MAX T1/PRI 5.0A Release Note

Number 4 **February 4, 1997**

This release note describes the new features and product corrections included in Ascend software release 5.0A. Use this release note in conjunction with your MAX T1/PRI documentation. To use this release note, follow these steps:

1. Read through the next section "What is in this release?" to determine which new features and product corrections apply to your environment.
2. Obtain the 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) 272-3634
   - Outside the United States, call (800) 697-4772
   - 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." Then configure the features that apply to you by reading the appropriate sections listed below.

What is in this release?

The following new features are included in this release:

Larger executable load images ("fat loads") enabled 11

A new system for loading larger system executables enables you to use tloadcode and TFTP from the debug monitor. Previously the redundant system images stored in the "top" and "bottom" halves of flash memory did not permit system loads larger than 960 KB for the MAX (or 448 KB for the Pipelines).

New Telnet password verification failure trap 14

This feature adds the IP address of the Telnet client to the existing security violation message indicating the maximum number of Telnet login attempts to a MAX has been exceeded.

Monitoring the modem status in the VT100 interface 15

This feature enables you to display and monitor the status of each individual modem on an 8-modem card and a 12-modem card.

Called number authentication supported. 16

This feature adds authentication by Called Number. It is similar to authentication by Caller ID (CLID), but uses the number (ID) of the unit being called instead of the number of the calling unit.

ATMP support for hostnames, secondary home agents 18

The ATMP foreign agent uses the home agent's IP address to set up the ATMP tunnel. Consequently, if the home agent is down, the foreign agent fails to set up the tunnel, thereby terminating the end user's session. Previously, you could configure only a single ATMP home agent in the RADIUS user profile. Now, you can configure a secondary home agent for use if the primary home agent is unavailable. In addition, you can specify the home agent using a symbolic hostname or an IP address in dotted decimal notation; in the past, only an IP address in dotted decimal notation was permitted.

New RADIUS server attribute identifying user session 20

A new RADIUS server attribute has been added that allows a RADIUS client to perform certain operations to an active session (for example, to disconnect a session or change a session's filters) by allowing the Ascend unit to match the operation request to the user session. The attribute, Ascend-Session-Svr-Key, is part of a RADIUS message initiated by a RADIUS client and sent to the Ascend unit. In addition, an option has been added to the Ethernet>Mod Config>RADIUS Server menu to allow a user to specify which attributes will be used.

Allow remote authentication before local 22

An option has been added to the Ethernet>Mod Config>Auth menu that allows you to use local authentication before or after remote authentication with a RADIUS or other authentication server. This feature allows local authentication, but allows authentication to work even if the remote authentication server is down.

Multilink or MP+ call now can span multiple MAX units 24

Multiple MAX units can now be configured to form a Stack, or group of MAX units, that allows a Multilink PPP (MP) or MP+ call to span the MAX units in the Stack.

DHCP Server function over bridged connection added 26

DHCP server functionality has been added to the MAX for remote clients that are connected to the MAX over a bridged WAN connection. This feature allows a MAX to assign a dynamic IP address to a remote DHCP client. You configure and enable the feature on the RADIUS server connected to the MAX.

Network Address Translation (NAT) for a LAN. 28

Network Address Translation for a LAN allows the Pipeline to connect a LAN to another network even if the devices on the LAN do not have valid addresses for the remote network. The Pipeline will translate between LAN and remote network addresses.

NET3 PTP signaling support added 31

NET3 point-to-point (PTP) signaling support has been added to all Ascend platforms that support BRI. NET3 PTP signaling is a variation of standard EURO-ISDN signaling used in Germany. It uses a fixed TEI, as opposed to a TEI assigned by the network.

TACACS+ support 32

This release adds support for TACACS+ authentication, authorization, and accounting on all platforms that currently support RADIUS accounting. TACACS+ *(Terminal Access Concentrator Access Control Server Plus)* is a server from Cisco Systems, Inc.

Updates to the immediate modem feature 38

Immediate modem service now has its own password protection and has been modified to support binary downloads.

RADIUS accounting statistics sent to choice of servers 39

A feature allowing a connection profile to specify RADIUS accounting servers has been added to allow connection accounting on a per-user basis. Accounting information is sent to the server specified in the connection profile.

RADIUS static routes can be stacked in OSPF 43

You can now stack static routes and specify that a temporary static route advertised for a RADIUS user override the normal static route advertised when the user isn't logged in .

MAXDial control panel added for WIN95 43

What was changed: This feature installs a new application named MAXDial in the Control Panel window on your Windows 95 desktop. You can use the MAXDial control panel to assign MAXs to the computer's serial ports or remove previous such assignments.

Network summaries for address pools 46

Summarizing host routes to reduce routing table overhead. IP addresses assigned dynamically from a pool are added to the routing table as individual host routes. You can now summarize this network (the entire pool), cutting down significantly on route flappage and the size of routing table advertisements.

Password implemented for immediate modem feature 49

A new password has been added that separately controls access to the immediate modem feature. Previously, the Telnet password controlled access to the immediate modem feature as well as to Telnet.

RADIUS accounting coldstart notification 50

A new packet type and two new attributes have been added that allow an Ascend Network Access Server (NAS) to notify the RADIUS accounting server when the NAS comes up. The packet is analogous to the SNMP coldstart trap.

OSPF Equal-cost Multipath routing available 52

Now, a MAX running OSPF alternates between two equal cost gateways. Previously, it only used the first gateway.

Defender authentication added 53

An Ascend unit can now authenticate users by directly contacting a Digital Pathways Defender authentication server.

SecurID ACE authentication support added 55

An Ascend unit can now authenticate users by directly contacting a SecurID ACE server.

DNIS enables TCP between MAX units 59

Enhanced DNIS support enables ISPs to receive TCP connections instead of switched calls.

Terminal server access using the X.75 protocol 61

Now, you can access the terminal server using the X.75 protocol. Full technical specifications for X.75 can be found in the CCITT Blue Book Recommendation X series 1988.

RADIUS IP Address Allocation 62

The RADIUS daemon is a database server that provides user profiles to MAX products. The RADIUS database can specify pools of IP addresses that a MAX can use to dynamically allocate IP addresses to incoming callers. Formerly, dynamic IP address allocation to callers was handled by each MAX individually, from a pool of addresses pre-assigned to each MAX. This new feature allows MAX units to allocate IP addresses to callers from a global pool of addresses that is shared among many units.

X.25 support for reverse charge request 65

This new feature enables you to configure a Connection Profile to request reverse charge through the X.25 facility field. This feature is provided for situations in which you do not wish the user to type the request reverse charge string at the PAD prompt, or in which the user is in immediate PAD mode and therefore cannot type the string.

Show system version command added 65

A show revision command has been added to the terminal server command line options for the show command.

Additional information for system resets now provided 66

The fatal error log now details the reason for a system reset and no longer describes a reset as a fatal error. Normal OSPF exits (those due to OSPF not being configured) are no longer entered in the fatal error log.

CLID authentication can return User Busy 67

You can now configure CLID authentication failures to return User Busy. Two different conditions can be returned in the DISCONNECT message.

Expect callback parameter added to dialout profile 161

A parameter has been added to the Telco options submenu of the Connections menu for configuring an Ascend MAX or to expect a callback from the machine called. This prevents problems that arise when CLID is set to Required on the machine that is expected to callback.

User-defined message for assigned IP address 69

A field has been added to the Ethernet>Mod Config>TServ submenu that allows you to define a message that indicates the IP address the terminal server has assigned. This message appears when a you select PPP from the terminal server prompt, or any time a PPP connection is made from the terminal server.

Debug command to change MAX modem strings 70

This feature adds a debug command that allows administrator's to change the AT command strings on the MAX digital modems.

Ascend Session Events sent in RADIUS-LOGOUT mode 71

Ascend units can now report the number of sessions by Class to a RADIUS authentication server using RADIUS -LOGOUT. Previously, this report could only be sent to a RADIUS accounting server using RADIUS-ACCOUNTING.

Define RIP-v2 values in RADIUS dictionary 75

The RADIUS daemon is a database server that provides user profiles to MAX products. RADIUS uses the Framed-Routing attribute to indicate whether the user sends RIP (Routing Information Protocol) packets, receives RIP packets, or both. Formerly, only the RIP version 1 values were specified; this release adds the RIP version 2 settings for the attribute.

DNS list size increased 75

You can now allow up to 35 DNS list addresses. The number of DNS addresses listed for terminal server logins was previously limited to six. You can now configure a number of addresses up to 35, which is the maximum supported by BSD.

Flexible RADIUS user pools. 76

Currently, you can set up RADIUS to pick the IP address space pool that assigns the address space for each user. More flexible pools allow users to set RADIUS so a user is assigned an address from any of the pools that have space. This new feature will allow an ISP to create a flexible pool space that allows them to use all 72 modems in the MAX. Without this feature an ISP has to either propagate a host route to some point inside their network or use a 128 block for the subnet.

Terminal server login timeout added. 76

This feature adds options for configuring the timeout value for inactivity at a login prompt. Previously the MAX waited five minutes before disconnecting the call.

Profile- or User-level DNS servers 77

IP address for the Domain name servers can now be set for an individual Ascend client in the IP Connection profile. Previously, the two DNS server addresses that were configured on the MAX were given to all users during IPCP negotiation.

Fixed interfaces appear first in SNMP IfTable 79

Fixed interfaces, such as ports or lines on the motherboard, now appear at the top of the SNMP IfTable before software entities. Previously, fixed interfaces appeared below software interfaces in the IfTable.

Terminal server and diagnostic functions 81

Termsrv and Diagnostics options have been added to the Do menu. Previously, these functions could be not be accessed through the menu interface.

Support for OSPF in MIB II 82

Ascend MAX products that support OSPF now support SNMP MIB II support for OSPF (Group 13). For more information refer to RFC 1253. OSPF support for MIB II does not include SNMP SET of OSPF tables or virtual interfaces for point-to-point links without an IP address.

OSPF can advertise a static route 82

An automatic feature has been added that allows a MAX running OSPF to advertise routes on behalf of another gateway (a “third-party”).

Debug option to display unwanted dial-outs packets 83

Display packets as an aid to writing filters. A new debug option captures and displays packets that cause the Ascend unit to dial out when a connection is not needed. You can then get the information you need to write a filter that prevents the packet from bringing up a connection.

Add template feature in Name/Passwords profile 87

This feature adds a new parameter that allows you to specify which Connection Profile to use as a template. Previously, the Name/Password profiles always used the Answer Profile as a template.

Connection Profile call time limit 88

You can now specify the maximum duration of an incoming call. Previously there was no limit on an incoming call duration.

Increase dial-out digits to 24 88

The number of dial-out digits was increased to 24.

BACP support over MP added 89

Support for Bandwidth Allocation Control Protocol (BACP) has been added.BACP is the Internet standard equivalent to Ascend Multilink Protocol Plus (MP+). All platforms that support MP+ will also support BACP.

MS-CHAP support 90

Support for the Microsoft - Challenge Handshake Authentication Protocol (MS-CHAP) format supported by Windows NT systems has been added to all Ascend platforms except the Pipeline 25.

