 R20, X.25 R22, X.25 T23

X.25 Reset/ Diag

Description: This parameter specifies whether Reset-Request packets include the diagnostic field.

At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

A Reset-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the reset, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the reset, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that Reset-Request packets include the diagnostic field.
- No specifies that Reset-Request packets do not include the diagnostic field.
  No is the default.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Clear/Diag, X.25 Restart/Diag

X.25 Restart/ Diag

Description: This parameter specifies whether Restart-Request packets include the diagnostic field.

At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

A Restart-Request packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote DTE did not request the restart, the diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the restart, the diagnostic field contains information specified in the Cause field by the remote DTE.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that Restart-Request packets include the diagnostic field.
- No specifies that Restart-Request packets do not include the diagnostic field.
  No is the default.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Clear/Diag, X.25 Reset/Diag

X.25 Seq Number Mode

Description: This parameter specifies whether the MAX uses modulo 8 or modulo 128 sequence number mode.

At the frame level, X.25 allows a sender to transmit a certain number of frames before requiring an acknowledgment of the first frame. The protocol increments a sequence number in the frame header, and places the value into the next outgoing frame. The sequence number identifies each frame that has not yet been acknowledged.

Usage: Press Enter to toggle between the choices.

- Normal specifies modulo 8 mode.
  In modulo 8 mode, the sequence number can contain three bits, allowing eight frames to be identified with a single sequence number.
  Normal is the default.
- Extended specifies module 128 mode.
  When substantial delays in transmission may occur, you can specify Extended so that the sequence number is enlarged to seven bits. When you choose this setting, 128 frames can be identified with a unique sequence number.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

X.25 T20

Description: This parameter determines the duration of the Restart timer—that is, the number of ten-second ticks the MAX waits before retransmitting a Restart-Request packet.

At the packet layer, a Restart-Request packet clears all virtual circuits. When the sending device receives a Restart-Confirmation packet, it can again issue a call to establish a virtual circuit.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). This default setting disables the timer. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 R20, X.25 T21, X.25 T22, X.25 T23

X.25 T21

Description: This parameter determines the duration of the Call-Request timer—that is, the number of ten-second ticks the MAX waits before clearing an outgoing call that has not been accepted.

When a device makes an outgoing call, it sends a Call-Request packet. If the remote DTE accepts the call, it sends back a Call-Connected Packet; if the DTE refuses the call, it sends back a Clear-Request packet.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). This default setting disables the timer. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25R21, X.25 T20, X.25 T22, X.25 T23

X.25 T22

Description: This parameter determines the duration of the Reset-Request timer—that is, the number of ten-second ticks the MAX waits before retransmitting a Reset-Request packet.

At the packet layer, a Reset-Request packet resets the packet sequence number for the logical channel to 0 (zero), and removes any outstanding data and Interrupt packets from the virtual circuit. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). This default setting disables the timer. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 R22, X.25 T20, X.25 T21, X.25 T23

X.25 T23

Description: This parameter determines the duration of the Clear-Request timer—that is, the number of ten-second the MAX waits before retransmitting a Clear-Request packet.

When a device makes an outgoing call, it sends a Call-Request packet. If the remote DTE accepts the call, it sends back a Call-Connected Packet; if the DTE refuses the call, it sends back a Clear-Request packet.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. The default is 0 (zero). This default setting disables the timer. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 R23, X.25 T20, X.25 T21, X.25 T22

X.25 Window Size

Description: This parameter establishes the maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required.

Usage: Press Enter to open a text. Then, type a number between 1 and 7. The default is 7. Press Enter again to close the text field.

Dependencies: The value you specify applies to all of the user's virtual circuits. However, the user can use the FACILITIES command at the PAD prompt to alter the window size on a per-call basis.

Parameter Location: Ethernet Profile: Ethernet/X.25/Any X.25 Profile

See Also: X.25 Default Packet Size, X.25 Max Packet Size, X.25 Min Packet Size

X.3 Param Prof

Description: This parameter specifies the default factory X.3 parameters profile for this user.

Usage: Press Enter to cycle through the choices.

- CRT
  CRT is the default.
- INFONET
- DEFAULT
- SCEN
- CC_SSP
- CC_TSP
- HARDCOPY
- HDX
- SHARK
- NULL

For a description of the parameters in each profile, see "X.3 parameters" on page 91 and "X. 3 parameter profiles" on page 94.

Dependencies: If Encaps is not set to X.25/PAD, this parameter does not appear in the menu.

Parameter Location: Connection Profile: Ethernet/Connections/Any Connection Profile/Encaps Options

Getting X.25/PAD status information

To obtain information about X.25/PAD service, use these commands at the terminal server prompt:

- show pad
  This command displays information about the PAD.
- show x25
  This command displays information about the X.25 frame and packet layer.

Using the show pad command

When you enter show pad, these statistics display:

```
Port      State              LCN       BPS       User        Called
Addr.
1           connected      8             9600      x25usr     4193428
2           connected      7             9600      x25usr
```

Table 20 lists the information provided in each column.

Table 20. Show pad information

Column	Description
Port	Specifies the port for the X.25 connection.
State	Indicates the state of the connection: • idle—The PAD is open, but no call has been issued. • calling—A call has been issued and is awaiting acceptance. • connected—The call is connected and in session. • clearing—A clear command has been issued, and the transmitter is awaiting a clear confirmation.
LCN	Specifies the LCN (Logical Channel Number) used for this PVC (Permanent Virtual Connection).
BPS	Indicates the data rate of the connection in bits per second.
User	Specifies the MAX user.
Called Addr	Identifies the X.121 address of the remote node.

Using the show x25 command

When you enter show x25, these statistics display:

```
Frame    State         BytesIn        BytesOut
1            LinkUp    5                 4
Packet   State         BytesIn         BytesOut
1           Ready       1                  1
```

Table 21 lists the information provided in each column.

Table 21. Show x25 information

Column	Description
Frame	Specifies the frame layer.
Packet	Specifies the packet layer.

Table 21. Show x25 information

Column	Description
State	Identifies the state of the connection at the frame or packet layer. For the frame layer, these states can occur: • SABMSent—An SABM (Set Asynchronous Balanced Mode) message has been sent to establish the operating mode as LAPB (Link Access Balanced Protocol), and the transmitter is awaiting a UA (Unnumbered Acknowledge response). • DISCSent—A DISC message has been sent to disconnect the frame level, and the transmitter is awaiting a UA (Unnumbered Acknowledge response). • FRMRSent—An FRMR has been sent, indicating that a mal-formed frame was received, and the sender is awaiting an SABM message. • LinkUp—The link is up and sending I-frames and S-frames. • Disconnected—A disconnect has been requested, and the sender is awaiting an SABM message. For the packet layer, these states can occur: • Ready—The packet level is ready to send and receive data. • DTERestart—The DTE has issued a Restart-Request. • DCERestart—The DCE has issued a Restart-Request. • BothRestart—Restart-Requests have been sent to both the DTE and the DCE. • InitState—Indicates the initial state of a call.
BytesIn	Specifies the number of bytes received from the remote node.
BytesOut	Specifies the number of bytes transmitted to the remote node.

X.25/PAD commands

Table 22 lists the commands you can enter at the PAD prompt. The underlined letters are the minimum you can enter for the command.

Table 22. X.25/PAD commands

Syntax	Description
CALL [?] | [[<address>][*P|*D|*F <data>]]	Generate a call by sending a Call-Request packet. • The <address> argument specifies the X.121 address to which the call is made. The address can contain up to 15 characters. If you do not specify a value for <address> , the MAX makes the call request for the last address specified. • The <data> following the *P and *D keywords is inserted into the last 12 bytes of the user data field. If you specify *P, the screen does not echo the data as you enter it, even if you set X.3 parameter number 2 to Echo; this specification is useful for entering passwords. If you specify *D, the screen echoes the data as you enter it. • If you specify *F, all the <data> is inserted into the user data portion of the call packet (with a maximum length of 124 bytes), and the packet is flagged as a “fast select” call. • If you enter the CALL command with only a question mark (?), the MAX displays the address the PAD would use if you entered the CALL command with no address.
CLR	Clear a virtual circuit by sending a Clear-Request packet (from a DTE) or a Clear-Indication packet (from a DCE).
FACILITIES [* | <facilities>]	Specify facilities to use in subsequent CALL commands. • When you specify an asterisk (*), the command clears the current facilities and resets them to their default values. The default facilities are window size 2 and packet size 128 (420202430707). • The <facilities> argument can consist of up to 63 hexadecimal digits. The value you specify is converted from hexadecimal format and becomes the byte sequence inserted in the Facilities field of outgoing Call-Request packets. • If you enter the FACILITIES command with no arguments, the MAX displays the current facilities.
FULL	Select full-duplex mode.

Table 22. X.25/PAD commands

Syntax	Description
HALF [*] | [[-] <ch1>, <ch2>,...]	Select half-duplex mode and specify the characters echoed. In half-duplex mode, most characters are not echoed. • When you specify an asterisk (*), no characters are echoed. • When you specify only a list of characters (<ch1>, <ch2>, and so on), only these characters are echoed. You must specify each character in decimal format. • When you insert a hyphen (-) before the list of characters, only the characters you specify are not echoed. • If you enter the HALF command with no arguments, the command sets half-duplex mode without altering the characters selected for echo using any previously entered HALF command. In half-duplex mode with echo enabled, the PAD does most of the work of echoing and then discards the data instead of sending it to the asynchronous device. The PAD can therefore provide line folding, tab expansion, linefeed insertion, carriage return and linefeed padding, and character and line deletion. For details on these features, see “X.3 parameters” on page 91. If you disable echo, the amount of processing the PAD must do on every character decreases substantially, and the PAD cannot perform line folding, tab expansion, or other actions described in the previous paragraph. This mode is most efficient for file transfers.
HELP	Display a list of X.25/PAD commands and syntax.
INTERRUPT	Generate an Interrupt packet. An Interrupt packet can transmit between 1 and 32 bytes of data to the remote DTE without being subject to flow control. The exchange of Interrupt packets does not affect the exchange of data packets and flow-control packets.

Table 22. X.25/PAD commands

Syntax	Description
LISTEN [ADDR=<address> | DATA=<data>]	Specify the match pattern for accepting an incoming call. • The MAX matches the <address> argument against the subaddress specified by the incoming call; if the subaddresses match, the incoming call is accepted on this asynchronous port. • The MAX matches the <data> against the last 12 bytes of the user data field of incoming calls; if the data matches, the incoming call is accepted on this asynchronous port.
PAR? [<param1>[,<param2>,...]]	Display the current values of the specified X.3 parameters. If you do not specify one or more parameters (<param1>, <param2>, and so on), the PAR? command displays all X.3 parameter values. For a list of X.3 parameters, see “X.3 parameters” on page 91.
PROF [<profile> | ?]	Configure the session using the values associated with an X.3 parameter profile. • The <profile> argument specifies the name of the X.3 parameter profile to activate. • The question mark (?) keyword displays the currently active profile, followed by a list of available profiles. • If you do not specify any arguments, the PROF command displays the currently active profile. For a description of each available X.3 parameter profile, see “X. 3 parameter profiles” on page 94.
RESET	Reset a virtual circuit by generating a Reset-Request packet with 0 (zero) cause (DTE originated) and 0 (zero) diagnostic.
RPAR? [<param1>[,<param2>,...]]	Display the current values of the specified X.3 parameters on a remote PAD. If you do not specify one or more parameters (<param1>, <param2>, and so on), the RPAR? command displays all X.3 parameter values on a remote PAD. For a list of X.3 parameters, see “X.3 parameters” on page 91.