Special handling for packetizing data from modems 91

We can now provide a way to control the manner in which we packetize data received from our modems. The data can be accumulated for a maximum number of milliseconds or a minimum number of bytes before being passed up to the encapsulation layer. Two new parameters have been implemented to facilitate this feature.

Multicast tree monitoring added 92

This feature adds a mechanism that allows the MAX to monitor whether it is able to receive multicast packets at its Internet interface. It also provides quick feedback to network operations if the MAX fails to receive regularly scheduled multicast traffic (“heartbeat” packets) on a specified multicast group address.

Auth TS Secure added 95

This feature enables you to configure the MAX using RADIUS authentication to accept a remote dial-in call to the terminal server or to drop the call if a Login-Host was not specified in the RADIUS users file. Previously, the MAX always dropped the call if no Login-Host was specified.

MAX authentication of calls via serial AIM ports 96

You can now specify a password for calls placed across the Host serial imux ports. Previously, all such calls did not undergo any form of authentication.

Name/Password profile includes terminal server users 97

Name/Password profiles are now recognized for terminal server authentication. Previously this profile was recognized only by PPP authentication.

Address expansion of RADIUS Server Clients list 98

The client address list has been expanded to support a range of addresses instead of a single client IP address. Previously, a maximum of three clients with one common secret key was supported. Previously, a maximum of three clients with one common secret is supported.

Forward multicast trace packets 101

This feature allows multicast clients to MTRACE (multicast trace) the path taken by multicast traffic. The MAX can now pass IGMP MTRACE packets from multicast clients to Mbone and MTRACE RESPONSE packets back to clients from MBone. Previously, a MAX user or other MBONE router user could not use MTRACE on multicast connections to Pipelines.

DBA RADIUS attribute names changed 101

This change gives the values used by the Ascend-DBA-Monitor attribute a set of unique names based upon the attribute name to eliminate any conflicts. Previously, a conflict in the RADIUS value None caused the Framed-Routing attribute, when configured as None, to use the value of 2, which means Listen, instead of zero when sending profile information to the MAX.

Checksum validation and redownload for 12MOD. 102

*T*he MAX now downloads the 12MOD modem code, waits for the modems to checksum the downloaded code, and then verifies the checksum matches before continuing with AT POST. Previously, the MAX downloaded the modem code and immediately commence with AT POST. This feature will help to reduce the POST failure rates for the MOD12 cards.

Specifying default routes on a per-user basis 102

You can now specify a default route on a per-user basis in a Connection Profile or a RADIUS user profile. If an operator is using a particular service, you can cause the Ascend unit to send traffic to the router that service uses, even if the router is not the default gateway shown in the system-wide routing table.

MAXDial support for Microsoft Fax added 104

Support for Microsoft Fax has been added to MAXDial with this release. Previously, there was no way to set Microsoft Fax to use hardware flow control (which was required). This release includes utilities to allow the use of Microsoft Fax with MAXDial.

Multi-line terminal server prompt 105

You can now configure a terminal server prompt of up to 80 characters and consisting of more than one line. Previously, the prompt could only consist of one line and was limited to 15 characters.

Two DNS domains configurable 107

You can now specify a second domain name server to be searched when making a connection that looks for a DNS host. Previously, you could specify only one domain name server.

Configurable source port for remote authentication and accounting 108

You can now specify the source port used to send remote authentication requests for all external authentication services the MAX supports, including RADIUS, TACACS, and Defender. You can also specify the source port used to send RADIUS or TACACS+ accounting requests. This new feature meets the needs of those users needing to specify the source port for various uses, including filtering.

Modification of RADIUS messages during MAX boot up 109

When RADIUS requests the release of RADIUS-allocated IP addresses, a timeout can occur. Formerly, the timeout was reported with a null user name. Now, the user name consists of a text string.

New maximum lengths for login and password prompts 109

In this release, the Login Prompt and Password Prompt parameters now allow you to specify a greater number of characters. This feature was implemented to accommodate existing user scripts.

Ascend X.25 PAD now sends no banner message 110

This feature sets the terminal server to display no banner when a terminal connects to the MAX over X.25. Previously, when a terminal connected to the MAX, the terminal received the banner message Ascend PAD.

Rate Limit default changed for receiving multicast packets 110

The default rate limit for multicast/Mbone packets has been increased to 100 seconds, which prevents the MAX from accepting packets from multicast clients. This change reverses effect of the previous default, 5 seconds, a fairly short interval that could result in excessive multicast traffic for some networks.

Terminal server kill command. 111

The new terminal server kill command enables you to disconnect a user who establishes a connection with the Ascend unit via Telnet. You can disconnect the user by session ID. The disconnect code that results is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects.

Per-user control and accounting for immediate modem and MAXDial 112

This feature adds per-user control of users accessing the MAX unit's modems through immediate modem or MAXDial. This feature also adds accounting to keep track of the calls made through immediate modem or MAXDial.

Call charge and call status for U.S. ISDN PRI lines 116

This feature allows SNMP managers to monitor Ascend units call charges and call status for U.S. ISDN PRI lines.

New RADIUS attribute for controlling service. 118

For RADIUS-authenticated clients, you can now use the type of connection (ISDN or modem) to prevent them from using a capability to which they have not subscribed.

Separate modem-user and digital-user profiles 119

This feature allows users dialing into a MAX authenticating with in SecurID ACE direct mode to specify one of the MAX unit's local profiles to be used for session parameters. The previous implementation of SecurID ACE always used the RADIUS default profile for all users who authenticated with a SecurID token card. It also enables an optional Lan Address setting to override the Lan Address in the specified profile (or in the default profile, if no specific profile is given). This feature also enables you to specify different profiles/addresses for each user, based on whether the user has dialed in with a modem (analog call) or ISDN (digital call). This means a single token card can be used for authenticating from two different remote setups (for example, a Pipeline 50 + desktop at home or a laptop and modem while travelling). This feature also changes slightly the way that quotations are done for password (rp) strings given in the ACE server shell strings.

Add PAP-TOKEN-CHAP to ACE authentication. 123

This feature enables user dialing into a MAX authenticating with direct SecurID ACE to bring up additional channels without the repeating the interaction required for the first token authentication .

Host BRI U-Interface slot card offered 124

The Host/BRI slot card for the MAX is now available with a U interface. The card functions identically to the BRI S-Interface slot card previously available.

SNMP callStatusType field added to callStatus table 134

This new SNMP feature enables you to differentiate incoming calls from outgoing calls.

New lanModemGroup in the Ascend Enterprise MIB 134

This new feature enables you to monitor the digital modem usage for analog calls. The disabled modem list subgroup is available only on MAX units with digital modems and a T1 network interface.

X. 25 Auto-call parameter name and field changed 141

The name of the Immed X.121 Addr field in the Encaps submenu of the PAD Connection Profile has been changed to Auto-Call X.121 field. The size of this field has been enlarged to permit 48 characters to be entered. Previously, this field allowed a maximum of 15 characters. The larger field permits inclusion of Call User Data in the Auto Call X.121 Addr field, a feature required by some hosts.

New trap for suspect modems 142

A new SNMP trap is generated when a modem moves to the suspect list. Ascend units create a "suspect" list for digital modems based on failed connection attempts and other factors. In this release, SNMP trap is generated and sent to the alarm filter group when a modem is placed on the suspect list.

Terminal server show users command added 143

A terminal server command has been added that displays a list of user sessions active on a system. Each user session is identified by the sessionID, with additional information about the session. The show users command has also been added to the online help for the show command.

Controlling whether RADIUS attributes 6 and 7 are sent. 145

You can now specify whether Ascend units send values for RADIUS attributes 6 and 7.

Optional prompt before authentication 145

An extra prompt has been added to the terminal server dialog before authentication that allows the Ascend unit's terminal server to mimic another terminal server's login sequence.

SNMP variables for tracking load and capacity 147

SNMP eventGroup fields have been added to keep track of totals relating to call and session events. Version 2.0 of the Ascend Enterprise MIB includes new eventGroup fields that record statistics about the total numbers of calls and sessions.

MPP should drop newest B channel first 150

The order in which MPP drops channels when bandwidth is decreased has changed.

Super-Call-ID for billing of multi-channel calls. 150

The SNMP Super-Call-ID feature keeps track of the calls associated with a multi-channel MP or MP+ session.Version 2.0 of the Ascend Enterprise MIB includes a new eventTable object that enables customers to use SNMP records to bill multi-channel sessions. This feature was available previously only in the RADIUS Accounting End Reco.

Modem transmit level can now be set 151

This feature allows users to modify the transmit level through Rockwell modem code.

10 modem pools configurable from WAN Options menu. 151

The number of static address pools you can configure from the WAN options submenu of the Ethernet Configuration Profile has been increased to a maximum of 10 pools. Previously, you could configure a maximum of two pools.

Enhanced RADIUS support for bridging connections 153

RADIUS-specified dialout connections can now be brought up based on ARP requests.An earlier software release enabled RADIUS configuration of bridging table entries. However, only a resident Connection profile could bring up the required connection. In this release, the Ascend unit can download a RADIUS profile to bring up the required connection.

Busy modem list added to SNMP 154

A sub-group that lists the modems currently being used for outgoing or incoming calls has been added to the Ascend MIB. This feature enables you to automate service management, including modem maintenance, to scale service and add capacity.

Active sessions indexed by session ID 157

This feature allows the MAX to determine whether more than one user is connected using the same user profile.

Additional features not in the user documentation 161

Problems corrected in this release 164

Upgrading system software 172

Larger executable load images (“fat loads”) enabled

A new system for loading larger system executables enables you to use tloadcode and TFTP from the debug monitor. Previously the redundant system images stored in the "top" and "bottom" halves of flash memory did not permit system loads larger than 960 KB for the MAX (or 448 KB for the Pipelines).

Loading a “fat” system executable

“Fat” loads are loads whose compressed size exceeds 960 KB for the MAX or 448 KB for the Pipeline. These system loads require special procedures for downloading into the Ascend unit.

Downloading a fat load

A fat system load can only be downloaded via tloadcode (TFTP) from the debug monitor. Fat loads cannot be downloaded via the console port.

An older system image that is less than the maximum 960 KB or 448 KB will still load in the same manner as previously. These loads are referred to as “thin” loads.

If your unit currently is using a thin load system version that is not “fat load aware,” you will first need to upgrade your current thin system to make it fat load aware. This thin system should be backed up in case of fat load failure. See Loading a thin system that is fat load aware in this note.

To load a fat load aware system executable using TFTP:

1 From the MAX Telnet interface, access the debug monitor by typing these characters in rapid succession:

`Esc [ Esc = (or Control "d", then select "D-diag")`

2 At the > prompt, type:

`tloadcode hostname filename`

where hostname is the name or IP address of your TFTP server, and filename is the name of the system software on the server.

For example, the command:

```
tloadcode tftp-server ascend.bin
```

will load a software ascend.bin into flash from the machine named tftp-server. The current configuration is also saved to flash before new code is received, as a precaution.

3 One of the following messages appears:

The following message is displayed at the default rate of 9600 bps if the load is thin:

```
UART initialized
thin load: inflate
.....................................................
starting system...
```

The following message appears at the default rate of 9600 bps if the load is fat:

```
UART initialized
fat load: inflate
.....................................................
starting system...
```

This completes code load if you have no errors.

Loading a thin system that is fat load aware

If a fat load has a CRC (cyclic redundancy check) error, the following message appears:

```
UART initialized
fat load: bad CRC!!
forcing serial download at 57600 bps
please download a "thin" system...
```

Immediately after this message appears, the serial console speed is switched to 57600 bps, and control is transferred to the boot ROM's Xmodem serial download routine. To recover from this error and load the fat system, you must load a thin system that is fat system aware. This thin load is required here because the boot ROM knows nothing about the new fat load format and only supports the traditional thin load. This thin load is probably not the system you will actually run, but it must be loaded first as a stepping stone toward downloading the desired fat system over the ethernet via tloadcode.

1 Invoke your Xmodem software to load the thin load through the console port.

2 Start the download of a thin load using the tloadcode command.

```
>>>> tloadcode:
```

The output of tloadcode has been modified slightly. When you download a traditional thin load, the following appears on the debug monitor screen:

```
> tload yourmachinename /loads/mhpt1.bin
saving config to flash
.....................................
.
loading code from 192.168.1.82:69
file /loads/mhpt1.bin...
thin load:
```

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

The change is the addition of the line “thin load” between the mention of the file name and the long series of dots.

3 After you have finished loading the fat aware thin load, reboot the unit.

4 Download the fat load using the tloadcode command.

When you download a fat load, the following appears on the debug monitor screen:

```
> tload yourmachinename /loads/mhpt1bri.bin
saving config to flash
.....................................
loading code from 192.168.1.82:69
file /loads/mhpt1bri.bin...
fat load part 1:
.....................................................................
............
fat load part 2:
.............................................
```

Note the “fat load part *x*:” messages. They notify you when the first and second halves of the fat load are being loaded.

Note: In certain rare circumstances, a customer might possess a fat load from an engineering release written in an older format. tloadcode will automatically detect the obsolete format and refuse to load it, displaying the following:

```
> tload squiddly /loads/mhpt1bri-moldy.bin
saving config to flash
.....................................
loading code from 192.168.1.82:69
file /ascend/mb4/rtr/mhpt1bri/mhpt1bri-fatty.bin...
obsolete fat load format--discarding downloaded data...
-----------------------------------------------------------------
```

Future unsupported loads

In the future, if you attempt to load a system that does not use the fat load format introduced by this feature, the load will be rejected if your current system does not support the new format.

```
> tload yourmachinename /loads/mhpt1bri-moldy.bin
saving config to flash
.....................................
loading code from 192.168.1.82:69
file /ascend/mb4/rtr/mhpt1bri/mhpt1bri-fatty.bin...
incompatible fat load format--discarding downloaded data
```

New Telnet password verification failure trap

This feature adds the IP address of the Telnet client to the existing security violation message indicating the maximum number of Telnet login attempts to a MAX has been exceeded.

How the trap has been modified

To Telnet into a MAX, a user must supply the appropriate password, which is then verified. If the user cannot supply the correct password, an SNMP trap message is sent to all SNMP clients enabled for SNMP security messages.

The message includes

- the session number for the attempted Telnet session
- the IP address of the host (the MAX)
- the associated IP address of the Telnet client that attempted the connection

in the following format:

```
mmm.mmm.mmm.mmm  Enterprise Specific Trap (15) Uptime: xx:xx:xx
Name.iso.org.dod.internet.private.enterprises.ascend.sessionStatus-
Group.
IpAddress: ttt.ttt.ttt.ttt
sessionStatusTable.sessionStatusEntry.ssnStatusUserIPAddress%d
```

where:

mmm.mmm.mmm.mmm	=	Host's IP address
ttt.ttt.ttt.ttt	=	Telnet client's IP address
%d	=	attempted Telnet session number

This trap message already existed in the listing of traps as an authentication failure (RFC-1215 trap-type 4). An authenticationFailure trap signifies that the MAX sending the trap is the addressee of a protocol message that is not properly authenticated. The only change to the trap is the addition of the IP address of the station that failed authentication.

The trap is documented in the Ascend trap listing as:

```
-- maxTelnetAttempts trap returns the objectID of the session entry
-- and the associated IP address

   maxTelnetAttemptsTRAP-TYPE
        ENTERPRISEascend
        VARIABLES { IpAddress }
        DESCRIPTION "The maximum number of login attempts for a telne
                session has been exceeded."
        ::= 15
```

Monitoring the modem status in the VT100 interface

This feature enables you to display and monitor the status of each individual modem on an 8-modem card and a 12-modem card.

User interface changes

The Main Status Menu now contains a V.34 Modem entry for each modem card. When you select the V.34 Modem entry for a card, the Modem Status menu displays. On this menu, each modem is correlated with a display character. An example Modem Stats window for an 8 modem card is shown in Figure 1.

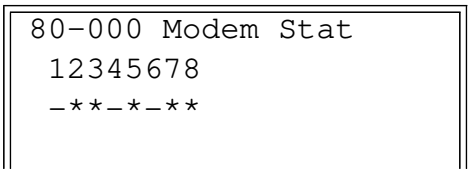


Figure 1. Example Modem Stats window

The display characters and their corresponding meanings are listed in Table 1.

Table 1. Modem status characters

Character	Description
.	This modem is non-existent.
f	This modem failed the POST (Power-On Self Test). The modem is unavailable for use.
-	The modem is not in use.
a	The modem has been instructed to dial or answer a call, and the unit is waiting for RLSD (Received Line Signal Detector) to go active.
A	RLSD has already gone active and the unit is waiting for result codes to be decoded. This state is entered only if RLSD precedes the codes.
*	A call is connected, and the unit is monitoring RLSD.
i	The modem is re-initializing after being reset.
q	The modem is re-initializing after being reset and an open request is waiting to be processed when re-initialization completes.
Q	The modem is re-initializing after being reset and an open request for Virtual Connection is waiting to be processed when re-initialization completes.

Character	Description
d	The first part of the dial string has been sent. This unit is pausing for the modem to read and process the second part before sending it.
v	A virtual connection session is active on modem. No call is active yet.
o	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls.
O	The user has disabled the modem from the MAX configuration interface. The modem is unavailable for calls and a B-channel is set to OutOfService.

Called number authentication supported

This feature adds authentication by Called Number. It is similar to authentication by Caller ID (CLID), but uses the number (ID) of the unit being called instead of the number of the calling unit.

Configuring Called Number Authentication

To support configuration for Called Number Authentication, the following changes have been made:

Profile	Description of change
Connection Profile	A new field, Called #, has been added. In many cases Called # will be the same as Dial #, but without the trunk group or dialing prefix prepended.
Answer Profile	Clid Auth= is changed to Id Auth=. There are several new options for this field. See Table 2 for descriptions of these new options, as well as the options previously available for Clid Auth.

Table 2. Id Auth parameter settings

Setting	Description of change
Ignore	Neither CLID (calling party number) nor DNIS (called number) affect incoming call authentication; that is, both are ignored.
Prefer	No change

Table 2. Id Auth parameter settings

Setting	Description of change
Require	No change
Fallback	No change
Called Require	Functions identically to "Require" above except the called number is checked rather than the calling party number.
Called Prefer	Functions identically to "Prefer" above except the called number is checked rather than the calling party number.

RADIUS changes

Client-Port-DNIS (attribute 30) is the field that implements Called Number authentication. The profile parameter in the user interface menu refers to the Called Number as Called #, and in the RADIUS users file it is Client-Port-DNIS.

Note: In the latest RADIUS IETF draft, this attribute is named Called-Station-Id. The draft states that it can be the DNIS and it may be different from the phone number the call comes in on.

A RADIUS entry for Called Number authentication must have the number being called in the first column and Password="Ascend-DNIS" on the first line. In the example shown below, User-Service=Dialout-Framed-User on the first line ensures that the profile will not be used for an incoming call with the name "1234" and the password "Ascend-DNIS."

RADIUS Examples

In the following examples, all authentication takes place through RADIUS.

Id Auth = Required

The parameter IP Auth has been set to Required. Two user profiles for this single user have been set up, one with the called number ID (set to 1234) and one with name/password (clara-p50/ascend). This two-step authentication first checks the called number ID and does not answer if it does not match. Next, it answers the call and checks name and password:

```
1234 Password = "Ascend-DNIS" User-Service = Dialout-Framed-
User
   Ascend-Require-Auth = Require-Auth


clara-p50   Password="ascend"
   User-Service = Framed-User,
   Framed-Protocol = MPP,
   Framed-Address = 192.10.11.12,
```

```
   Framed-Netmask = 255.255.255.248
```

Note that incoming calls are answered only when the called number ID matches, saving the time and expense of handling an invalid call. In the next example, Id Auth = Prefer, incoming calls are answered whether or not the called number ID matches, even though both examples have exactly the same authentication requirements.

Id Auth = Prefer

The parameter IP Auth has been set to Prefer. Authentication takes place in a single step where the called number ID is checked in combination with name/password authentication. Although this configuration uses the same criteria for authentication as the one above, it uses only a single user profile in RADIUS and is therefore simpler to configure and maintain.

```
clara-p50   Password="ascend", Client-Port-DNIS = 1234
   User-Service = Framed-User,
   Framed-Protocol = MPP,
   Framed-Address = 192.10.11.12,
   Framed-Netmask = 255.255.255.248
```

Ascend-Require-Auth

Prior to this feature, the Ascend-Require-Auth attribute (201) was used to indicate when name/password authentication was required after calling party ID (CLID) authentication. Now Ascend-Require-Auth can also indicate when name/password authentication is required after called number (DNIS) authentication as in the first example.

ATMP support for hostnames, secondary home agents

The ATMP foreign agent uses the home agent's IP address to set up the ATMP tunnel. Consequently, if the home agent is down, the foreign agent fails to set up the tunnel, thereby terminating the end user's session. Previously, you could configure only a single ATMP home agent in the RADIUS user profile. Now, you can configure a secondary home agent for use if the primary home agent is unavailable. In addition, you can specify the home agent using a symbolic hostname or an IP address in dotted decimal notation; in the past, only an IP address in dotted decimal notation was permitted.

New RADIUS attributes

Two new RADIUS attributes enable you to specify a primary home agent and a secondary home agent.

Ascend-Primary-Home-Agent

Description: This attribute specifies the first home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.

Usage: Specify the primary home agent using this syntax:

Ascend-Primary-Home-Agent="<hostname> | <ip_address> [:<udp_port>]"

- The <hostname> argument indicates the home agent's symbolic hostname.

- The <ip_address> argument indicates the home agent's IP address in dotted decimal notation.

  Specify an IP address if a DNS server is not set up for the home agent. You can specify a hostname or an IP address, but not both.
- The optional <udp_port> argument indicates the UDP port on which the foreign agent communicates with the home agent.

  The default value is 5150.
- The colon (:) separates the hostname or IP address from the UDP port specification.