Table 22. X.25/PAD commands

Syntax	Description
RPROF [<profile> | ?]	Configure the remote PAD using the values associated with an X.3 parameter profile defined on the local PAD. • The <profile> argument specifies the name of the X.3 parameter profile to activate. • The question mark (?) keyword displays the currently active profile, followed by a list of available profiles. • If you do not specify any arguments, the RPROF command displays the currently active profile. For a description of each available X.3 parameter profile, see “X. 3 parameter profiles” on page 94
RSET [<param1>:<value1> [,<param2>:<value2>,...]]	Set the specified X.3 parameters (<param1>, <param2>, and so on) to the specified values (<value1>, <value2>, and so on) on the remote PAD. For a discussion of X.3 parameters and their possible values, see “X.3 parameters” on page 91.
RSET? [<param1>:<value1> [,<param2>:<value2>,...]]	Set the specified X.3 parameters (<param1>, <param2>, and so on) to the specified values (<value1>, <value2>, and so on) for the remote PAD; then, display each parameter and its value. If you specify the RSET? command without specifying any parameters or values, the MAX displays the current parameter values for the remote PAD. For a discussion of X.3 parameters and their possible values, see “X.3 parameters” on page 91.
SET [<param1>:<value1> [,<param2>:<value2>,...]]	Set the specified X.3 parameters (<param1>, <param2>, and so on) to the specified values (<value1>, <value2>, and so on). For a discussion of X.3 parameters and their possible values, see “X.3 parameters” on page 91.
SET? [<param1>:<value1> [,<param2>:<value2>,...]]	Set the specified X.3 parameters (<param1>, <param2>, and so on) to the specified values (<value1>, <value2>, and so on); then, display each parameter and its value. If you specify the SET? command without specifying any parameters or values, the MAX displays the current parameter values. For a discussion of X.3 parameters and their possible values, see “X.3 parameters” on page 91.
STATUS	Request the status of a virtual call placed to a remote DTE.

Table 22. X.25/PAD commands

Syntax	Description
TABS {LCL <num1>}{REM <num2>}{EXP <num3>}	Set and read 3 non-standard parameters that control tab expansion.These parameters are not accessible by the remote host using Q-bit packet PAD commands. You must keep the PAD's view of the current screen position accurate by setting EXP to 0 (zero) and LCL to the number of columns to which your terminal expands tabs. These settings enable the PAD to perform correct line folding, line deletion, and character deletion. • The LCL keyword sets the number of columns to which tabs are expanded locally (<num1>). If the EXP keyword disables local tab expansion, LCL <num1> specifies the number of columns to which the asynchronous device expands tabs sent to it. You can specify a number between 0 and 16. Zero specifies that no expansion takes place. • The REM keyword sets the number of columns to which tabs are expanded remotely (<num2>)—that is, on input from the terminal to the network. You can specify a number between 0 and 16. Zero specifies that no expansion takes place. • The EXP keyword enables (1) or disables (0) tab expansion locally. If you specify 1 after this keyword, tabs are expanded according to the LCL specification.

X.3 parameters

The user's terminal or host DTE can modify operations that the PAD performs by setting one or more X.3 parameters. Table 23 provides a list of these parameters.

Note: This table uses the term "DTE-C" to refer to a DTE that sends and receives characters. A standard DTE sends and receives packets.

Table 23. X.3 parameters

Parameter	Description	Possible values
1—Escape from data transfer	Specifies whether the terminal server user can escape from data transfer mode in order to modify or display other X.3 parameters using the X.25 PAD commands.	0—Escape not allowed 1—Escape allowed (the default)

Table 23. X.3 parameters

Parameter	Description	Possible values
2—Echo	Specifies whether the PAD performs a local echo to the DTE-C of all the characters it receives from the device.	0—No echo 1—Echo (the default)
3—Data forwarding signal	Specifies defined sets of characters that, when received from the DTE-C, cause the PAD to terminate packet assembly and forward the packet to the host DTE.	0—None (full packet) 1—Alphanumerics 2—Carriage return (the default) 4—ESC, BEL, ENQ, ACK 8—DEL, CAN, DC2 16—ETX, EOT 32—HT, LT, VT, FF 64—All other characters in columns 0 and 1 of International Alphabet #5
4—Idle timer	Specifies a time interval between characters received from the DTE-C. If the timer expires, the PAD terminates packet assembly and forwards the packet.	0—No timer 1–255—Delay value in twentieths of a second
5—Ancillary device control	Enables flow control from the PAD to the DTE-C. The PAD indicates whether it can accept characters from the DTE-C by transmitting the special characters X-ON/ X-OFF.	0—Not operational 1—Use X-ON (DC1 of International Alphabet #5) and X-OFF (DC3 of International Alphabet #5)
6—PAD service signals	Enables the DTE-C to determine whether it can transmit PAD service signals to itself. For a complete list of PAD service signals, see “PAD service signals” on page 95.	0—Do not transmit service signals 1—Transmit service signals
7—Procedure on break	Specifies the action that PAD takes upon receiving a break signal from the DTE-C.	0—No action 1—Transmit Interrupt packet 2—Reset 4—Indication of break (PAD message) 8—Escape from data transfer 16—Discard output to DTE-C 21—Combine actions 1, 4, and 16

Table 23. X.3 parameters

Parameter	Description	Possible values
8—Discard output	Specifies whether the PAD should discard packets it receives rather than disassemble them and transmit them to the DTE-C. This parameter works together with parameter #7. If you set parameter #7 to 16, the PAD discards all output to the DTE-C after it receives a break signal. Setting parameter #8 to 0 (zero) restores normal data delivery to the terminal.	0—Normal data delivery (the default) 1—Discard output to the DTE-C
9—Carriage return padding	Specifies whether the PAD inserts padding characters after a carriage return to enable a printing DTE-C to use the carriage return and maintain the hard copy's readability.	0—No padding 1-7—Number of padding characters inserted after the carriage return
10—Line folding	Enables the PAD to automatically determine the line length of character strings. You do not need to set this parameter if the terminal has auto-wraparound capability.	0—No line folding (the default) 1–255—Number of characters per line
11—DTE-C speed	Indicates the access speed of the DTE-C. This parameter is read only.	10—50 bps 5—75 bps 9—100 bps 0—110 bps 1—134.5 bps 6—150 bps 8—200 bps 2—300 bps The following values are dependent on the PAD type: 4—600 bps 3—1200 bps 7—1800 bps 11—75 bps from a DTE-C, 1200 bps to a DTE-C. 12—2400 bps 13—4800 bps 14—9600 bps 15—19200 bps 16—48000 bps 17—56000 bps 18—64000 bps

Table 23. X.3 parameters

Parameter	Description	Possible values
12—Flow control	Enables the DTE-C to specify flow control for incoming data from the PAD. The DTE-C indicates whether it can accept characters from the PAD by transmitting the special characters X-ON/ X-OFF.	0—Not operational 1—Use X-ON (DC1 of International Alphabet #5) and X-OFF (DC3 of International Alphabet #5)
13—Linefeed insertion	Specifies that the PAD inserts a linefeed when it detects a carriage return.	0—Option not selected 1—Linefeed insertion after a carriage return in data the PAD sends to the DTE-C 2—Linefeed insertion after a carriage return in data the PAD receives from the DTE-C 4—Linefeed insertion after echo of each carriage return to the DTE-C
14—Linefeed padding	Specifies that the PAD automatically inserts padding characters after detecting a linefeed character in a data stream transmitted to the DTE-C.	0—No padding 1-7—Number of padding characters inserted after the linefeed
15—Editing	Specifies whether the PAD performs editing during the data transfer state. Editing requires the PAD to recognize certain characters in the data stream so that it can take the appropriate action. These characters can be a backspace, delete, or other characters in the International Alphabet #5.	0—No editing in data transfer 1—Editing in data transfer
16—Character delete	Specifies the character to use as the “character delete” character.	0–127 (a character from the International Alphabet #5)
17—Line delete	Specifies the character to use as the “line delete” character.	0–127 (a character from the International Alphabet #5)
18—Line display	Specifies the character to use as the “line display” character.	0–127 (a character from the International Alphabet #5)

X. 3 parameter profiles

A user can select a set of PAD parameter values for a given session. Each set of parameters comprises an X.3 parameter profile. You can specify the default X.3 parameter profile using the MAX unit’s X.3 Param Prof parameter in the Connection Profile. For more information on this parameter, see “X.3 Param Prof” on page 84.

Table 24 lists the contents of each X.3 parameter profile.

Table 24. X.3 parameter profiles

X.3 parameter profile	Contents
CRT	1:64, 2:1, 3:2, 4:0, 5:0, 6:5, 7:2, 8:0, 9:0, 10:0, 11:0, 12:1, 13:4, 14:0, 15:1, 16:8, 17:24, 18:18, 19:2, 20:0, 21:3, 22:0
INFONET	1:1, 2:0, 3:2, 4:0, 5:0, 6:0, 7:21, 8:0, 9:2, 10:0, 12:1, 13:0, 14:2, 15:1, 16:8, 17:24, 18:18, 19:0, 20:0, 21:0, 22:0
SCEN	1:64, 2:1, 3:2, 4:0, 5:1, 6:5, 7:21, 8:0, 9:0, 10:0, 12:1, 13:4, 14:0, 15:1, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
CC_SSP	1:1, 2:1, 3:126, 4:0, 5:1, 6:1, 7:2, 8:0, 9:0, 10:0, 12:1, 13:0, 14:0, 15:0, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
CC_TSP	1:0, 2:0, 3:0, 4:20, 5:0, 6:0, 7:2, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0, 15:0, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
HARDCOPY	1:64, 2:1, 3:2, 4:0, 5:2, 6:5, 7:21, 8:0, 9:5, 10:80, 12:1, 13:4, 14:5, 15:1, 16:8, 17:24, 18:18, 19:1, 20:0, 21:3, 22:0
HDX	1:1, 2:1, 3:2, 4:0, 5:2, 6:5, 7:2, 8:0, 9:0, 10:0, 12:1, 13:4, 14:0, 15:1, 16:8, 17:24, 18:18, 19:2, 20:0, 21:3, 22:0
SHARK	1:0, 2:0, 3:2, 4:0, 5:0, 6:0, 7:2, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0, 15:0, 16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0
DEFAULT (MINIMAL)	1:64, 2:1, 3:2, 4:0, 5:2, 6:5, 7:2, 8:0, 9:25, 10:72, 12:1, 13:5, 14:25, 15:1, 16:8, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
NULL	1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0,15:0, 16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0

PAD service signals

The PAD transmits PAD service signals to the terminal server in order to acknowledge PAD commands and to inform the user about the internal state of the PAD. The terminal server user can suppress the reception of PAD service signals by setting PAD parameter #6 to 0 (zero).

Table 25 lists the PAD service signals.

Table 25. PAD service signals

Service signal	Description
RESET DTE	The remote DTE has reset the virtual circuit.
RESET ERR	A reset has occurred because of a local procedure error.
RESET NC	A reset has occurred because of network congestion.

Table 25. PAD service signals

Service signal	Description
COM	A call has been connected.
PAD ID	Precedes a string that identifies the PAD.
ERROR	The terminal server user entered an X.25/PAD command using faulty syntax.
CLR	A virtual circuit has been cleared.
ENGAGED	In response to the STAT command, this signal indicates that a virtual call is up.
FREE	In response to the STAT command, this signal indicates that a virtual call is cleared.
PAR with X.3 parameter reference numbers and their current values	This string is a response to the SET? command.

Sample X.25/PAD session

This section describes a basic X.25/PAD session.

Suppose that 555-6000 is the number of the hunt group for accessing the MAX unit's digital modem. The display for an X.25/PAD session looks like this one:

```
ATDT 769-6000

CONNECT 9600

ASCEND TERMINAL PAD v0.99:  ASYNC PORT # 1, 9600 BAUD

*
```

The asterisk (*) is a prompt for input.

If you have set Immed Service=X.25/PAD, and specified an X.121 address for the remote computer using the Immed X.121 Addr parameter or the Ascend-X25-X121Address attribute, the terminal server immediately connects you to the remote machine. If you have not specified a remote address, you must enter the CALL parameter. For example, to connect to a computer at 311021755555, enter this command line:

```
CALL 311021755555
```

The PAD responds with this message:

```
COM
```

You are now connected to the remote computer and its prompt or message appears on the screen. You can now send and receive data.