Example: To specify the home agent max1.home.com at IP address 10.0.0.1, and indicate that the foreign agent should use UDP port 6001, specify one of these lines in the RADIUS user profile:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"
```

```
Ascend-Primary-Home-Agent="10.0.0.1:6001"
```

Dependencies: Keep this additional information in mind:

- If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Ascend-Primary-Home-Agent attribute, you need not specify a value for <udp_port>.

  By the same token, if you specify a value for the <udp_port> argument of Ascend-Secondary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.
- Use Ascend-Primary-Home-Agent in place of the Ascend-Home-Agent-IP-Addr attribute.
- To specify a secondary home agent for use if the primary home agent is unavailable, use the Ascend-Secondary-Home-Agent attribute.

See Also: Ascend-Home-Agent-UDP-Port, Ascend-Secondary-Home-Agent

Ascend-Secondary-Home-Agent

Description: This attribute specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. The attribute also indicates the UDP port the foreign agent uses for the link.

Usage: Specify the secondary home agent using this syntax:

```
Ascend-Secondary-Home-Agent="<hostname> | <ip_address> [:<udp_port>]"
```

- The <hostname> argument indicates the home agent's symbolic hostname.
- The <ip_address> argument indicates the home agent's IP address in dotted decimal notation.

  Specify an IP address if a DNS server is not set up for the home agent. You can specify a hostname or an IP address, but not both.
- The optional <udp_port> argument indicates the UDP port on which the foreign agent communicates with the home agent.

  The default value is 5150.
- The colon (:) separates the hostname or IP address from the UDP port specification.

Example: To specify max2.home.com at IP address 10.0.0.2 as the secondary home agent, and indicate that the foreign agent should use UDP port 6002, specify one of these lines in the RADIUS user profile:

```
Ascend-Secondary-Home-Agent="max2.home.com:6002"
```

```
Ascend-Secondary-Home-Agent="10.0.0.2:6002"
```

To specify a primary home agent and a secondary home agent, enter these lines in the RADIUS user profile:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"
Ascend-Secondary-Home-Agent="max2.home.com:6002"
```

The foreign agent first tries max1.home.com on UDP port 6001. If the name cannot be resolved, or if max1.home.com does not respond, the foreign agent then tries max2.home.com on UDP port 6002.

Dependencies: If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Ascend-Secondary-Home-Agent attribute, you need not specify a value for <udp_port>. By the same token, if you specify a value for the <udp_port> argument of Ascend-Secondary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: Ascend-Home-Agent-UDP-Port, Ascend-Primary-Home-Agent

New RADIUS server attribute identifying user session

A new RADIUS server attribute has been added that allows a RADIUS client to perform certain operations to an active session (for example, to disconnect a session or change a session's filters) by allowing the Ascend unit to match the operation request to the user session. The attribute, Ascend-Session-Svr-Key, is part of a RADIUS message initiated by a RADIUS client and sent to the Ascend unit. In addition, an option has been added to the Ethernet>Mod Config>RADIUS Server menu to allow a user to specify which attributes will be used.

Enabling the Session Key

You enable the Session Key attribute in the Ethernet>Mod Config>RADIUS Server menu. When the Session Key is enabled, all new session entries are assigned a session key

To enable the Session Key attribute:

1 Open the Ethernet>Mod Config>RADIUS Server menu.

```
40-A00 Mod Config...
 RADIUS server...
  Server=Yes
  Client #1=255.255.255.255
  Client #2=0.0.0.0
  Client #3=0.0.0.0
  Server Port=1700
  Server Key=
  Session Key=Yes
  Attributes=Any
```

2 Set Server=Yes.

3 Set Session Key=Yes
Session keys will only be assigned if this attribute is set to Yes. The default is No.

Set the Attributes required for identification of a session. The available options are Any, Session, and All. Table 3 describes how each option works when Ascend-Session-Svr-Key is used.

Table 3. Options for specifying attributes in session key identification

Attributes Option	Description
Any	Any Attribute can be used to identify the session. If multiple attributes are sent, the order in which they are checked is: **1** session key **2** session id **3** user name **4** IP address. **Note:** Any is the default.
Session	Only the Session Key is used for identification. If you select Yes for the Session attribute and the Session Key attribute is not enabled, an error message is displayed. This option is not available if Server=No. The default for the Session attribute is No.
All	All Attributes that are applicable must be present and pass validation before any operation is performed on the connection. This option is N/A when Session Key=No. For example, if a session has a user name, IP address, session id and session key, than all four attributes must be sent. As another example, if a session has a user name, session id and session key, than these attributes must be sent; the IP address is not required.

RADIUS attribute added

A new attribute, Ascend-Session-Svr-Key, has been added to the RADIUS dictionary.

Ascend-Session-Svr-Key

Description: When the session key option is set to Yes, Ascend-Session-Svr-Key is included as part of the RADIUS Accounting-Start packet sent by the RADIUS server when a session starts.

Usage: Figure 2 shows the structure for Ascend-Session-Svr-Key. Table 4 shows the values of the fields in Ascend-Session-Svr-Key.

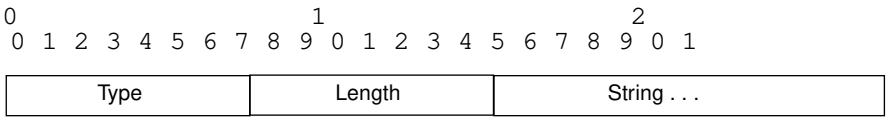


Figure 2. Ascend-Session-Svr-Key attribute structure

Table 4. Ascend-Session-Svr-Key field values

Field	Value
Type	151
Length	18
String	Composed of 16 octets.

For example, an Accounting packet might have the following attributes:

User-Name(1)
NAS-Identifier(4)
NAS-Port (5)
Acct-Status-Type (40)
Acct-Delay-Time (41)
Acct-Session-Id (44)
Acct-Authentic (45)
Framed-Protocol (7)
Framed-Address (8)
Ascend-Session-Svr-Key (151)(only when Session Key=Yes)

Allow remote authentication before local

An option has been added to the Ethernet>Mod Config>Auth menu that allows you to use local authentication before or after remote authentication with a RADIUS or other authentication server. This feature allows local authentication, but allows authentication to work even if the remote authentication server is down.

How it works

Previously, the order of authentication was always:

local connection profiles>simple name/password>remote

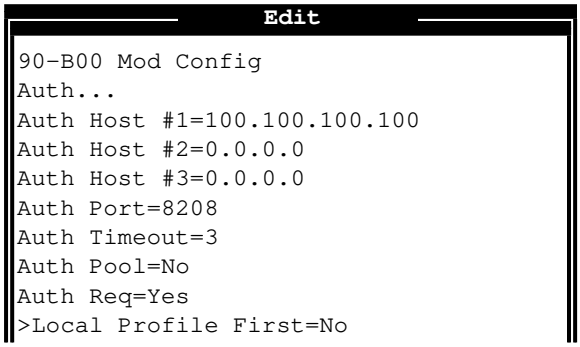
When Local Profiles First=No, the order of authentication is:

remote>local connection profiles>simple name/password

Configuring for remote authentication first

To configure a MAX to authenticate remote profiles before local profiles:

1 Open the Auth submenu of the Ethernet Mod Config menu.



2 Select Local Profile First=No

The default is Local Profile First=Yes. This is the same behavior as previously, before the Local Profile First added was added.

Note: If Auth=None, Local Profile first will be N/A.

Setting the Timeout to work with Local Profiles First=No

Remote authentication is tried first in Local Profile First=No, so the system has to wait for the remote authentication to time out. This may take longer than the timeout specified for the connection and causes all connection attempts to fail. To prevent this, set the value for Auth Timeout low enough to not cause the line to be dropped, but still high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

Authentication methods and remote authentication

Some authentication methods do not work the same without a remote authenticator as they do with one. Table 5 shows authentication methods and the specific information you will need to consider if you use a particular method with Local Profile First=No.

Table 5. Authentication methods

Method	Remote Authentication Considerations
PAP	None. Works the same with or without remote authentication.
CHAP	None. Works the same with or without remote authentication.
PAP-TOKEN	Works either way, but will not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.
PAP-TOKEN-CHAP	Brings up one channel, but all other channels fail.
CACHE-TOKEN	If the remote side has ever authenticated using a challenge, CACHE-TOKEN will not work with local profiles. If the remote side has not ever authenticated, there will be no problem with the local profiles.

EOI 1113 (4503)

Multilink or MP+ call now can span multiple MAX units

Multiple MAX units can now be configured to form a Stack, or group of MAX units, that allows a Multilink PPP (MP) or MP+ call to span the MAX units in the Stack.

Ascend units effected: MAX 4000

Call spanning using a Stack configuration can be effective when:

- a MAX running MP+ (and a member of the Stack) is asked for another phone number and has no available lines
- a rotary is used to access multiple MAXes using the same phone number, making it impossible to assume that a subsequent call is answered by the same MAX as the original call

MP/MP+ call spanning is protocol-independent, and should work with all protocols supported by the MAX.

Note: A Stack requires that a dial-in client use an endpoint discriminator. Most products that support MP or MP+ use an endpoint discriminator, but the specification for MP does not require it.

How MP/MP+ call spanning works

A Stack is a group of MAXes that have the same Stack information, and are on the same physical LAN. There is no “master” MAX; the MAXes in the Stack use an Ethernet multicast packet to locate each other.

Because these multicast packets are unlikely to cross a router, the MAXes in a single stack must be on the same physical LAN. MAXes running in a stack can generate fairly high levels of network traffic, another reason to keep them on the same physical LAN.

Once a Stack is created, every MP/MP+ call that comes to any member of the stack will be compared with MP/MP+ calls to other members of the Stack to determine if it is part of an already existing bundle. If this call is part of a new MP/MP+ bundle, the call will be answered and handled by the same MAX, as a MAX that is not in a Stack would do.

If the call is part of an already existing bundle, information about the bundle will be exchanged between MAX that answered the incoming MP/MP+ call and the MAX that owns the existing MP/MP+ bundle. The MAX that answered a subsequent call belonging to a bundle forwards all data packets to the MAX that owns the MP/MP+ bundle.

To balance the load among all available WAN channels, data packets for the WAN will be assigned to available channels on a rotating basis. Packets destined for a WAN interface that is not local to the bundle owner will be forwarded to the MAX that answered the second or subsequent call to be sent across the WAN link. This MAX must, of course, be in the same Stack as the bundle owner.

Connection profiles not shared within a Stack

A Stack does not support sharing of connection profiles between theMAXes in the Stack. Every MAX in the Stack that is set up to use internal authentication must retain all authentication information for every call. This requirement can be eliminated by using a centralized authentication server, such as RADIUS.

Phone numbers for new MP+ channels

Currently, if an MP+ call into a MAX that is not in a Stack needs to add an additional channel to an existing bundle, the MAX must provide a local phone number for the new channel. If an MP+ requests an additional channel from a MAX in a Stack, the MAX that owns the bundle will attempt to provide a local phone number. If no phone number is available, the MAX will as other members of the Stack for an available phone number to use for the new channel.

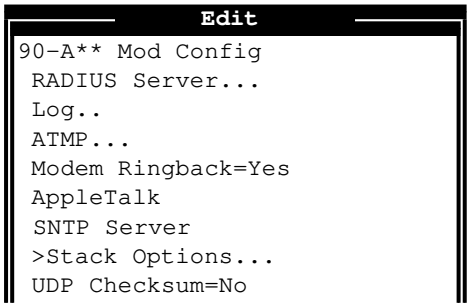
An MP call does not pass phone numbers when it adds a channel. The originator of the call must know all of the possible phone numbers to begin with.

Configuring and disabling a MAX Stack

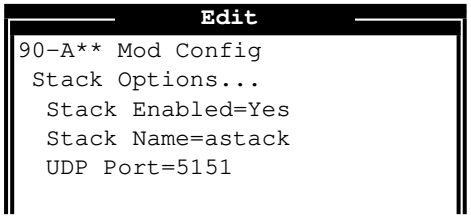
To configure a MAX stack:

1 Select the MAXes that will be members of the stack.
These MAXes must be on the same physical LAN.

2 Open the Ethernet>Mod Config menu and select Stack Options.



The Ethernet>Mod Config>Stack Options... menu appears.



3 Use Stack Enabled=Yes.

4 Specify a unique name for the stack in the Stack Name parameter.
A Stack name is 16 characters or less. This is the name members of a Stack use to identify other members of the same stack. The Stack name must be unique among all MAXes that communicate with each other, even if they are not on the same LAN.

If a MAX receives calls from two MAXes on different LANs that are members of different Stacks with the same Stack name, the MAX receiving the calls will assume the two MAXes with the same Stack name are the same bundle.

Note: Multiple stacks can exist on the same physical Ethernet LAN if the stacks have different names.

5 Specify the UDP port.

This is a reserved UDP port for intrastack communications. The UDP Port must be identical in all members of a stack, but is not required to be unique among all stacks.

Disabling a MAX Stack

To disable a Stack, use Stack Enabled=No in each of the MAXes in the Stack.

Adding and removing a MAX

You can add a MAX to an existing Stack at any time without rebooting the MAX or affecting Stack operation. Since a Stack is a collection of peers, none keeps a list of the stack membership. The MAXes in a Stack communicate when they need a service from the Stack.

Removing a MAX from a stack requires care, since any calls using a channel between the MAX to be removed and another MAX in the Stack could be dropped. There is no need to reboot a MAX removed from a Stack.

DHCP Server function over bridged connection added

DHCP server functionality has been added to the MAX for remote clients that are connected to the MAX over a bridged WAN connection. This feature allows a MAX to assign a dynamic IP address to a remote DHCP client. You configure and enable the feature on the RADIUS server connected to the MAX.

How the DCHP Server works

A DHCP Server can assign IP addresses dynamically to remote DHCP clients. In the MAX, the connection must be over a bridged WAN connection.

For example, if a group of DHCP clients are on a LAN connected to a Pipeline (Figure 3) and the Pipeline is connected to the MAX over a Bridged PPP connection, the MAX will be able to assign dynamic IP addresses to any of the DHCP clients on the remote LAN. The RADIUS server holds the configuration information the MAX uses to identify and authenticate a DHCP client.

When the DHCP client requests an address, the MAX allocates an IP address from one of its IP Address Pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment after the 30 minute period expires. The MAX keeps track of all the IP addresses it has assigned in its local memory.

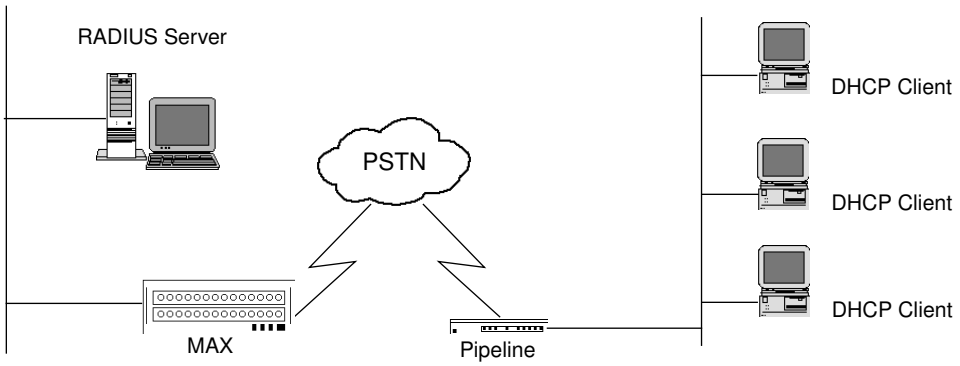


Figure 3. Example connection with DHCP clients

A MAX loses the entries for current (unexpired) IP address assignments when it is reset. A client may hold an unexpired IP address assignment when the MAX is reset. The reset MAX may assign the same address to a new client as the one being held by a client from before the reset. These duplicate IP addresses causes network problems until the first assignment expires or one of the clients reboots.

Configuring the DHCP server

Note: You can also configure the MAX as a DHCP server in a Connection profile or an Answer profile (for NAT for LAN only). Refer to "Network Address Translation (NAT) for a LAN" on page 28 for information on configuring the DHCP server in a Connection profile.

You configure the DHCP server by modifying appropriate connection profile in the RADIUS users file (in the /etc/raddb directory). To modify the connection profile, add the following two attributes to the entry for the connection to the LAN with DHCP clients (in Figure 3, the entry for the Pipeline):

- **`Ascend-DHCP-Reply=DHCP-Reply-Yes`**
  This enables the DHCP server functionality for the connection profile. To disable the DHCP server, set this attribute to **`DHCP-Reply-No`**.
- **Ascend-DHCP-Pool-Number**=*the appropriate value*
  Specify a number to define the IP pool number to use when allocating dynamic IP addresses. The possible values are 0 to n, where n is the last defined IP pool number. The default is 0.

  Note: If you omit this attribute, the first IP pool is used.

New RADIUS attributes added

Two new RADIUS attributes have been added to the RADIUS dictionary:

Ascend-DHCP-Reply

Description: Ascend-DHCP-Reply enables or disables DHCP server functionality for associated MAX units.

Usage: There are two possible values for this attribute:

DHCP-Reply-Yes enables the DHCP server for this connection profile.

DHCP-Reply-No is the default value; it disables the DHCP server for this connection profile.

Ascend-DHCP-Pool-Number

Description: Ascend-DHCP-Pool-Number defines the IP pool number for the DHCP server to use when allocating dynamic IP addresses. This attribute is optional. If it is not set, the first defined IP pool is used.

Usage: The values for this attribute are a number from 0 to *n*, where *n* is the last defined IP pool number. The default is 0, which causes the first defined IP pool to be used.

Dependencies: The maximum value of this attribute is determined by the number of IP pools defined.

Network Address Translation (NAT) for a LAN

Network Address Translation for a LAN allows the Pipeline to connect a LAN to another network even if the devices on the LAN do not have valid addresses for the remote network. The Pipeline will translate between LAN and remote network addresses.

Network address translation (NAT) for a LAN

Access to public networks, including the Internet, require the use of an official IP address that is unique across the entire network. Typically, ranges of addresses are assigned by a central authority, and these in turn are distributed under local management. If access to a public network is not needed, then local management may assign any addresses as they see fit, even if the addresses are not official or perhaps even officially assigned to another company.

Because the supply of addresses is rapidly diminishing a company may not be able to get official addresses for their entire network. Other sites may already be configured with unofficial addresses, but now want access to the Internet, where an official address is required. For these reasons, when routing to the Internet, a facility to borrow an official address and dynamically translate between the local and official addresses is necessary. Ascend has previously released Network Address Translation (NAT) for the Pipeline 25-*Px* as a single user solution to this problem. This feature expands NAT functionality to support a local area network, rather than a single station.

Overview

When NAT is enabled, the Pipeline will attempt to perform IP address translation on all packets received. The Pipeline has no notion of what may or may not be official addresses on the LAN.

The Pipeline acts as a DHCP client on behalf of all hosts on the LAN and relies on the MAX unit (acting as the DHCP server) to provide addresses suitable for the remote network from its IP address pool. On the local network, the Pipeline and the hosts all have “local” addresses on the same network that are only used for local communication between the hosts and the Pipeline over the Ethernet.

When the first client on the LAN requests access to the remote network, the Pipeline gets this address through PPP negotiation. When subsequent clients request access to the remote

network, the Pipeline asks for an IP address from the MAX using a DHCP request packet. The MAX then sends an address to the Pipeline from its IP address pool. The Pipeline uses the dynamic addresses it receives from the MAX to translate IP addresses on behalf of local clients.

As packets are received on the LAN, the Pipeline determines if the source IP address has been assigned a translated address. If so, then the packet is translated, and forwarded out the WAN. If no translation has been assigned (and is not pending), then a new DHCP request is issued for this IP address. While waiting for an IP address to be offered by the MAX, corresponding source packets will be dropped. Similarly, for packets received from the WAN, the Pipeline checks the destination address against its table of translated addresses. If the destination address exists and is active, the Pipeline forwards the packet. If the destination address does not exit, or is not active, the packet is dropped.

IP addresses are typically offered by the MAX only for a limited duration, but the Pipeline automatically renews the lease on these addresses. If the connection to the remote server is dropped, all leased addresses are considered revoked. Therefore, TCP connections will not persist across calls.

Figure 4 illustrates a basic NAT for LAN set up.

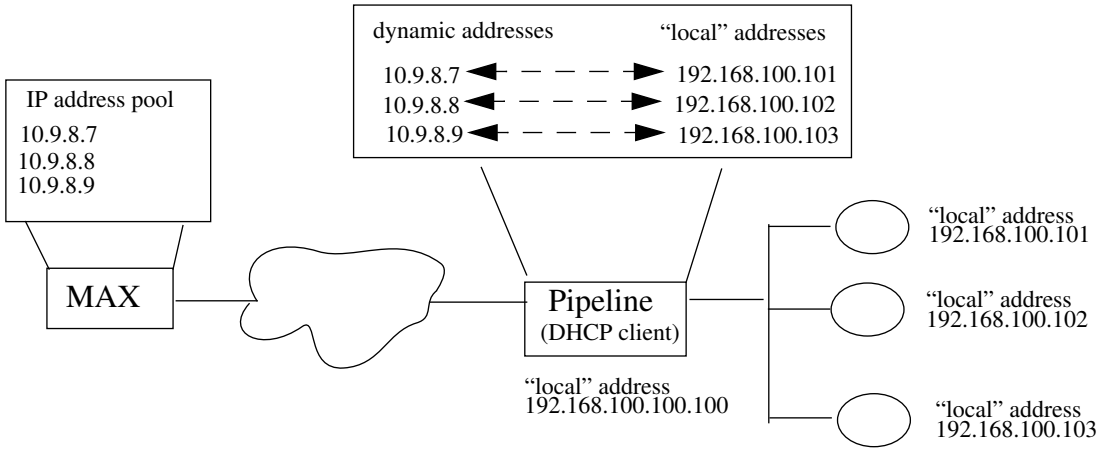


Figure 4. NAT for LAN setup

Note that in Figure 4, the Pipeline itself does not have an address on the remote network. This means that the Pipeline can only be accessed from the local network, not from the WAN.

In some installations, the MAX will be handling both NAT DHCP requests and ordinary DHCP requests. In this situation, if the ordinary DHCP clients are connecting to the MAX over a non-bridged connection, you must have a separate DHCP server to handle the ordinary DHCP requests; the MAX will only handle the NAT DHCP requests.

Configuring NAT on the Pipeline

Configuring NAT for the LAN requires that you configure both the Pipeline and the MAX it connects to.

Refer to the 5.0a release notes for the Pipeline for information on configuring NAT on the Pipeline.