When you finish your session with the remote computer, make sure to log out properly. When you do so, the remote computer may clear the call. This message displays:

```
CLR XX XX
```

If the remote computer does not clear the call, you must do so yourself. Enter the special PAD recall character to signal the PAD that you want to enter a command. When you do so, the PAD prompt appears. Now, enter this command to clear the call:

```
CL or CLEAR
```

This message appears, confirming that the PAD has cleared the call:

```
CLR CONF
```

Local echo parameter added for Telnet

A MAX unit with a terminal server can echo characters locally. This allows users of these machines to connect to non-standard Telnet ports and programs. A new field has been added to the TServe options submenu of the Ethernet profile to configure the default setting for the local echo option.

A new Telnet command argument is also available for setting the local echo option from the command line and overriding the default .

How the local echo option works

Local echo mode is a line-by-line mode, where the line that appears as it is typed is not actually transmitted until a carriage return is entered. If local echo is enabled, the line transmitted is echoed on the local MAX terminal screen

A MAX unit with terminal server will initially have the default for local echo mode set to **Off**. A user can change this setting from the command line for the current session.

Note: If the remote server turns local echo on or off in its option negotiation for a telnet session, this setting will override the setting made locally.

Controlling local echo

The initial default setting for the local echo option is **No**. You can set the default behavior for local echo through the terminal server profile, configured in the Local Echo field of the Ethernet/Mod Config/TServ options submenu (Figure 5). This submenu sets the default terminal server behavior for the MAX.

The local echo field is not available if either the TS Enabled setting is no (terminal server not enabled) or if the telnet setting is no (telnet not enabled).

Note: The default local echo setting can be overridden from the Telnet command line.

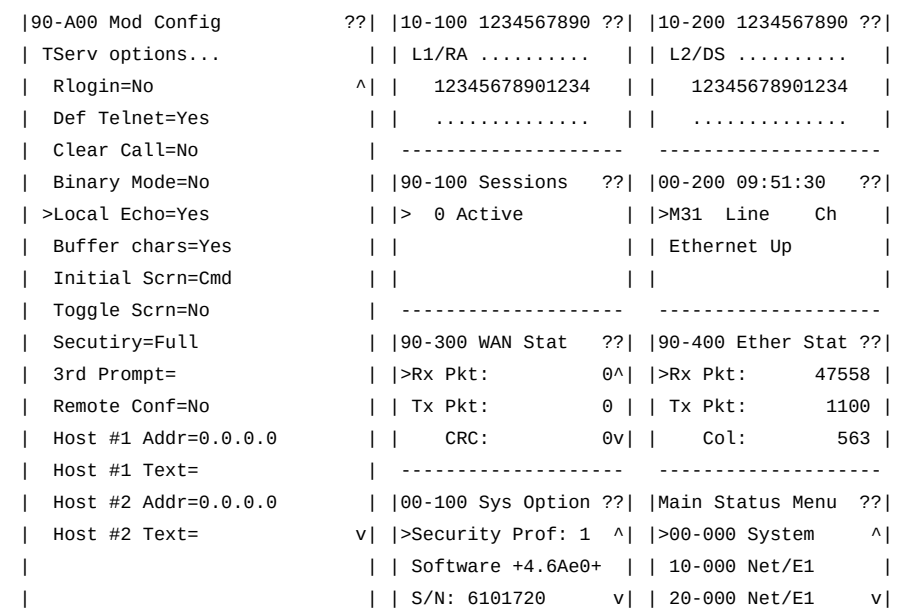


Figure 5. Ethernet Profile TServe Options Submenu

Setting the default for local echo

In the Ethernet/ModConfig/TServe options... submenu set the option to **`Yes`** to turn the default local echo option on. Set the option to **`No`** to turn local echo off and default to remote echo.

Setting local echo using Telnet command arguments

You can override the default setting using the Telnet command line.To set the local echo option from the command line, type one of the following:

Entry	Result
`telnet -l[e] host`	Turns local echo on.
`telnet -r[e] host`	Turns local echo off

PPP outdial for the v.110 card

Previously, the v.110 module in the MAX supported only incoming calls to the terminal server. Now, the MAX can make outgoing calls to a client on the other side of a v.110 terminal adapter using the PPP protocol. This feature also supports the callback feature via v.110 for the MAX Link Client software product.

To support this new functionality, 20 new settings for the Data Svc parameter in the Connection Profile have been added:

- v110 2.4 56K
- v110 4.8 56K
- v110 9.6 56K
- v110 19.2 56K
- v110 38.4 56K
- v110 2.4 56KR
- v110 4.8 56KR
- v110 9.6 56KR
- v110 19.2 56KR
- v110 38.4 56KR
- v110 2.4 64K
- v110 4.8 64K
- v110 9.6 64K
- v110 19.2 64K
- v110 38.4 64K
- v110 2.4 64KR
- v110 4.8 64KR
- v110 9.6 64KR
- v110 19.2 64KR
- v110 38.4 64KR

Each setting contains these elements:

- The string "v100".
- The bit rate for the v.110 card.

  The available bit rates are 2.4, 4.8, 9.6, 19.2, and 38.4.

  The MAX tries to communicate with the remote v.110 TA using the specified bit rate. If the MAX cannot sync up with the remote TA using the specified bit rate, it attempts to use one of the other four bit rates.
- The data service in use.

  A v.110 call is a digital call using one of these data services:

  - 56K, the unrestricted Switched-56 data service
  - 56 KR, the restricted Switched-56 data service
  - 64K, the unrestricted Switched-64 data service
  - 64KR, the restricted Switched-64 data service

For example, if you set Data Svc=v110 38.4 64KR, the MAX attempts to communicate with the remote v.110 TA using a bit rate of 38.4 over a line using the restricted Switched-64 data service.

Korean signaling

The Ascend software in MAX 4000 E1 units now supports Korean signaling, which is used in 70% of the Korean market.

Korean signaling is a version of the CCITT R2 signaling protocol, which can be used on E1 digital trunks for establishing/clearing 64Kbit/s switched circuits. Signaling is performed by A/B bit manipulation in channel 16 of the E1 frame (line signaling) only, and does not use in-band MF tone generation/detection (register signaling), as does R2 signaling.

Note: Korean signaling currently supports incoming calls only. However, its incoming call routing capabilities are very limited, because it does not receive answer-number digits from the network or distinguish between voice and data calls. If the default incoming call routing is not suitable for an application, the call can be routed by slot and port assignments.

Configuring Korean signaling in the MAX

In the MAX, you configure R2 signaling in the Net/E1 line profile. Table 26 lists the new parameters and parameter values.

Table 26. Korean signaling configuration

Location	Parameters
Net/E1→Line Config→Line N... (Line Profile)	Sig Mode=KOREAN

Sig Mode

Description: This parameter specifies the signaling that the line uses.

Usage: Press Enter to cycle through the choices.

- None indicates a leased line.
- ISDN specifies that the interface supports ISDN D-channel signaling.

  This setting is valid only if the MAX has the ISDN D-channel signaling option; otherwise, the MAX displays an error message.

  This setting is the default.
- DPNSS indicates that the interface supports DPNSS or DASS 2 signaling.

  DPNSS is another out-of-band signaling mode developed prior to ISDN. Its implementation in terms of channel usage varies from one country to another.
- R2 indicates that the interface supports R2 signaling.

  R2 signaling is a CCITT standardized signaling protocol, which can be used on E1 digital trunks for establishing and clearing 64Kbit/s switched circuits. Signaling is performed through a combination of A/B bit manipulation in channel 16 of the E1 frame (line signaling), and in-band MF tone generation/detection (register signaling).
- KOREAN indicates that the interface supports Korean signaling.

  Korean signaling is a version of the CCITT R2 signaling protocol that can be used on E1 digital trunks for establishing/clearing 64Kbit/s switched circuits. Signaling is performed by A/B bit manipulation in channel 16 of the E1 frame (line signaling) only, and does not use in-band MF tone generation/detection (register signaling), as does R2 signaling.

Note: Korean signaling currently supports incoming calls only. However, its incoming call routing capabilities are very limited, because it does not receive answer-number digits from the network or distinguish between voice and data calls. If the default incoming call routing is not suitable for an application, the call can be routed by slot and port assignments.

Parameter Location: Line Profile: Net/E1→Line Config→Any Line Profile→Line *n*

Dependencies: When R2 is selected, the Switch Type parameter is N/A. When KOREAN is selected, the Switch Type and # Complete fields are N/A.

See Also: Switch Type, # Complete

Secure Access support

Refer to the *Ascend Secure Access User's Guide* (part number 7820-0429-001) for complete instructions on using SAM and adding firewalls to your Ascend unit.

Ascend currently supports simple "static" packet filters. Each connection may have a call and/or a data filter profile. Each filter profile may have up to 12 inbound and 12 outbound packet filters. Each packet filter may be either a generic or an IP filter.

Secure Access adds these features to the current Ascend filtering:

- the capability to easily write "dynamic" packet filters, also known as "firewalls," which permit traffic to be normally blocked except when triggered by an event, such as an inbound or outbound connection request.
- the ability to log traffic passing through the router and thus provide an audit trail to track IP connections and packet content.
- the capability for the router to send an appropriate ICMP message when a packet is not forwarded due to a firewall.

A limitation of current Ascend packet filters and most other router packet filters is that they are not able to securely deal with a number of IP protocols. Secure Access uses "dynamic" packet filters, which allow the firewall to block all packets except for those that are specifically required for a single session and only for the length of the session.

Unlike the current limitations on the number of filters in a profile, Secure Access does not place a limit on the number of packet filters (that is "rules") in a firewall profile. The only limitation is based on the compressed size of the firewall profile or the limit of memory on the router.

To enable Secure Access on your Ascend unit, you must obtain a hash code.

Current Ascend packet filters continue to be supported and so no configuration changes on Ascend units are necessary until Secure Access firewalls are actually used.

Using SAM

Configuration of a firewall is done on a network-connected workstation external to the Ascend unit using the SAM graphical user interface. You then upload the completed firewall to the MAX where it will be used.

The external application, Secure Access Manager (SAM), allows you to select what services will be permitted to pass through the firewall and what hosts are allowed access to the services.

Once the data has been filled in, SAM can upload the firewall profile to an Ascend unit or save the profile into a file.

Refer to the *Ascend Secure Access User's Guide* (part number 7820-0429-001) for complete instructions on using SAM and adding firewalls to your Ascend unit.

New menu added to the Telnet interface

A new Firewalls menu has been added to the Telnet interface:

```
Edit
20-600 Firewalls
>20-601 Sales
```

When Secure Access has been enabled on the Ascend unit, this menu appears and stores all the firewalls that have been downloaded to your system using SAM. When you open the Firewalls menu, this submenu appears:

```
Edit
20-601 Sales
>Name=Engineering
 Version=1
 Length=2936
```

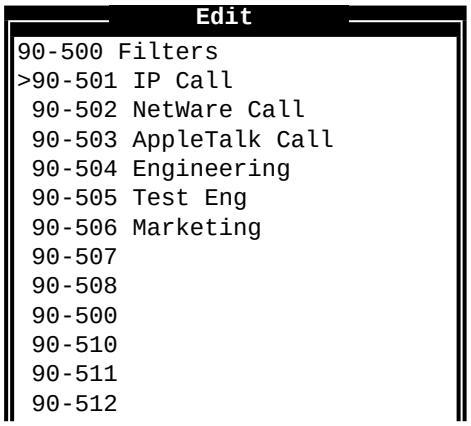
Note that only the Name field can be edited. The Version and Length parameters are determined by the firewall you create in SAM. Firewalls must be modified using SAM.

Firewall numbers in the Telnet interface

To ensure backward compatibility with the current Ascend filter implementation, you must number firewalls created with SAM differently than filters created using the Telnet interface. You can continue to assign existing filters to Profiles exactly as before. However, if you want to assign a firewall created with SAM to a Profile, you must add 100 to the last two digits of its index in the telnet interface. The numbering scheme for filters is:

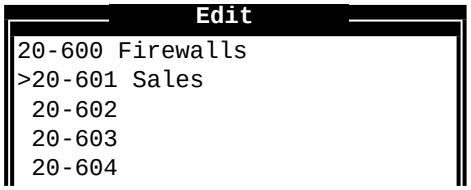
- 0 indicates that no filtering is being used
- 1-99 indicates that a filter created using the Telnet interface is being used
- 100-199 indicates that a filter created using SAM is being used.

For example, suppose you have already created these Ascend filters:



If you want to use the Engineering filter in a Connection or Mod Config Profile, enter the number 4 in the Data Filter or Call Filter field (in a Connection Profile) or in the Filter field (in the Mod Config, Ether options field).

Now suppose you have created a firewall using SAM and downloaded them to your Ascend unit. The Firewalls menu may look similar to this:



To use the Sales filter in a Connection or Mod Config Profile, enter the number 101 in the Data Filter or Call Filter field (in a Connection Profile) or in the Filter field (in the Mod Config, Ether options field).

Assigning firewalls to a Connection Profile

Firewalls assigned to a Connection Profile are used to filter incoming or outgoing traffic on a WAN connection. Filters assigned to a Connection Profile are activated whenever the WAN session comes online.

To assign a firewall to a Connection profile:

1. Create a firewall filter using SAM.
2. Download it to the Ascend unit.
3. Select Ethernet, Connections, *a Connection Profile*, Session options.
4. Enter the number of the firewall filter you want to use in the Data filter field.
   This number is derived from the number in the Firewall menu by adding 100 to the last 2 digits of the firewall index. For example, if the firewall is number 20-503, enter number 103 in the Data Filter field.
5. Exit the Connection Profile and save your changes.

Assigning firewalls to the Mod Config profile

Firewalls assigned to the Mod Config Profile are used to filter incoming or outgoing traffic on the Ethernet interface. Filters assigned to a the Mod Config Profile are activated as soon as you save the changes to the Mod Config Profile.

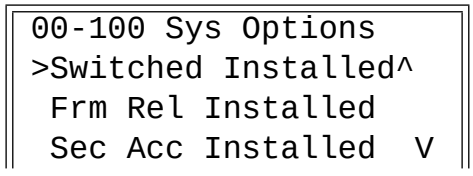
When you assign a filter to the Mod Config Profile,

To assign a firewall to the Mod Config Profile:

1. Create a firewall filter using SAM.
2. Download it to the Ascend unit.
3. Select Ethernet, Mod Config, Ether options.
4. Enter the number of the firewall filter you want to use in the Filter field.
   This number is derived from the number in the Firewall menu. For example, if the firewall is number 20-503, enter number 103 in the Data Filter field.
5. Exit the Connection Profile and save your changes.

New Sys Options field

Secure Access has been added to the Sys Option window. All software that includes the Secure Access feature will include a “Sec Acc” field. If the feature has not yet been enabled, the option will be marked as “Not Inst”. If the feature has been enabled, the option will be marked as “Installed.”



New parameters

These new parameters have been added or enhanced to support firewalls on Ascend products:

- Name
- Version
- Length

Name

Description: This parameter specifies the name of the firewall. This name is originally created using the Secure Access Manager (SAM) graphical user interface.

Usage: Press Enter to open a text field. Then, type the name of the firewall. Press Enter again to close the text field.

Parameter Location: Ethernet, Firewalls, *any Firewall*

Version

Description: Each firewall contains a version number to ensure that any firewall that is uploaded to the router will be compatible with the firewall software on the router. Secure Access Manager (SAM) checks the version number before uploading a firewall. In the event that a router with a stored firewall profile receives a code update that make the existing firewall incompatible, a default firewall is enabled, permitting only Telnet access to the Ascend unit.

Usage: This parameter cannot be edited.

Parameter Location: Ethernet, Firewalls, *any Firewall*

Length

Description: This specifies the length of the firewall uploaded to the Ascend unit from Secure Access Manager (SAM).

Usage: This parameter cannot be edited.

Parameter Location: Ethernet, Firewalls, *any Firewall*

Syslog messages

Syslog messages may be generated for packets seen by the firewall if specified by SAM. By default, SAM will cause a syslog message to be generated for all packets blocked by a firewall.

Syslog messages created by firewalls will use the standard format:

```
<date> <time> <router name> ASCEND: <interface> <message>
```

- <date> indicates the date the message was logged by syslog.
- <time> indicates the time the message was logged by syslog.
- <router name> indicates the router this message was sent from.
- <interface> is the name of the interface (ie0, wan0, and so on) or ‘call’ if the packet is logged by the call filter as it brings up the link.
- The <message> format has a number of fields, one or more of which may be present:
  `<protocol> <local> <direction> <remote> <length> <frag> <log> <tag>`

– <protocol> is the 4 hexadecimal digit Ether Type, or the network protocol name—“arp,” “rarp,” “ipx,” “appletalk.”

  <protocol>, for IP protocols, is either the IP protocol number (up to 3 decimal digits) or one of the following names:

  ip-in-ip

  tcp

  icmp

  udp

  esp

  ah

  In the special case of icmp, it will also include the ICMP Code and Type ([Code]/[Type]/icmp).

– <local>, for non-IP packets, is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. On a non-bridged WAN connection, the two MAC addresses will be all zeros.

  <local>, for IP protocols, is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it will also include the TCP or UDP port number ([IP-address];[port]).

– <direction> is an arrow “<-”, “->” showing the direction (receive and send respectively) in which the packet was traveling.

– <remote>, for non-IP protocols, has the same format as <local> non-IP packets but shows the destination Ethernet MAC destination address of transmitted packets and the source Ethernet MAC address of received packets.

  <remote>, For IP protocols, has the same format as <local> but shows the IP destination address of transmitted packets and the IP source address of received packets.

– <length> is the length of the packet in octets (8-bit bytes).

– <frag> is used to report “frag” if the packet has a non-zero IP offset or the IP More-Fragments bit is set in the IP header.

– <log> is used to report one or more messages based upon the packet status or packet header flags. The packet status messages include:

  corrupt—the packet is internally inconsistent

  unreach—the packet was generated by an “unreach=” rule in the firewall

  !pass—the packet was blocked by the data firewall

  bringup—the packet matches the call firewall

  !bringup—the packet did not match the call firewall

  TCP flag bits that will be displayed include syn, fin, rst.

  syn is will only be displayed for the initial packet which has the SYN flag and not the ACK flag set.

– <tag> contains any user defined tags specified in the filter template used by SAM.

Outgoing calling party number for PRI lines in RADIUS

The RADIUS daemon can now supply an outgoing calling party number; this number is part of the profile information the Ascend unit uses when placing a call over an E1 PRI line.

The Ascend-Billing-Number attribute (249) supplies the calling party number, and is equivalent in function to the Bill # parameter in your Ascend unit's local (non-RADIUS) Connection Profile. To specify a number for billing purposes that is different from the one associated with the Ascend unit, include the Ascend-Billing-Number attribute in the RADIUS profile that characterizes the outgoing call. Set the Ascend-Billing-Number attribute equal to the billing number. Furthermore, when the device at the far end answers the call, the calling-party number reported is the one you set for the Ascend-Billing-Number attribute.

Not all WAN providers allow this feature. You must determine whether your WAN provider accepts the request by the Ascend unit to insert a calling party number.

In the following example, when the MAX places a call to test-max, the number it dials is 5551212. The calling party number reported to the answering device and used for billing purposes is 4444444. If the setting Ascend-Billing-Number=4444444 were deleted, the calling party number would be the phone number of the telephone line or channel connected to the MAX over which the call was placed.

```
# Define a route that associates network 10.0.100 with dialout
# on PRI line WAN1.
route-1 Password = "ascend", User-Service = Dialout-Framed-User
   Framed-Route = "10.0.100.0/24 10.0.100.1 1 n test-max"


# Define a user profile for placing an outgoing call on PRI line WAN1.
# The Ascend-Billing-Number attribute specifies a billing number to
use
# for the call. This billing number is the calling party number.
test-max Password = "ascend", User-Service = Dialout-Framed-User
   User-Name = "test-max",
   Ascend-Dial-Number = "5551212",
   Ascend-Billing-Number = "444444",
   Framed-Protocol = PPP,
   Framed-Address = 10.0.100.1,
   Framed-Netmask = 255.255.255.0,
   Ascend-Metric = 2,
   Framed-Routing = None,
   Framed-Route = "10.5.0.0/24 10.0.100.1 1",
   Ascend-Idle-Limit = 30,
   Ascend-Send-Auth = Send-Auth-PAP,
   Ascend-Send-Secret = "passwrd1"
```

Fallback when RADIUS times out

A new option for CLID authentication enables a fallback position for CLID-authenticated RADIUS entries. In previous releases, if CLID authentication was required and a RADIUS query timed out, the call was rejected. In this release, a new CLID authentication option enables the MAX to fall back to regular name/password authentication specified in a resident profile (a Connection Profile or Password Profile).

Clid Auth

Description: This parameter specifies whether the MAX uses the calling party's phone number to authenticate incoming calls. CLID stands for calling party ID.

Usage: Press Enter to cycle through the choices.

- Ignore

  Ignore indicates that calling-party information is not required for authentication.

- Prefer

  Prefer specifies that when CLID is available, the calling-party's phone number must match the Calling # parameter (or the equivalent value in a RADIUS profile) before answering the call. However, if the CLID is not available, the MAX does not drop the call for that reason alone; instead it tries to authenticate using standard PAP/CHAP or terminal server authentication.

- Fallback

  Fallback handles the case where CLID authentication is specified in a RADIUS profile, as described next. However, if the RADIUS server query times out so CLID authentication could not be completed, the MAX does not drop the call for that reason alone; instead it looks for a resident profile (a Connection Profile or Password Profile) to use for standard PAP/CHAP or terminal server authentication.

- Required

  Required indicates that the calling-party's phone number must match the value of the Calling # parameter (or the equivalent value in a RADIUS profile) before the MAX can answer the call. If the CLID is not available, the MAX does not answer the call.

  When CLID authentication is Required and RADIUS is being used, the first line of the users profile does not include the username and password—instead it must specify the Calling number in the following format:

  ```
  <phonenum> Password="Ascend-CLID"
  ```

  See the *MAX RADIUS Supplement* for details.

Dependencies: In some installations, the WAN provider might not be able deliver CLIDs, or individual callers might choose to not publish the calling party ID. Ask your WAN provider whether ANI (Automatic Number Identification) is available, and whether the network conveys the calling party number to the receiving party. In some cases, the network does not deliver the calling party number, such as when the MAX is behind some PBXs.

Parameter Location: Answer Profile: Ethernet→Answer→PPP Options

See Also: AnsOrig, Calling #

New Traceroute command added to terminal server

A Traceroute command has been added to the terminal server interface. This command is similar to the existing terminal server Ping command. Traceroute is intended for use in network testing, measurement, and management. It is useful for locating slow routers and in diagnosing IP routing problems. It is available on all platforms that offer a terminal server interface and IP routing and Telnet or Rlogin.

Note: The Traceroute command is available from the terminal server interface if outgoing Telnet or Rlogin is enabled, or if the user has Operations security.

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route packets follow or finding the gateway that's discarding your packets can be difficult. The Traceroute command utilizes the IP protocol "time to live" field and attempts to elicit an ICMP Time Exceeded response from each gateway along the path to some host.

The Traceroute command syntax is:

```
traceroute [ -n ] [ -v ] [ -m max_ttl ] [ -p port ] [ -q nqueries ]
[ -w waittime ] host [ datasize ]
```

Note: The only mandatory parameter is the destination host name or IP number.