Configuring NAT on the MAX

Where you configure NAT on the MAX depends on how your users are connecting to the MAX:

- Configure NAT in the Answer profile if you are using settings in the Answer profile to build the connection using the Use Answer as Defaults parameter (for RADIUS) or if you are using Names/Passwords profiles.
- Configure NAT in a Connection profile if you are using Connection profiles for users or if you are using the Template Connection # parameter (for Names/Passwords profiles).
- Configure NAT in a RADIUS profile if you are using RADIUS.

To configure NAT on the MAX:

1. From the main edit menu:
   - select Ethernet>Answer>DHCP options *or*
   - select Ethernet>Connections> *NAT Connection Profile*>DHCP options
2. Set Reply Enabled=Yes.
3. Set Pool Number to the IP address pool to use for allocating IP addresses to NAT clients.
   Set Pool Number to 0 to indicate that any pool can be used.
4. Set MAX Leases to the number of addresses that will be given to the Pipeline.
5. If you use RADIUS to authenticate users and you do not authenticate users that request DHCP, set Use Answer as Defaults to Yes in the Answer profile. Otherwise, the MAX will not act as a DHCP server for these clients.

See below for detailed descriptions of the NAT Routing, NAT Profile, Reply Enabled, Pool Number, and MAX Leases parameters.

New parameters

Reply Enabled

Description: This parameter specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection.

Usage: Press Enter to cycle through the choices:

- Yes specifies that the MAX will process DHCP packets.
  - If the connection to the MAX is over a bridged connection the MAX will respond to all DHCP requests.
  - If the connection is over any other type of connection, the MAX will only respond to NAT DHCP packets.
- No specifies that the MAX will not process DHCP packets; it routes or bridges DHCP packets as any other packet.
  This is the default.

Parameter Location: Ethernet > Answer > DHCP options Ethernet > Connections > DHCP options

Pool Number

Description: This parameter specifies the IP address pool to use to assign addresses to NAT clients.

Usage: Press Enter to open a text field. Then enter the IP address pool to use to assign IP addresses to clients using this connection. The valid range is from 0 to 150. The default is 0. A value of 0 means the MAX will assign any address from any available pool.

Dependencies: Keep this additional information in mind:

- Pool Number is N/A if Reply Enabled=No.

Parameter Location: Ethernet > Answer > DHCP option> Ethernet > Connections > DHCP options

Max Leases

Description: This parameter specifies the number of dynamic addresses to assign to NAT clients using this connection. When NAT is used, an initial dynamic address is automatically assigned via the PPP negotiations. This can be used to perform address translation for a single client on the LAN. When additional clients attempt to route packets through this connection, they must first be assigned their own dynamic address. The Max Leases parameter restricts the number of addresses to be given out through this connection, thus limiting the number of clients on the remote LAN who can access the Internet.

Usage: Press Enter to open a text field. Then enter the maximum number of addresses to assign to clients using this connection. The valid range is from 1 to 254. The default is 4.

Dependencies: Keep this additional information in mind:

- Pool Number is N/A if Reply Enabled=No.

Parameter Location: Ethernet > Answer > DHCP options
Ethernet > Connections > DHCP options

New RADIUS attributes

The RADIUS attribute Ascend-DHCP-Reply corresponds to Reply Enabled.

The RADIUS attribute Ascend-DHCP-Pool-Number corresponds to Pool Number.

The RADIUS attribute Ascend-DHCP-Maximum-Leases corresponds to Max Leases.

NET3 PTP signaling support added

NET3 point-to-point (PTP) signaling support has been added to all Ascend platforms that support BRI. NET3 PTP signaling is a variation of standard EURO-ISDN signaling used in Germany. It uses a fixed TEI, as opposed to a TEI assigned by the network.

Configuring NET3 PTP signaling

To configure a MAX for NET3 PTP signaling:

1 Open Net/BRI>Line Config>*any profile*.

2 Select NET3 PTP.

3 Close the Line Profile.

TACACS+ support

This release adds support for TACACS+ authentication, authorization, and accounting on all platforms that currently support RADIUS accounting. TACACS+ *(Terminal Access Concentrator Access Control Server Plus)* is a server from Cisco Systems, Inc.

Introduction

TACACS+ supports what Cisco calls the "three A's"—authentication, authorization, and accounting.

- Authentication

  Authentication enables you to determine whether a dial-in user has permission to access the Ascend unit.

- Authorization

  Under TACACS+, authorization takes place as a set separate from authentication. In the authorization step, the Ascend unit sends parameters specifying the username, port, encapsulation type, protocol, and address pool (for a framed user) or the username, port, and service (for an unframed user) to the TACACS+ server. TACACS+ returns a set of parameters that specify the limits of the user's network access and the specific characteristics of the WAN connection. The TACACS+ procedure is different from the RADIUS server's implementation; in RADIUS, authentication and authorization take place in the same step.

- Accounting

  Like RADIUS accounting, TACACS+ accounting provides statistics on an authenticated session; you can use the information for billing purposes or to troubleshoot operations.

Ascend currently supports the TACACS+ parameters listed in Table 6. For complete information on each parameter, consult the Cisco documentation.

Table 6. TACACS+ parameters supported by Ascend

Parameter syntax	Description
acl=<number>	Specifies an index into the Firewall/Filter table
timeout=<number>	Indicates the number of seconds that this session can remain connected. This value appears in the maxSessionTime field of the miscInfo profile.

Table 6. TACACS+ parameters supported by Ascend

Parameter syntax	Description
idletime=<number>	Specifies the idle time of the session, in seconds. This value appears in the idleLimit field of the Session profile.
routing=<true or false>	Sets up the ip.routingMode field in the profile.
addr-pool=<number>	Sets the ip.assignPoolIndex field in the profile, and sets the ip.assignAddress field in the profile to TRUE.
addr=<ip-address>	Sets the ip.hostAddress field in the profile, and sets the ip.netmask field in the profile to HOST_NETMASK.
autocmd=<telnet or ppp>	If set to telnet, sets the mgmtType field to CALL_MGMT_TCP_RAW. If set to ppp, sets the userService field in the miscInfo profile to Framed_User, the loginService field to Login_Service_Undefined, and the framedProtocol field to Framed_Protocol_PPP. This setting also starts a second round of authorization for the purpose of obtaining the PPP parameters.
cmd-arg=<string>	Currently, the first cmd-arg value appears in the tcp.loginHost field of the profile, and any subsequent ones appear in the tcp.loginPort field of the profile.

The initial profile that TACACS+ uses is either the lanAnswerProfile (if the forceDefault flag is TRUE), or the factory default InetProfile. The hostName is copied from the user field of the authData profile; then, the recvPassword field is filled in and the callMode is set to CALL_ANS_ONLY.

Support for TACACS+ authentication

No new parameters appear in the Ethernet>Mod Config>Auth menu, but some parameters have been modified to support TACACS+ authentication. These parameters are:

- Auth
- Auth Host #*n*
- Auth Key
- Auth Port
- Auth Timeout

The sections that follow describe each Auth menu parameter that now supports TACACS+ authentication.

Keep this additional information in mind:

- The Metric, Profile Reqd, and Use Answer as Default parameters in the Answer Profile now apply to TACACS+ authentication as well as RADIUS and TACACS authentication.

- The terminal server can now authenticate with TACACS+; the TACACS+ server sends the username and password prompts.

Auth

Description: This parameter enables remote authentication and authorization for incoming PPP, Combinet, and terminal server calls. The Auth parameter applies to both synchronous and asynchronous PPP encapsulation.

Usage: Press Enter to cycle through the choices.

- None disables the use of an authentication server.

  None is the default.
- TACACS (Terminal Access Concentrator Access Control Server) is a very simple query/response protocol that enables the MAX to check a user's password, and permit or prevent access.

  If you choose TACACS and the MAX cannot find a local Connection profile matching the incoming call, it requests remote authentication by a TACACS server.

  TACACS supports PAP (Password Authentication Protocol), Combinet name and password validation, and terminal server validation. TACACS does not support CHAP (Challenge Handshake Authentication Protocol). PAP and CHAP are both PPP authentication protocols. CHAP is the more secure.
- TACACS+ is an extension of TACACS.
- RADIUS (Remote Authentication Dial In User Service) is a protocol by which users can have access to secure networks through a centrally managed server.

  You can store virtually all Connection profile information on the RADIUS server in a flat ASCII database.

  If you choose RADIUS and the MAX cannot find a local Connection profile matching the incoming call, it requests remote authentication by a RADIUS server. In a RADIUS query, the MAX provides a user ID and password to the server. If the validation succeeds, the server sends back a complete profile; this profile specifies routing, packet filtering, destination-specific static routes, and usage restrictions for the user.

  RADIUS supports PAP and CHAP, Combinet name and password validation, and terminal server validation.
- RADIUS/LOGOUT is identical to RADIUS, except that when you select RADIUS/LOGOUT, the MAX sends a request to the RADIUS server to initiate logout when the session ends.

Dependencies: Keep this additional information in mind:

- The Auth parameter applies only to PPP calls (Encaps=PPP), Combinet calls (Encaps=COMB), and terminal server calls.
- If you select TACACS, TACACS+, RADIUS, or RADIUS/LOGOUT, you must specify at least one authentication server using the Auth Host parameter.

Parameter Location: Ethernet profile: Ethernet>Mod Config

See Also: Auth Host, Auth Key, Auth Port, Auth Timeout, Encaps

Auth Host #*n* (*n*=1–3)

Description: This parameter specifies the IP address of each authentication server that the MAX can use when placing or receiving PPP, MP+, or Combinet calls. You can specify a

RADIUS, TACACS, or TACACS+ server that carries out both authentication and authorization.

The MAX first tries to connect to Auth Host #1; if it receives no response, it tries to connect to Auth Host #2. If no response comes from Auth Host #2, the MAX tries to connect to Auth Host #3.

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

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0; this setting indicates that no authentication server exists.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If you set Auth=RADIUS, TACACS, or TACACS+ and specify Auth Host #1 and Auth Host #2, the MAX uses the second host if it gets no response from the first one.

  In addition, the MAX uses the second host until that machine fails to serve requests; the MAX does not use the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests.
- The Auth Host parameter does not apply when you have disabled authentication services (Auth=None).

Parameter Location: Ethernet profile: Ethernet>Mod Config

See Also: Auth, Auth Key, Auth Port, Auth Timeout

Auth Key

Description: This parameter specifies a RADIUS, TACACS, or TACACS+ client password for use with an authentication or authorization request.

Usage: Press Enter to open a text field. Then, type the client password exactly as it appears in the RADIUS clients file, the TACACS configuration file, or the TACACS+ configuration file. The password is case sensitive. Press Enter again to close the text field.

Parameter Location: Ethernet profile: Ethernet>Mod Config

See Also: Auth, Auth Host, Auth Port, Auth Timeout

Auth Port

Description: This parameter specifies the UDP port number that the MAX uses in remote validation requests for RADIUS, TACACS, and TACACS+ authentication and authorization.

Usage: Press Enter to open a text field. Then, enter a port number. The value you enter must match the port number that the RADIUS, TACACS, or TACACS+ daemon uses.

The default value for the RADIUS daemon appears in the /etc/services file on the UNIX host on which the daemon is running. The default value for the TACACS or TACACS+ daemon is 49.

Press Enter again to close the text field.

Parameter Location: Ethernet profile: Ethernet>Mod Config

See Also: Auth, Auth Host, Auth Key, Auth Timeout

Auth Timeout

Description: This parameter sets the number of seconds the MAX waits for a response to a RADIUS, TACACS, or TACACS+ authentication or authorization request. If the MAX does not receive a response within the time specified by Auth Timeout, it sends the request to the next authentication server specified by the Auth Host parameter.

Usage: Press Enter to open a text field. Then, type the number of seconds the MAX should wait for a response to an authentication or authorization request. You can specify a number from 1 to 10. The default is 1. Press Enter again to close the text field.

Dependencies: The Auth Timeout parameter applies only when you set the Auth parameter to TACACS, TACACS+, RADIUS, or RADIUS/LOGOUT. If Auth=None, the Auth Timeout parameter does not apply.

Parameter Location: Ethernet profile: Ethernet>Mod Config

See Also: Auth, Auth Host, Auth Key, Auth Port

Support for TACACS+ authorization

TACACS+ authorization permits users to use PPP when logged in using the terminal server, and also supports the use of FireWalls. You can now specify a TACACS+ authorization host when setting up the MAX. This feature supports the same TACACS+ functionality as the Cisco product line.

No new parameters appear in the Ethernet>Mod Config>Auth menu, but some parameters have been modified to support TACACS+ authorization. These parameters are:

- Auth
- Auth Host #*n*
- Auth Key
- Auth Port
- Auth Timeout

For information on each of these parameters, see“Support for TACACS+ authentication” on page 33.

The router can now send two additional packet types—TACACS+ authorization-request and authorization-reply packets. These are the only two packet types added.

Support for TACACS+ accounting

No new parameters appear in the Ethernet>Mod Config>Accounting menu, but some parameters have been modified to support TACACS+ accounting. These parameters are:

- Acct
- Acct Host #*n*
- Acct Key
- Acct Port

The sections that follow describe each parameter that now supports TACACS+ accounting.

Acct

Description: This parameter allows you to specify the type of accounting service to use for incoming and outgoing bridging/routing calls, and for incoming terminal server calls.

Usage: Press Enter to cycle through the choices.

- RADIUS enables RADIUS accounting.

  When the MAX begins a terminal server, bridging, or routing session, it sends an Accounting Start Packet to the RADIUS accounting server. This packet describes the type of session being opened, and the name of the user opening the session. (The MAX does not send an Accounting Start Packet if a call fails authentication.) At the end of a session, the MAX sends an Accounting Stop Packet. If the user is running an unmodified Ascend RADIUS daemon, the RADIUS accounting server saves the information in the accounting packets in a RADIUS log file.

  In some cases, a session can begin with a user login, and then authentication follows. This type of situation occurs when a terminal server user chooses PPP or SLIP after login. In such a case, the MAX sends an Accounting Start Packet after login and not after authentication.
- TACACS+ enables TACACS+ accounting.
- None specifies that no accounting takes place.

  None is the default.

Dependencies: Keep this additional information in mind:

- If you set Acct=RADIUS, you must specify at least one RADIUS accounting server using the Acct Host #*n* parameter.

  The RADIUS server must be running a version of the RADIUS daemon that specifically supports accounting.
- If you set Acct=TACACS+, you must specify at least one TACACS+ accounting server using the Acct Host #*n* parameter.
- RADIUS accounting is disabled if you set Auth=RADIUS/LOGOUT.
- When you set Acct=TACACS+, the Acct Timeout and Sess Timer parameters do not apply.

  Because TACACS+ uses TCP, it has its own timeout method.
- When you set Acct=TACACS+, the Acct-ID Base parameter does not apply.

  This parameter applies only to RADIUS accounting, and enables you to specify whether the session ID is presented in decimal or hexadecimal format. TACACS+ uses only decimal format.
- The server you use for accounting can be the same server you use for authentication and authorization; this scenario works best in low-traffic situations.

Parameter Location: Ethernet profile: Ethernet>Mod Config>Accounting

See Also: Acct Host #*n*, Auth

Acct Host #*n*

Description: This parameter specifies the IP address of each RADIUS or TACACS+ accounting server. The MAX first tries to connect to Acct Host #1. If it gets no response, it attempts to

connect to Acct Host #2. If both these connection attempts fail, the MAX attempts to connect to Acct Host #3.

If Acct=RADIUS, all three Acct Host parameters must specify RADIUS servers. If Acct=TACACS+, all three Acct Host parameters must specify TACACS+ servers.

Usage: Press Enter to open a text field. Then, type the IP address of each RADIUS or TACACS+ accounting server.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address using a slash. The default value is 0.0.0.0/0. The default setting specifies that no accounting server is available.

Press Enter again to close the text field.

Dependencies: The Acct Host #*n* parameter does not apply when Acct=None.

Parameter Location: Ethernet profile: Ethernet>Mod Config>Accounting

See Also: Acct

Acct Key

Description: This parameter specifies a RADIUS or TACACS+ shared secret. A shared secret acts like a password between the MAX and the accounting server.

Usage: Press Enter to open a text field. Then, type the text of the shared secret. The value you specify must match the value assigned in the RADIUS clients file or the TACACS+ configuration file. Press Enter again to close the text field.

Parameter Location: Ethernet profile: Ethernet>Mod Config>Accounting

See Also: Acct, Acct Host #*n*

Acct Port

Description: This parameter specifies the UDP port number that the Ascend unit uses in accounting requests.

Usage: Press Enter to open a text field. Then, type a UDP port number. The value you specify must match the port number the accounting daemon uses. For RADIUS, the default value is 1646. For TACACS+, the default value is 49. Press Enter again to close the text field.

Parameter Location: Ethernet profile: Ethernet>Mod Config>Accounting

See Also: Acct, Acct Host #*n*

Updates to the immediate modem feature

Immediate modem service now has its own password protection and has been modified to support binary downloads.

The ability to download binary files via modem requires no configuration. It is always enabled for users dialing out on the MAX unit's modems.

The new Imm. Modem Pwd parameter is located in the Tserv Options submenu of the Ethernet Profile. This parameter is a text field that accepts a password up to 64 characters. If the field is

non-null, users will be prompted for a password before being allowed access to a modem and modem dialout service will be denied if the user does not enter the proper password. The Imm. Modem Pwd parameter is N/A if the terminal server is not enabled, or if Modem Dialout or Immediate Modem are disabled.

RADIUS accounting statistics sent to choice of servers

A feature allowing a connection profile to specify RADIUS accounting servers has been added to allow connection accounting on a per-user basis. Accounting information is sent to the server specified in the connection profile.

How it works: A network reseller may service many different ISPs, each with a different and access policy. The reseller carries traffic of individual users and must filter and bill this usage according to the policies of the appropriate ISP.

The new per-user accounting feature allows network resellers to direct accounting information about specific users to RADIUS servers belonging to ISPs. It does this by allowing a reseller to specify the location of a RADIUS accounting server within a Connection profile. This means that different connection profiles can specify different RADIUS servers.

Each connection profile also specifies the accounting policy by allowing accounting data to be sent:

- only to the RADIUS accounting server specified in the Connection profile
- only to the server specified in the existing Accounting submenu of the Ethernet profile.
- to both servers

Note: The default behavior of the MAX is to use the default server.

When an accounting event occurs, the MAX sends an accounting message to the server specified in the connection profile. Each accounting message is placed on a list to wait for acknowledgment from the RADIUS server. The MAX retries sending the accounting message. The oldest entry on the list is discarded when the total number of entries on the list exceeds the maximum.

Note: There is no SNMP support for this feature.

Specifying the server for accounting messages

To specify a server or servers to receive accounting messages from a MAX:

1 Open the Ethernet Connection profile.

2 Select Accounting.
The Accounting submenu sample data appears below.

Note: The following is an example of the new Accounting submenu of the Connection profile. For complete information on these parameters, refer to the documentation that came with your MAX.

```
Edit
90-101 Alpha...
 Accounting...
  Acct Type=User
  Acct Host #1=1.2.3.4
  Acct Port=1646
  Acct Timeout=1
  Acct Key=******
  Acct-ID Base=10
```

Table 7. Accounting menu field descriptions

Field	Values	Description
Acct Type	None	The MAX sends accounting information only to the default accounting server specified in the Ethernet profile.
	User	The MAX logs accounting information to the RADIUS server specified as Acct Host #1.
	User+Default	The MAX logs accounting information to the RADIUS server specified as Acct Host #1 as well as the default accounting server specifics in the Ethernet profile.
Acct Host #1	IP address	The IP address of the RADIUS server specified as Acct Host #1. The field is valid when Acct=User or Acct=User+Default. N/A when Acct=None.
Acct Port	Integer in the range [1 .. 32767] inclusive	The port for the RADIUS server specified as Acct Host #1. The field is valid when Acct=User or Acct=User+Default. N/A when Acct=None.
Acct Key	string	Shared secret between the Ascend unit and the RADIUS accounting server. This key is used in calculating the authenticator. Can be any string value up to 20 characters. Default value is an empty string.

Table 7. Accounting menu field descriptions

Field	Values	Description
Acct Timeout	Integer in the range [1 .. 60] inclusive	The time interval that specifies how long the Ascend unit is to wait for a reply from the server. If the server does not send a reply before the timeout expires, it sends another packets to the accounting server. If the Ascend-User-Acct-Type is user+default, then two separate packets are sent: one to the defined accounting server, the other to the default accounting server. The field is valid when Acct=User or Acct=User+Default. N/A when Acct=None. The MAX resends unacknowledged accounting records to the RADIUS server when this timeout expires.
Acct-ID Base	0 or 16	The numeric base (base 10 or base 16) for the session ID. The field is valid when Acct=User or Acct=User+Default. N/A when Acct=None.

Specifying a RADIUS accounting server in RADIUS profiles

You can specify a RADIUS accounting server within a RADIUS server profile. To support this feature, the following new RADIUS attributes are defined.

Ascend-User-Acct-Type (138)

Description: Specifies whether accounting information will be sent to the RADIUS server specified for the connection, the default accounting server for the MAX (if any), or to both servers.

Usage: Integer with the following values:

0	The MAX sends accounting information only to the default accounting server specified in the Ethernet profile.	Ascend-User-Acct-None
1	The MAX logs accounting information to the RADIUS server specified as Ascend-User-Acct-Host(139).	Ascend-User-Acct-User
2	The MAX logs accounting information to the RADIUS server specified as Ascend-User-Acct-Host(139) as well as the default accounting server specifics in the Ethernet profile.	Ascend-User-Acct-User-Default

Ascend-User-Acct-Host(139)

Description: Specifies the IP address of the RADIUS accounting server to which accounting information for this connection will be sent (Acct Host #1).

Usage: `ipaddr` containing the IP address of the destination RADIUS server.

Ascend-User-Acct-Port(140)

Description: Specifies the port used by the RADIUS server specified as Acct Host #1.Integer in the range [1 .. 32767] inclusive (Acct Port).

Usage: Integer in the range [1 .. 32767] inclusive.

Ascend-User-Acct-Key(141)

Description: Shared "secret" between the Ascend unit and the RADIUS accounting server. This key is used in calculating the authenticator (Acct Key).