Options are:

Table 27. Traceroute command options

-n	Prints hop addresses numerically rather than symbolically and numerically (this eliminates a nameserver address-to-name lookup for each gateway found on the path).
-v	Verbose output. Received ICMP packets other than Time Exceeded and ICMP Port Unreachable are listed.
-m *max_ttl*	This sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.
-p *port*	Sets the base UDP port number used in probes. Traceroute hopes that nothing is listening on any of the UDP ports from the source to the destination host (so an ICMP Port Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range. The default is 33434.
-q *nqueries*	Sets the maximum number of queries for each hop. The default is 3.
-w *waittime*	Sets the time to wait for a response to a query. The default is 3 seconds.

Table 27. Traceroute command options

host	This mandatory parameter specifies the destination host by name or IP address.
datasize	Sets the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

Note: The -r and -s options (present in the UNIX version of Traceroute) are not supported.

The Traceroute command attempts to trace the route an IP packet would follow to some Internet host by launching UDP probe packets with a small TTL (time to live) and then listening for an ICMP “time exceeded” reply from a gateway. Probes start with a TTL of one and increase by one until we get an ICMP “port unreachable” message (which means we got to the host) or hit the maximum TTL.

Three probes are sent at each TTL setting and a line is printed showing the TTL, address of the gateway and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a 3 second timeout interval, a “*” is printed for that probe.

We don’t want the destination host to process the UDP probe packets so the destination port is set to an unlikely value, such as 33434.

Possible annotations after the time field are as follows:

Table 28. Time field options

!H	Host reached.
!N	Network unreachable.
!P	Protocol unreachable.
!S	Source route failed. This should not occur and may indicate that there is a problem with the associated device.
!F	Fragmentation needed. This should not occur and may indicate that there is a problem with the associated device.
!h	Communication with the host is prohibited by filtering.
!n	Communication with the network is prohibited by filtering.
!c	Communication is otherwise prohibited by filtering.
!?	Indicates an ICMP sub-code. This should not occur.
!??	Reply received with inappropriate type. This should not occur.

Analog modem diagnostic command in debug monitor

A new modem diagnostic command, modemDiag, has been added to the debug menu. This command displays diagnostic information related to an Ascend analog modem disconnect.

To use the modemDiag command, you must first enter debug mode by quickly typing this four-character sequence

Esc [Esc =

To toggle the modem diagnostics on or off, type:

modemDiag

at the debug monitor prompt.

After modemDiag has been turned ON and an analog caller disconnects, an output similar to this will be displayed:

```
TERMINATION REASON.......... LOCAL REQUEST
LAST TX data rate........... 300 BPS
HIGHEST TX data rate........ 300 BPS
LAST RX data rate........... 300 BPS
HIGHEST RX data rate........ 300 BPS
Error correction PROTOCOL... LAPM
Data COMPRESSION............ V42Bis
Line QUALITY................ 000
Receive LEVEL............... 053
```

This output will stop when modemDiag is turned OFF, by typing modemDiag again.

ATMP tunneling between IP networks

ATMP tunnels enable a mobile node to access a home network through two Ascend devices—a foreign agent and a home agent—across the Internet. Typically, the mobile node is a dial-in user. If the home network is an IP network, ATMP can also enable LAN-to-LAN connectivity through the tunnel.

Note: This functionality does not apply to IPX home networks.

To enable an IP router to connect as a mobile node, the foreign agent's RADIUS entry for the mobile node must specify *the same netmask as the home network*. For example, to connect to a home network whose router has this address:

```
10.168.3.1/28
```

The foreign agent's RADIUS entry for the remote router would contain lines like this:

```
Framed-Address = 10.168.6.21,
Framed-Netmask = 255.255.255.240,
```

With this address for the mobile node router, the connecting LAN can support up to 14 hosts.

- The "all zeros" (network base) address for the subnet is 10.168.6.16.

The network base address represents the network cable itself, which is always address 0.

- The “all ones” (broadcast) address for the subnet is 10.168.6.31.
  The broadcast address of any subnet is always all ones.
- The remaining host address range for the LAN is:
  `10.168.6.17 – 10.168.6.30`

In this example, the mobile node router has this address:

`10.168.6.21/28`

Routes to and from the mobile node’s LAN are handled differently, depending on whether the home agent is configured in router mode or gateway mode.

- Home agent in router mode
  If the home agent is directly connected to the home network, it should be configured to respond to ARP requests for the mobile node by setting Proxy ARP=Always.
  If the home agent is not directly connected to the home network, the situation is the same as for any remote network: routes to the mobile node’s LAN must either be learned dynamically from a routing protocol or configured statically.
  The mobile node always requires static routes to the home agent as well as to other networks reached through the home agent. (It cannot learn routes from the home agent.)
- Home agent in gateway mode
  If the home agent forwards packets from the mobile node across a nailed WAN link to the home IP network, the answering unit on the home network must have a static route to the mobile node's LAN.
  In addition, because no routing information is passed on the connection between the mobile node and the home agent, the mobile node’s LAN can only support local subnets that fall within the network specified in the RADIUS entry.
  For example, using the example RADIUS entry shown above, the mobile node could support two subnets with a netmask of 255.255.255.248: one at the 10.168.6.16 address and the other at the 10.168.6.24 address. The answering unit on the home network would have only one route to the router itself (10.168.6.21/28).

GSM data call support with 3.1khz SIC codes (DASS 2)

Prior to this release, GSM data calls through an ISDN network using DASS2 were masked with the SIC code as 10 = A- LAW 64K. However, this mask was removed and the calls were appearing with a SIC code of 18 = (3.1kHz audio at 9.6K). The MAX 4000 would not recognize this SIC code and dropped the incoming calls.

This new feature now allows the MAX to transparently route GSM data calls using the 3.1kHz SIC codes.

Setting the numeric base of the accounting session ID

Using the new Acct-ID Base parameter, you can now specify the numeric base of the RADIUS attribute Acct-Session-Id as either 10 or 16.This new feature provides improved compatibility between Ascend products and existing customer accounting systems.

Acct-ID Base

Description: This parameter specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16. It controls how the Acct-Session-ID attribute is presented to the accounting server.

The Acct-Session-ID attribute is defined in section 5.5 of the RADIUS accounting specification, which can be found at: ftp://ietf.cnri.reston.va.us/internet-drafts/draft-rigney-radius-accounting-01.txt

Usage: Press Enter to cycle through the choices.

- 10 (decimal) specifies that the numeric base is 10.
  The default is 10.
- 16 (hexadecimal) specifies that the numeric base is 16.

Example: When you set Acct-ID Base=10, a typical session ID is presented to the accounting server in this way:

```
"1234567890"
```

When you set Acct-ID Base=16, the same session ID is presented in this way:

```
"499602D2"
```

Dependencies: Changing the value of Acct-ID Base while sessions are active results in inconsistent reporting between the Start and Stop records.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→Accounting

New Filter persistence parameter

A new parameter, Filter persistence, has been added to the Connection Profile of all Ascend units that support Filter Profiles. This parameter must be set to Yes to allow a connections' firewalls to persist when the connection is torn down, such as by connection timeout. The default case is No, implying that, by default, connection firewalls do not persist when a call is terminated.

Note: Typically a firewall will persist for about an hour after its associated connection has been torn down.

Background on firewall and filter persistence

The idea of filter persistence is intended to allow an Ascend unit to preserve its filter/firewall specifications throughout the lifetime of its connections.

Firewalls differ from filters in that firewalls have been designed to alter their behavior as traffic passes through them, where filters remain unchanged through their lifetimes. This has required a change in the way firewalls and filters are associated with connections.

Ascend filters as they were originally implemented provided for the construction and destruction of filters whenever the state of a connection changed. This causes the Ascend unit to create and destroy filters during connection state changes without any reference to the state of the filters.

With Secure Access Firewalls, it is necessary to preserve the firewall state across the many transitions that connections may experience. Where filters could be built or destroyed at any time to accommodate changes due to Multilink and idle-inactivity conditions, firewalls simply cannot.

To resolve this problem, Ascend filters and firewalls can now be persistent. A persistent filter or firewall is maintained even when its associated connection becomes inactive. Additionally, the filter or firewall can be applied when an additional session becomes associated with a connection, as is the case with additional channels of an MPP connection.

Note: Firewalls must have persistence to work correctly, but filters do not.

Filter persistence and Connection Profiles

Connection Profiles describe different contact sites. Perhaps, for a small office, one profile would apply to a corporate home office, and another profile would apply to an Internet service provider. In each case, the user would like to use the Secure Access Firewall capability to prevent unauthorized incursions into the local network by others.

With dial-on-demand and automatic call timeout, the dynamic firewall capabilities of Secure Access Firewall would prevent in-progress TCP sessions (such as telnet or rlogin) from proceeding after a call termination and restart (due to inactivity, for example). Without persistence, a new firewall is constructed when a call starts up with no knowledge of any TCP sessions in progress, and consequently would block packets for those sessions when starting the line back up. This has the effect of rendering the in-progress telnet (or rlogin, etc.) sessions inoperative, possibly destroying work in progress that is dependent on them.

Filter persistence is a way to tell the Ascend unit to keep a firewall around even after the call is terminated. When a new call is placed to (or is received from) the same station, the Ascend unit remembers the original firewall and uses it as if the call had never been terminated. Thus, the user can continue working without loss.

Conversely, there may be times when a single Connection Profile is used for several different sites. This might be the case if you use the same Connection Profile to describe multiple different callers. In this case, you do not want the filters and firewalls to be persistent, since the Ascend unit cannot know if calls are arriving from the same users.

Filter persistence

Description: This parameter specifies whether the filter or firewall assigned to a Connection Profile should persist after the call has been disconnected.

Usage: Press Enter to cycle through the choices:

- Yes specifies that the filter or firewall assigned to this Connection Profile will persist after the connection has been torn down.

  Note: Typically a firewall will persist for about an hour after its associated connection has been torn down.
- No specifies that the filter or firewall assigned to this Connection Profile will not persist after the connection has been torn down.

  No is the default.

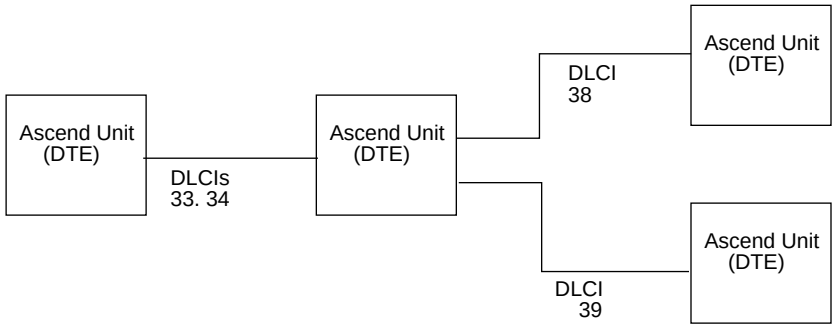
Parameter Location: Ethernet, Connections, any Connection Profile, Session options

See Also: Call Filter, Data Filter, Name, Version, Length

New Backup parameter features

In previous releases, if a Connection Profile in an Ascend unit was configured for Frame Relay and for backup, the Ascend unit did not bring up the backup connection when some, but not all, of the DLCIs in the connection to the Frame Relay switch were unusable. With this release, the Backup parameter causes the Ascend unit to bring up the backup connection when any of the DLCIs become unusable.

For example, consider this frame relay configuration. The Ascend unit connects to two remote routers, DTE 1 and DTE 2, through the frame relay cloud. The PVC (permanent virtual circuit) to DTE 1 consists of DLCIs 34 and 38, while the PVC to DTE 2 consists of DLCIs 33 and 39.



Suppose DTE 2 suddenly becomes unreachable, either because the link between the frame relay switch and DTE 2 fails, or because the link between the Ascend unit and the frame relay switch fails. In either case, the Ascend unit brings up the backup for DTE 2. (Specifically, the backup for the Connection Profile using DLCI 34.) Formerly, if the link to the frame relay switch remained up but, the Ascend unit would not bring up the backup connection, even though some of the Pivots, but not all, in that link had failed.

⇓ **If the primary connection is a nailed-up link to a frame relay switch and the backup connection is an ISDN BRI line, follow these steps to configure the unit for backup:**

1 Set FR Type=DTE or NNI in the Frame Relay Profile that carries the primary connection.

Each of these settings enables the Ascend unit to query the device at the other end of the Frame Relay Profile about the status of the DLCIs in the connection.The FR Type parameter on the remote device must be set to NNI or DCE.

2 Set Backup to the name of ISDN BRI backup Connection Profile.

3 In the backup Connection Profile, set the Idle parameter.

When the primary (nailed-up) connection is restored, traffic is redirected to it, idling the ISDN BRI link. The ISDN BRI connection is released after the period of time specified by the Idle parameter.

RADIUS Ascend-Menu Item attribute changes

The Ascend-Menu-Item attribute (206) enables you to define a menu of selectable items for a RADIUS-authenticated user. The purpose of the menu is to predefine a list of terminal server

options accessible by the user. The menu appears in lieu of the terminal server prompt and is defined on a per-profile basis.

The attribute contains a new <match> option that lets you enter one or more characters in order to choose a menu item. The attribute is described in the section that follows.

Ascend-Menu-Item (Attribute 206)

Description: Ascend-Menu-Item defines a single menu item that appears in lieu of the terminal server prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile. Additional entries are ignored. The menu items display in the order in which they appear in the RADIUS profile.

Using this attribute, you can configure the terminal server users file entry to give the user a custom menu of items from which to choose. The server uses the custom menu to present the user with a subset of terminal server commands. The user does not have access to the regular menu or to the terminal server command line; the menu items you specify are the only ones that appear.

Usage: Enter your specifications using this format:

Ascend-Menu Item=<command>;<text>[;<match>]

- <command> is the string sent to the terminal server when the user selects the menu item.
  The <command> specification must be in a format that the Ascend terminal server understands, and can contain up to 80 characters.
- <text> is the text displayed to the user.
  The maximum length for <text> is 31 characters.
- <match> is the pattern the user must type to select the item.
  The maximum length for <match> is 10 characters. Blanks are considered part of the matching pattern.
- The first semi-colon (;) that appears acts as the delimiter between <command> and <text>; the second semi-colon that appears acts as the delimiter between <text> and <match>.

If any entry consists of an option containing more that the maximum number of characters allowed, the RADIUS server discards the entry.

Example: Suppose you set these attributes:

```
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 machine",
   Ascend-Menu-Item="show arp;Display ARP Table"
```

The terminal server displays this text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
         Enter Selection (1-4, q)
```

Now, suppose you also enter specifications for the <match> option, as in this entry:

```
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. Ctrl-C stops ping;p",
```

Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's machine;t",
Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",

The terminal server displays this text:

```
ip=Display ip stats          p=Ping server. Ctrl-C stops ping
t=Telnet to Ken's machine    dsp=Display arp table
                Enter Selection (q=quit)
```

Note that you cannot combine numeric menu selections with pattern matching. The first Ascend-Menu-Item determines whether the screen displays numbered selections or patterns. This example shows what you should not do:

emma Password = "m2dan", User-Service=Login-User
Ascend-Menu-Item="show ip stats;ip=Display ip stats",
Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C stops ping;p",
Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's machine;t",
Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",

If you mix numbered selections and pattern matching as in this example, the terminal server screen displays the following text:

```
1. ip=Display ip stats              3. t=Telnet to Ken's machine
2. p=Ping server. Ctrl-C stops ping  4. dsp=Display arp table
             Enter Selection (1-4, q)
```

Dependencies: The Ascend-Menu-Item attribute is sent in Authentication-Response packets.

Check for PPP before authentication of remote session

In this release, the Ascend unit checks each packet for a PPP header before authentication of a remote terminal server session. If it detects a PPP header, it starts a PPP session. This new feature applies to all Ascend products that support digital modems and CHAP/PAP authentication.

ATMP connections that bypass a foreign agent

ATMP tunnels enable a mobile node to access a home network through two Ascend devices—a foreign agent and a home agent—across the Internet. In this release, if a home agent MAX has the appropriate RADIUS entry for a mobile node, the mobile node can connect directly to the home agent.

An ATMP-based RADIUS entry that is local to the home agent enables the mobile node to bypass a foreign agent connection, but it does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS entries for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

For example, the following RADIUS entry authenticates a mobile NetWare client that will connect directly to the home agent. In this example, the home agent is configured in gateway mode (it forwards packets from the mobile node across a nailed WAN link to the home IPX network):

```
mobile-ipx Password = "unit"
        User-Service = Framed-User,
        Ascend-Route-IPX = Route-IPX-Yes,
        Framed-Protocol = PPP,
        Ascend-IPX-Peer-Mode = IPX-Peer-Dialin,
        Framed-IPX-Network = 40000000,
        Ascend-IPX-Node-Addr = 12345678,
        Ascend-Home-Agent-IP-Addr = 192.168.6.18,
        Ascend-Home-Network-Name = "dave's max",
        Ascend-Home-Agent-Password = "pipeline"
```

Note: If the home agent is configured in router mode (if it forwards packets from the mobile node to its internal routing module), the Ascend-Home-Network-Name line is not included in the user entry. The Ascend-Home-Network-Name attribute specifies the name of the answering unit across the WAN on the home IPX network.

Inverse ARP for Frame Relay

Inverse Address Resolution Protocol (InARP) allows a device to resolve the protocol address of another device when the hardware address is known. In the case of Frame Relay the hardware address is the DLCI. The Ascend implementation of Inverse ARP will only respond to Frame Relay and IP Inverse ARP requests.

Inverse ARP requests *must* be of the following type:

- ARP protocol type of IP (0x8000)
- ARP hardware address type is the 2 byte Q.922 address

All other types will be discarded.

The Inverse ARP response will fill in the following fields:

- ARP source protocol address is the IP address of the Ascend device. This is found in the Mod Config, Ether Options, IP Adrs parameter.
- ARP source hardware address is the Q.922 address of the local DLCI.

Note: The Ascend unit does not issue any Inverse ARP requests.

Refer to RFCs 1293 and 1490 for details on Inverse ARP.

Displaying the software load name

In this release of the Ascend software, the name of the software load is displayed in the Sys Options status window and in fatal error messages. The load name is an important aid to troubleshooting error conditions.

Ascend software releases are distributed in software *loads*, which vary according to the functionality and target platform for the binary. For example, these are some of the loads available for the current release:

Table 29. Software Loads

Load name	Platform and functionality
m18bri.bin	MAX-1800 BRI
m18briip.bin	MAX-1800 BRI (IP only)
mhpt1.bin	MAX-HP T1
mhpt1ip.bin	MAX-HP T1 (IP only)
mhpt1bip.bin	Multiband MAX-HP (IP only)

and so forth...

The load appears in the Sys Options status window, for example:

```
00-100 Sys Option
>Multiband MAX-HP      ^
 Load: mhpt1bip
 Switched
Installed     v
```

The load name is also displayed in fatal error messages. For example:

```
> fat
WARNING: Index: 201 Load: mhpt1bip Revision: 4.6ci1
       Date: 06/03/1996.       Time: 13:04:48
       Location: b0149048 b013f6c0 b014915c b0073450 00000000
b2807400
```

Host status group SNMP support for V.110 data svc

The hostStatusDataSrv in the Ascend MIB's hostStatusTable (Ascend 7) now supports V.110 PPP outdial data svc types. 20 new data svc types have been added to support v.110 outdial.

hostStatusDataSvc changes

20 new data service types have been added to the hostStatusDataSvc type MIB object.

```
hostStatusDataSvc   OBJECT-TYPE
       SYNTAX          INTEGER {
            ...
            ...
            ...
```

```
                /Additions/
                                serviceV110-24-56K( 38 ),
                                serviceV110-48-56K( 39 ),
                                serviceV110-96-56K( 40 ),
                                serviceV110-192-56K( 41 ),
                                serviceV110-384-56K( 42 ),
                                serviceV110-24-56KR( 43 ),
                                serviceV110-48-56KR( 44 ),
                                serviceV110-96-56KR( 45 ),
                                serviceV110-192-56KR( 46 ),
                                serviceV110-384-56KR( 47 ),
                                serviceV110-24-64K( 48 ),
                                serviceV110-48-64K( 49 ),
                                serviceV110-96-64K( 50 ),
                                serviceV110-192-64K( 51 ),
                                serviceV110-384-64K( 52 ),
                                serviceV110-24-64KR( 53 ),
                                serviceV110-48-64KR( 54 ),
                                serviceV110-96-64KR( 55 ),
                                serviceV110-192-64KR( 56 ),
                                serviceV110-384-64KR( 57 )
   ACCESSread-only
   STATUSmandatory
   DESCRIPTION“The type of service from the current call
profile
         for the indexed host slot and port.”
   ::= { hostStatusEntry 7 }
```

The definitions of the 20 new enumerations are as follows:

- serviceV110-24-56K(38):

  The call should be set up as a data call with explicit request for 56Kbps unrestricted data transfer with v.110 bitrate of 2400

- serviceV110-48-56K(39):

  The call should be set up as a data call with explicit request for 56Kbps unrestricted data transfer with v.110 bitrate of 4800

- serviceV110-96-56K(40):

  The call should be set up as a data call with explicit request for 56Kbps unrestricted data transfer with v.110 bitrate of 9600

- serviceV110-192-56K(41):

  The call should be set up as a data call with explicit request for 56Kbps unrestricted data transfer with v.110 bitrate of 19200

- serviceV110-384-56K(42):

The call should be set up as a data call with explicit request for 56Kbps unrestricted data transfer with v.110 bitrate of 38400

- serviceV110-24-56KR(43):
  The call should be set up as a data call with explicit request for 56Kbps restricted data transfer with v.110 bitrate of 2400
- serviceV110-48-56KR(44):
  The call should be set up as a data call with explicit request for 56Kbps restricted data transfer with v.110 bitrate of 4800
- serviceV110-96-56KR(45):
  The call should be set up as a data call with explicit request for 56Kbps restricted data transfer with v.110 bitrate of 9600
- serviceV110-192-56KR(46):
  The call should be set up as a data call with explicit request for 56Kbps restricted data transfer with v.110 bitrate of 19200
- serviceV110-384-56KR(47):
  The call should be set up as a data call with explicit request for 56Kbps restricted data transfer with v.110 bitrate of 38400
- serviceV110-24-64K(38):
  The call should be set up as a data call with explicit request for 64Kbps unrestricted data transfer with v.110 bitrate of 2400
- serviceV110-48-64K(39):
  The call should be set up as a data call with explicit request for 64Kbps unrestricted data transfer with v.110 bitrate of 4800
- serviceV110-96-64K(40):
  The call should be set up as a data call with explicit request for 64Kbps unrestricted data transfer with v.110 bitrate of 9600
- serviceV110-192-64K(41):
  The call should be set up as a data call with explicit request for 64Kbps unrestricted data transfer with v.110 bitrate of 19200
- serviceV110-384-64K(42):
  The call should be set up as a data call with explicit request for 64Kbps unrestricted data transfer with v.110 bitrate of 38400
- serviceV110-24-64KR(43):
  The call should be set up as a data call with explicit request for 64Kbps restricted data transfer with v.110 bitrate of 2400
- serviceV110-48-64KR(44):
  The call should be set up as a data call with explicit request for 64Kbps restricted data transfer with v.110 bitrate of 4800
- serviceV110-96-64KR(45):
  The call should be set up as a data call with explicit request for 64Kbps restricted data transfer with v.110 bitrate of 9600
- serviceV110-192-64KR(46):
  The call should be set up as a data call with explicit request for 64Kbps restricted data transfer with v.110 bitrate of 19200
- serviceV110-384-64KR(47):

The call should be set up as a data call with explicit request for 64Kbps restricted data transfer with v.110 bitrate of 38400

New RADIUS Ascend-Data-Svc values

You can set the Ascend-Data-Svc attribute (247) to two new values: Nailed-56KR and Nailed-64K.

- Nailed-56KR represents the 56K data service for restricted data over nailed-up lines.
- Nailed-64K represents the 64K data service over nailed-up lines.

These values have been added to support Frame Relay Profile definitions.

This example assigns the Nailed-64K data service to the profile:

```
frdlink-top-1 Password="ascend" User-Service=Dialout-Framed-User
    Ascend-FR-Nailed-Grp=1,
    Ascend-FR-Profile-Name="fr1",
    Ascend-FR-Type=Ascend-FR-DCE,
    Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
    Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
    Ascend-Data-Svc=Nailed-64K
```

IPX Type 20 packet propagation support

Some applications (like NETBIOS) 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.

Some applications, like NetBIOS over IPX, will not work when they are an Ascend production as a router between Home and Work network - Ascend config now supports a flag to switch IPX Type 20 propagation ON and OFF.

SNMP Enhancements

The following new features have been added to SNMP:

- Return a more detailed breakdown of product codes in the mib-2 system sysObjectID
- Add new BRI status information
- Expanded options for tsave command

mib-2 system sysObjectID changes

There are new values returned from the { mib-2 system sysObjectID } product identification OID:

{ ascend products max 1 } for Max200

{ ascend products max 2 } for Max1800

{ ascend products max 4 } for Max4000

{ ascend products pipeline 2 } for Pipe25

{ ascend products pipeline 3 } for Pipe25PX

{ ascend products pipeline 4 } for Pipe25FX

{ ascend products pipeline 5 } for Pipe50

{ ascend products pipeline 6 } for Pipe75

{ ascend products pipeline 7 } for Pipe130

{ ascend products pipeline 8 } for Pipe400

slotItemStatus object added to the Ascend MIB

Within the { ascend slots } group there is a new slotItemStatus := { ascend slots 3 1 6 }. This read-only object reports the status of the item in the slot:

```
slotItemStatusOBJECT-TYPE
    SYNTAXINTEGER {
            statusOther( 1 )--for non-BRI slot
            slotItemNotRunning( 2 )--the item in the slot is not running
            briLinkNotStuffed( 3 )--for those interfaces that are not
          --  part of this variation, but are part of the array due to
          --static array sizing
           briLinkDisabled( 4 )--The link has been explicitly disabled
          --by the user in the configuration information
            briDown( 5 )--No physical link
            briNotInit( 6 )--No link at Layer 2
            briNotInitWithL2( 7 )--Management entity state NOT_INIT, but
          --we do have a layer 2 link established
            briPInit( 8 )--Initialized as a point-to-point link
            briMInit( 9 )--Initialized as a multi-point link
       }
    ACCESSread-only
    STATUSmandatory
    DESCRIPTION "The current status of this item in this slot."
    ::= { slotItemEntry 6 }
```

TFTP configuration support added to the Ascend MIB

The sysConfigTftpCmd { ascend systemStatusGroup sysConfigTftp 1 } now has the following values that can be set:

- tsave (1), save the current configuration to a file. This saves only non-default parameter values.
- trestore (2), upload a valid configuration from a file via TFTP
- tsave -a (3), save the current configuration to a file. This saves all parameter values, even those with default values.
- tsave -m (4), save the current configuration to a file, using the MIB OID (relative to the Ascend Enterprise) instead of the VT-100 interface names. This saves only non-default parameter values.
- tsave -am (5), save the current configuration to a file, using the MIB OID (relative to the Ascend Enterprise) instead of the VT-100 interface names. This saves all parameter values, even those with default values.

Carriage return now allowed with asynchronous PPP

Prior to this release, if a calling unit connected to an Ascend unit through an analog modem, V.120 device, or V.110 device, and the calling unit sent a carriage return before starting asynchronous PPP, the Ascend unit would not start PPP. Now, a device calling into an Ascend unit using a modem, V.120, or V.110 connection can run scripts that send a carriage return before starting asynchronous PPP.

Allow phone number specification in CRS command

Formerly, you could specify a phone number for outgoing calls using only the V.25bis CRN command. You can now specify a phone number using the V.25bis CRS command.

This feature applies when the Ascend unit is connected to a device with serial host interfaces, such as a video codec or a router; the feature includes changes to the V.25bis protocol extensions developed by Ascend Communications and Cisco.The V.25bis protocol defines a means of initiating a call to the WAN through the serial host interface.

The phone number can contain up to 20 characters. Specifying a phone number in the CRS command simplifies the placement of a BONDING call. You can specify a BONDING or other profile in the CRS command, followed by a phone number. The specified phone number is stored in the current Call Profile.

ATMP multi-mode agent support

In this release, an Ascend device can be configured to act as an ATMP (Ascend Tunnel Management Protocol) home agent or foreign agent on a tunnel-by-tunnel basis. A typical network topology would be something like this:

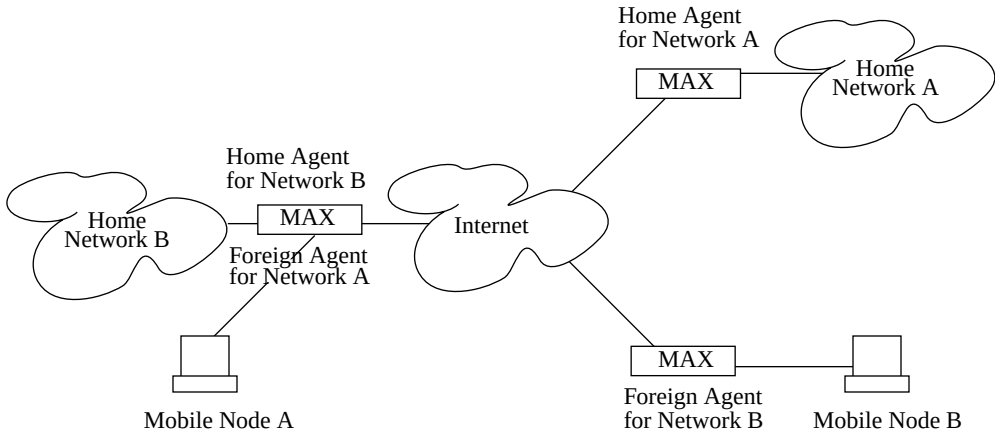


Figure 6. MAX acting as both home agent and foreign agent

Configuring the MAX as a multi-mode agent

To configure the MAX to act as a foreign agent and home agent on a tunnel-by-tunnel basis:

1 Open the Ethernet Profile.

2 Open the ATMP options submenu.

```
Edit
90-B00
 ATMP options...
  ATMP Mode=Both
  Type=Router
  Password=string
  SAP Reply=No
  UDP Port=5150
```

3 Set ATMP Mode to Both.

`ATMP Mode=Both`

This setting indicates that the MAX will function as both a home agent and foreign agent on a tunnel-by-tunnel basis.

4 Set the connection type to Router or Gateway, as appropriate.

5 Specify a password.

The password is needed only when accessing this unit as a home agent.

6 Specify the SAP reply setting.

For example:

`SAP Reply=No`

This field is used only when accessing this unit as a home agent. It enables or disables a home agent's ability to reply to the mobile node's IPX Nearest Server Query. If set to Yes, then the home agent will reply to the mobile node's Nearest Server Query if it knows about a server on the Home Network. If set to No, the home agent simply tunnels the mobile node's request to the home network.

7 Specify the UDP port if necessary, or leave the default 5150.

8 Close the Ethernet Profile.

ATMP multi-mode parameter

ATMP Mode

Description: This parameter specifies whether ATMP (Ascend Tunnel Management Protocol) is enabled and, if so, whether this unit is a home agent or a foreign agent.

Usage: Press Enter to cycle through the choices.

- Disabled specifies that ATMP is not enabled.
  Disabled is the default.
- Foreign specifies that this unit is a foreign agent.
- Home specifies that this unit is a home agent.
  Both specifies that the MAX will function as both a home agent and foreign agent on a tunnel-by-tunnel basis.

Dependencies: If you set ATMP Mode=Disabled, all other fields in the ATMP Options menu are set to N/A.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→ATMP Options

See Also: ATMP Gateway, Password, Type, UDP Port

Major improvement in Digital Modem code

All products that support digital modems will have new code with this release. The new code supports up to 33.6 Kbps carrier speed for DM 12 and DM 8 slot cards (12 and 8 modem cards) and allows up to 33.6 Kbps analog dial-in clients.

On Ascend products that have digital modems, the following parameter choice was added to support the new speed: In the Max Baud parameter, you can now set the value to 33600 (which is now the default). Previously, the default setting and highest rate was 28800. This parameter is located in Ethernet/Mod Config.

Note: The new digital modem card requires a different software option than the old digital modem card. As such, you cannot install both types of cards in the same system.

OSPF Global Options (ASBR enabled)

The MAX would become an Autonomous System Boundary Router (ASBR) when it was not set to do so. A new submenu of the OSPF Global settings may be set to enable or disable ASBR.

Parameter Location: Ethernet>Mod Config>OSPF global options>Enable ASBR

Support for high-bandwidth multicast applications

For high-bandwidth data, voice, and audio multicast applications, this release of the Ascend software supports these new features:

- Multicast rate limiting
- Prioritized packet dropping

Multicast rate limiting

To prevent multicast clients from creating response storms to multicast transmissions, you can configure the MAX to limit the rate at which packets are accepted from clients. The multicast rate limit specifies how many seconds the MAX waits before accepting another packet from multicast clients. By default, it accepts one packet from multicast clients every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Note: To communicate with a multicast (MBONE) router, the MAX acts as a multicast client on one interface, receiving queries from the router and responding using IGMP-v1. The interface on which the multicast router resides is the MAX unit's MBONE interface. A multicast rate limit on the MBONE interface is ignored.

To configure the multicast rate limit on Ethernet (if the Ethernet is not the MBONE interface):

1 Open the Ethernet Profile.

2 Specify the multicast rate limit on Ethernet.
For example:

```
Multicast Rate Limit=10
```

3 Close the Ethernet Profile.

There is no RADIUS support for rate limiting on Ethernet.

To configure the multicast rate limit on a WAN connection (if the link is not the MBONE interface):

1 Open a Connection Profile.

2 Specify a number of seconds in the Multicast Rate Limit parameter.
For example:

```
Multicast Rate Limit=10
```

3 Close the Connection Profile.

Multicast rate limiting on a WAN connection is supported in RADIUS via the Ascend-Multicast-Rate-Limit attribute.

Multicast Rate Limit

Description: This parameter specifies how many seconds the MAX waits before accepting another packet from a multicast client. By default, it accepts one packet from multicast clients every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

In the Ethernet Profile, the rate limit applies to multicast clients on the Ethernet. In a Connection Profile, the rate limit applies to multicast clients across that WAN connection. If a multicast rate limit is specified on the MAX unit's MBONE (multicast backbone) interface, it is ignored.

Usage: Press Enter to open a text field, and then type the number of seconds. The default value is 5. If this parameter is set to 0, no rate limiting is applied.

Press Enter again to close the text field.

Example: Multicast Rate Limit=2

Dependencies: This parameter has no effect when applied to the MBONE interface.

Parameter Location: Connection Profile:Ethernet->Connections->any profile
Ethernet Profile:Ethernet->Mod Config

See Also: Multicast Forwarding, Mbone Profile, Multicast Client

Prioritized packet dropping

For high-bandwidth data, voice, and audio multicast applications, the transmitting device may send more packets across a connection than available bandwidth can handle. If the MAX is the receiving device under extremely high loads, high priority packets will be less likely to be dropped than low priority packets. Priority is determined by UDP port ranges.

Table 30. UDP port ranges and packet priority

UDP Port Range	Type of Traffic	Priority
0—16384	Unclassified	Lowest (50)
16384—32768	Audio	Highest (70)
32768—49152	Whiteboard	Medium (60)
49152—65536	Video	Low (55)

Upgrading system software

To upgrade your MAX with this version of software, follow these steps:

1. Obtain the correct binary, either by downloading it from the FTP server or by contacting Ascend as described in "How to use this Release Note" on page 1.
2. If necessary, activate a Security Profile that allows for field upgrade.
3. If you're not sure how, see the section on Security Profiles in your documentation that came with your product.

4 Save your current MAX configuration to your computer's hard disk.

Uploading system software overwrites all existing profiles. Save your current profiles to your hard disk before you begin upgrading system software or you will have to reconfigure all your profiles. If you're not sure how, see the section on saving a configuration to disk in your Ascend product documentation.

Note: For security reasons, saving a configuration to disk wipes out all passwords in the text file. When you restore the configuration, the default (factory-set) passwords are reinstated. See the section on Security Profiles in your Ascend product documentation for more details.

5 Type the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):

```
Esc [ Esc -
```

(Press the escape key, the left bracket key, the escape key, and the minus key, in that order, in rapid succession.) You will see the following string of Xmodem control characters:

```
CKCKCKCK
```

If you don't see those characters, you probably didn't press the four-key sequence quickly enough. Try again—most people use both hands and keep one finger on the escape key.

6 Use the Xmodem file transfer protocol to send the system binary to the MAX.

7 Your communications program begins sending the binary file to your MAX. This normally takes anywhere from 5 to 15 minutes. The time displayed on the screen does not represent real time. Don't worry if your communication program displays several "bad batch" messages. This is normal.

8 When the upgrade process is complete, the MAX resets itself. When the self-test is complete, the Configure Profile appears in the Edit window with all parameters set to default values.

9 Restore your configuration from the text file saved on your hard disk.
If you are not sure how to restore a configuration, see the section on restoring a configuration in your Ascend product documentation.

Problems fixed in this version

The following problems were fixed in Ascend system software, version 4.6C:
TR 693: After LCP completion, reconfiguration was not correct

The connection negotiations handled by Link Control Protocol (LCP) was not retained. As a result MRU values were not known. Setting MRU to 1500 enabled a workaround.

TR 809: IP Pools count out of sync with actual users logged in

With pre-allocated IP Pools, pool addresses could be lost with multiple MP connections. Additionally, pool addresses were not always freed if a call ended while waiting for a response from RADIUS. In some cases users could not connect and were issued the message, `Number of remaining allocated addresses: 0'.

TR 895: Frame relay link goes out of service periodically

Frame Relay Annex D control messages were lost under high loads. These are now assigned a

high priority, providing a much higher success rate (even when a lack of buffers would otherwise prevent transmission), and are also given a high priority during periods of reduced latency.

TR 915: Callback used with CLID did not work

When performing callback with CLID authentication enabled, the MAX did not properly disconnect the originating unit (about 20 seconds was required to completely disconnect). As a result, the original caller did not see the message "LAN session up."

TR 944: Alarm LED did not function

The Alarm LED did not light if a WAN was disabled or had an error. The product has been modified to exclude the Yellow Alarm condition and to light if any WAN has an error state.

TR 947: MAX 4000 (4.5Ci12) PPP LCP fails when accessed by a 1200bps modem.

Problem detected as early as release 4.5Ap17 up to 4.5Ci12, users with modem speeds as low as 1200 bps were unable to negotiate access to the MAX 4000. On the MAX side, a Config Request was repeated on encountering the slow modem and then access was rejected (NAK). The client side resulted in an LCP time-out error.

TR 979: MAX 4000 (4.4Bp34) SNMP billing did not report PPP to MP.

When a user changed from PPP to MP both eventType 4 (service changed) and eventType 15 (MP) were not logged.

TR 985: MAX 4000 (4.6A) multichannel calls appeared as a 64k and a 0k session.

When an MP+ user dialed in, the call was seen from a Pipeline 50 (or a Cisco 2503) as 2 sessions rather than a single 2-channel call. The sessions were composed of a 64k session and a 0k session. If one channel was dropped due to lack of traffic, it was the 64k channel. From the Pipeline 50 or Cisco 2503, it appeared that a single 64k session was still active, but no router activity was present.

TR 992: Problem handling TCP Urgent Data Segments

When making a telnet call from the MAX terminal server through a Cisco protocol translator, the TCP Urgent Data Segment issued back to the MAX would cause it to hang.

TR 995: MAX (4.6Ai3) host ports return to default settings after reboot.

The MAX was unable to operate with multiple video calls and would reset itself to the default settings on reboot. For example, if the box was reconfigured so that ports 2, 4, and 6 were set as slaves to ports 1, 3, and 5, rebooting the system returned the settings to the default.

TR 1017: MAX 4000 (4.6Ai3) RADIUS would not show calling number consistently.

In the RADIUS callback accounting reports, a line item for the Client-Port-DNIS was inconsistently included (sometimes it was included and for no apparent reason, sometimes it was not). It is no longer included for callback accounting.

TR 1048: MAX 4000 (4.6Ai12) displayed two sessions for a single two-channel session.

When a Pipeline 25-Px called in, 2 sessions were displayed for a single 2-channel session. The problem was a display-only problem with the MAX 4000.

TR 1053: Using Immed-Raw-TCP and SILENT=YES, the Max 4000 would send 'connected'.

With the MAX configured to SILENT=YES, no response should have been issued, but the MAX would respond with 'connected' when using 'Immed-raw-tcp'.

TR 1054: Occasional transmit Ethernet silence on MAX4000

When transmitting (only), the MAX would occasionally stop outbound Ethernet transmissions for a short period of time, but would then resume normally.

TR 1055: MAX had a very slow echo response with analog callers

The MAX had a 5- to 10-second delay to echo characters for analog callers. The clock source was not properly updated in all cases when BRI and/or PRI lines were inserted and removed. (In Australia this occurred on BRI lines even when not physically attached.)

TR 1066: ISDN backup problems when Frame Relay circuit was in Yellow Alarm

In some cases, the ISDN backup did not initiate with the reason LAN Security Error. The backup failed to initiate when some (but not all) of the DLCIs in a connection remained up. Now backup monitors for loss of DLCIs. (See New Feature number 1539.)

TR 1073: RADIUS filters on second line not applied when auth is sett to PAP-TOKEN-CHAP

When an MP+ call is made from a P50 to a MAX, the filters defined in RADIUS are applied to the connection, but when a second channel is added, filters are not applied to the second channel.

TR 1074: MAX 4000 (4.6Ai12) could not do CLID and CHAP in the same profile.

When both authentication protocols were used, the user would be assigned to a port, but LAN SESSION UP could not be enabled.

TR 1075: Using Immediate-RLOGIN, the Binary flag was ignored

For RLOGIN, when performing ZMODEM uploads, or during UUCP sessions, the Binary flag was ignored, causing the session to fail.

TR 1078: OSPF routing attributes verified

When the default route was changed to PRIVATE, the default link-state advertisement (LSA) was not removed.

TR 1080: OSPF link state databases would not synchronize

A MAX running OSPF would have trouble synchronizing its link state database. This was caused by a problem with the flooding mechanism and would result in a large numbers of retransmissions.

TR 1085: After synching with Host/BRI, Motorola 220 Terminal Adapter's Ring Indicator stayed on

Using a host BRI card installed on the MAX and slotting channels from the PRI line to supply desktop BRI support, users with a Motorola terminal adapter set to auto answer would experi-

ence locking, and no AT commands could be issued.

TR 1092: Quiesce feature was not available on modems 9-12 on 12-port modem cards

Quiesce functionality and the supporting menus were added for modem slots 9 through 12 on the MAX.

TR 1102: MAX did not listen for PPP after carriage return

The MAX did not respond to PPP data after a carriage return. Since dialup modem scripts can issue one or more CRs before sending PPP data, the MAX was modified so that CRs would not cause calls to be terminated in error.

TR 1103: ESF LMU not functioning properly

The Line Monitoring Unit (LMU) function of Extended Super Frame (ESF) did not return error statistics. The MAX was expecting requests only for DSX.

TR 1115: Duplicate SYSLOG close records were logged in error

Calls on the pending list would be logged 'closed' in error and again on completion of an orderly shutdown.

TR 1119: RADIUS OSPF route removal was not propagated to neighbors

When static routes created by RADIUS were deactivated, they were properly removed from the MAX's routing table, but updates were not issued to neighbors.

TR 1122: LCP negotiations were authenticated by RADIUS, but ended at Terminal Server

Both the attributes User-Service and Framed-Protocol were not sent with PPP authentication, but are now included to support third party RADIUS servers.

TR 1124: Periodically ISDN users could not connect - no HDLC ch. available

After a period of time, ISDN users could not connect because no HDLC channels were available. Rebooting the MAX would clear the problem. It was determined that occasionally an ISDN call's WAN session would fail to completely close when the call terminated and subsequent calls received on the same line would not come up correctly.

TR 1136: MAX sometimes stopped responding to pings and had poor WAN performance.

A problem with buffer usage flags reporting incorrect information caused the MAX to slow down or not respond at all.

TR 1140: 64-character user names not supported in 4.6Bi4

64-character names were rejected improperly due to a change in 4.6Bi4. Now external authentication of names (or passwords) longer than the maximum is attempted via RADIUS.

TR 1143: MAXDial lost connections or was slow when sequence errors were reported by LAN

If ACK packets were dropped between the client side and the MAX, the MAX resent the data

packets, causing the client side to respond with a sequence error notification. Resynchronization problems eventually caused the connection to time out.

TR 1144: No routing to multiple subnets on the same physical wire

Remote sites could not ping subnets on the local Ethernet segment of the MAX other than the subnet assigned to the local MAX. To do this, multiple networks on the same wire are accessed by assigning a second IP address on the second network using the Ethernet/ModConfig/Ether option.

TR 1162: With RADIUS, if User-Service was not specified, the user could not launch a PPP session

When using the RADIUS server, if the value of User_Service was not sent back with the RADIUS response, the user could not initiate a PPP session. Now the value in Framed_Protocol determines the user's service when the value in User_Service is not set or is not available.

TR 1176: Loop-Start with ESF did not comply with AT&T specification as C&D bits did not

mirror A&B The MAX could not run loop start provisioned for ESF/B8ZS. The C&D bits always showed a value of zero. Now, according to the AT&T spec, they mirror the A&B bits.

TR 1185: ASBR and Show OSPF product corrections

The MAX would become an Autonomous System Boundary Router (ASBR) when it was not set to do so. A new submenu, OSPF Global settings, may be set to turn off ASBR.

TR 1194: Previous IPX routes would not go away after bridging enabled

If the MAX was configured to route IPX and IP, then reconfigured to bridge IPX and reset, the routing table for the previous External Ethernet and Pool address was not removed. Resetting the MAX had no effect.

TR 1196: Users entering MAX terminal server got Invalid Auth Realm for banner

The MAX did not properly distinguish between a successful attempt to obtain a banner message and an Access-Reject message. As a result, users saw `Invalid authentication realm' for the initial banner in error.

TR 1057: SNMP - ISDN Billing for 1TR6 not working under 4.6Ai12

A feature added only for German 1TR6 lines to support ISDN billing information was not working as designed, and is corrected in this incremental release.

TR 1070: Australian SPCs not working correctly on Max E1

For the Australian network, Channel Numbers 16-30 are designed to be incremented by one time slot, leaving time slot 16 available for D Channel signaling. An error in the MAX incremented slots 17-30, which resulted in the MAX locking up and requiring a reset in order to restore connectivity. Associated with this problem, D Channel congestion was reported, which prevented calls from being placed until the hardware was reset.

TR 1118: Asynch calls failed on MAX1600 E1 with BRI card

Modem calls into a MAX 1600 E1 (BRI) would fail to connect properly.

TR 1131: MAX4000 E1 reset with no Fatal Error Log if the ConnProfile had no Dial Number

If a MAX with an active Connection Profile, a valid IP address, but no Dial Number, was pinged by another device, it would attempt to dial and fail multiple time. Finally it would reset with no Fatal Error logged.