Usage: String with a maximum of 20 characters. Default is an empty string.

Ascend-User-Acct-Base(142)

Description: The numeric base (base 10 or base 16) for the session ID (Acct-ID Base).

Usage: Ascend-User-Acct-Base Base-10 0
Ascend-User-Acct-Base Base-16 1

Ascend-User-Acct-Time(143)

Description: The time interval that specifies how long the Ascend unit is to wait for a reply from the server. If the server does not send a reply before the timeout expires, it sends another packets to the accounting server. If the Ascend-User-Acct-Type is user+default, then two separate packets are sent: one to the defined accounting server, the other to the default accounting server (Acct Timeout).

Usage: An integer in the range 1 to 60 inclusive.

Accounting record structure

Accounting records sent to the RADIUS accounting server contain all of the following attributes. Additional attributes may be present.

- User-Name attribute
- NAS-Identifier attribute (NAS IP address, plus type and length)
- Class attribute (if any)
- Acct-Status-Type attribute (START or STOP)
- Acct-Session-Id attribute
- Acct-Session-Time attribute (if this is a logout event)
- Framed-Protocol
- Framed-Address

RADIUS static routes can be stacked in OSPF

This feature affects the MAX when it has a RADIUS user profile that defines a static route to the same destination as one of the MAX unit's IP Route profiles or a RADIUS route-x profile. When the RADIUS user connects, the metric for the User profile overrides the metric in the RADIUS route-x profile or the MAX IP Route profile.

The MAX unit's routing table gets information from the following static and dynamic sources:

- static routes from the MAX IP Route profiles
- static routes from the RADIUS route-x profiles
- static routes from the MAX Connection profiles
- static routes from the RADIUS user profiles
- dynamic routes from RIP updates
- dynamic routes from OSPF updates

For example, suppose a MAX has a static route to network xxx.xxx.xxx.xxx/yy with a metric of 10. A user profile in RADIUS to the same network has a metric of 7. When the route is not connected, the MAX routing table indicates this route has a metric of 10. When the route is connected, the MAX routing table indicates it has a metric of 7 with an "r" in the flags column to indicate the route came from RADIUS. Furthermore, the old route with a metric of 10 remains in the routing table, with an "*" in the flags column, indicating it is a hidden route.

Changes to the iproute command

This feature adds a new flag to the "iproute show command." The user route shown for radius users is marked with an "r." The normal static route temporarily moves down on the list, and appears with a "*" (the flag for a hidden route) in front of it.

Note: There is no new user configuration required for this feature. Standard OSPF configuration is covered in the documentation that came with your Ascend unit.

MAXDial control panel added for WIN95

This feature installs a new application named MAXDial in the Control Panel window on your Windows 95 desktop. You can use the MAXDial control panel to assign MAX units to the computer's serial ports or remove previous such assignments.

How it works

MAXDial enables you to assign an Ascend MAX to a physical serial port or virtual MAXDial serial port on a Windows workstation. You need to install the MAXDial's virtual serial port and associate MAXs with serial ports on the computer. You can perform both of these tasks from the MAXDial control panel, installed using the procedure in Installing the MAXDial control panel, below. From this control panel you can assign MAX unit's to the computer's serial ports or remove previous assignments.

Installing the MAXDial control panel

To assist you in the MAXDial installation, a Windows help file coaches you through the process of installing the software. You can install the software simply by running Setup and following the instructions on the screen.

The procedure given below is a full description of the steps involved in the installation and duplicates the information in the help file launched when you run Setup.

1 From the Windows 95 desktop, pull down Start/Settings/Control Panel

2 Click Add New Hardware to start the Add New Hardware wizard.

3 Click Next at the first screen.

4 The second screen will offer to have Windows detect new hardware.

5 Select No and click Next.

Note: You are about to add a virtual COM port to the system; since this is essentially fake hardware, there is no way Windows can find it.

6 Select Ports (COM & LPT) from the menu of hardware types and click Next.

7 Select Have Disk from the menu of manufacturers that appears.

8 Insert the MaxDial 32 installation disk into any drive.

9 Enter the drive letter if it differs from the default shown and click OK.

10 Select MaxDial Serial Port from the menu of models that appears (this should be the only available selection) and click Next.

Windows 95 displays the following message “Windows can install your hardware...”.

11 Click Next, ignoring the warning message “Your hardware may not be set to use these resources...”.

Wait while Windows copies files to the hard drive.

12 When thefollowing message appears “Windows has finished installing the software,...” click Finish.

13 Windows displays a message to reboot the machine.

You can restart now (by pulling down Start>Shut Down>Restart the computer and selecting Yes) or after you complete Configuring a MAXDial serial port.

14 Proceed to Configuring a MAXDial serial port.

Configuring a MAXDial serial port

Configure the new serial port using the MAXDial control panel as described in Configuring a MAXDial serial port, in this document.

1 Open the Windows control panel.

2 From the Start menu, choose Settings, then Control Panel.

3 Double-click the MAXDial Ports icon in the Control Panel.

The MAXDial Serial Port Setup dialog box appears. This dialog box lists all serial ports on the system, including any MAXDial virtual ports that were installed by the Add New Hardware wizard (see Installing the MAXDial control panel). The IP address and name of the MAX currently assigned to each port is shown in columns to the right of the port name in the list box. If no MAX is assigned to a port, the MAX column shows Unassigned and the IP Address column is blank.

4 Double-click the serial port you want to configure.
The Configure Port dialog box appears.

5 Do one of the following:
- If the port is currently assigned to a MAX and you wish to unassign it, click the Unassigned radio button, then click the OK button to close the dialog box.
- If the port is currently unassigned, follow Step 6 through Step 7 to configure the port, then click OK to close the dialog box.

6 Click the Assign radio button.

7 Enter the MAXs IP address into the IP Address field.
You can also click Find to open the Find MAXs dialog box, from which you can choose from a listing of MAXs found on the local network.

8 Enter the immediate port number in the dialog box that appears.
Check with the system administrator if you do not know this number.

9 If an Immediate Modem password has been assigned to the MAX, enter that password in the Password field. Otherwise, leave the Password field blank.

10 Click OK to close the dialog box.

11 Click Close to close the Serial Port setup dialog box.
The MAXDial control panel connects to the MAX and download configuration information needed to configure the port. If an error or timeout occurs during the download, the user is warned via a message box.

You can now proceed to Defining a modem for the serial port (optional) or restart the computer, if you did not do so in Step 13 of the installation procedure. To restart the computer, pull down Start>Shut Down>Restart the computer and select Yes.

Defining a modem for the serial port

Although defining a modem for the port is optional, many Windows 95 programs will work better if you do. To define a modem for the port:

1 Pull down Start>Settings>Control Panel and click Modems to start the Modems control panel.

2 At the first screen, select Add.

3 If you are using a portable computer, Windows may present a screen offering a choice between PCMCIA modems and Other. If this appears, select Other and click Next; otherwise go on to the next step.

4 The following message appears “Windows will now try to detect your modem...” Click Next.

5 Wait until the following message appears: “Please wait while Windows attempts to detect your modem...”

6 Windows displays the message “The following modem was found...”. If the selection is correct, click Next.
If Windows has detected the modem incorrectly, change the selection and click Next.

7 Click Finish when the following message “Your modem has been set up successfully...” appears.

8 You should now restart the computer, if you did not do so in Step 13 of the installation procedure. To restart the computer, pull down Start>Shut Down>Restart the computer and select Yes.

Although defining a modem for the port is optional, many Windows 95 programs work better if you do. To define a modem for the port:

1 Pull down Start>Settings>Control Panel and click Modems to start the Modems control panel.

2 At the first screen, select Add.

A message appears "Windows will try to detect your modem...".

If you are using a portable computer, Windows may present a screen offering a choice between PCMCIA modems and Other. If this appears, select Other and click Next; otherwise go on to the next step.

3 Click on the checkbox labelled "Don't detect my modem. I will select it from a list" and then click Next.

A list of modem manufacturers appear.

4 Click on the Have Disk button.

5 Insert the MAXDial 32 installation disk into any drive.

6 Enter the drive letter if it differs from the default shown and click OK.

7 Select Ascend digital modem from the list of models that appears (this should be the only choice) and click Next.

8 Select the MAXDial port you are configuring from the list of ports that appears and click Next.

9 Click Finish when the message "Your modem has been set up successfully..." appears.

10 You should now restart the computer, if you did not do so in Step 13 of the installation procedure. To restart the computer, pull down Start>Shut Down>Restart the computer and select Yes.

Network summaries for address pools

Summarizing host routes to reduce routing table overhead. IP addresses assigned dynamically from a pool are added to the routing table as individual host routes. You can now summarize this network (the entire pool), cutting down significantly on route flappage and the size of routing table advertisements.

These enhancements apply to all Ascend units that support IP address pools: the MAX 4000, MAX 2000, MAX 1800, and the MAX 200Plus. The only part of this document that applies to the Pipeline 130, 75, 50, and 25, are the definitions of the black-hole and reject interfaces. In normal Pipeline operation, these two interfaces would not be used.

The new pool summary feature enables the router to advertise a single route for the network defined in an address pool, and not to advertise individual host routes for each assigned address. Packets destined for a valid host address are routed to that host, and packets destined for an invalid host address are rejected with an ICMP "host unreachable" message or discarded.

To summarize IP address pools you must, (1) network-align the address pool, (2) enter a static route for the pool subnet, (3) make all connection profiles and radius user profiles that provide IP addresses from these pools private, (4) turn on pool summarization.

1 To network-align the MAX's address pools follow these rules:

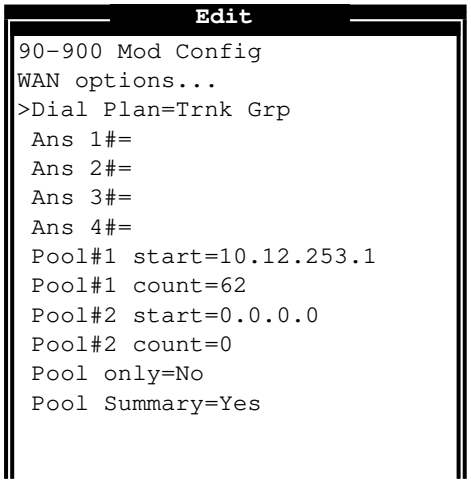
- The pool-count number must be two less than the total number of addresses in the pool.

  Add 2 to the pool-count. (Pool-count + 2) should give the total number of addresses in the subnet. Calculate the netmask for the subnet based on this total. (The Ascend netmask notation section in you manual lists the netmask verses total addresses.

- The pool-start address must be the first host address.

  Subtract 1 from the pool-start address. (Pool-start –1) should give the valid zero address for the subnet.

For example, verify the following configuration is network aligned:



- Pool-count = 62

  Add 2 + 62 = 64: The netmask for 64 addresses is 255.255.255.192. (Note: 256 - 64 = 192). The Ascend subnet notation for a 255.255.255.192 netmask is /26.

- Pool-start = 10.12.253.1

  Subtract 10.12.253.1 - 1 = 10.12.253.0, which is a valid zero address for the 255.255.255.192 netmask. Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same netmask.

  The resulting address pool network is:
  10.12.253.0/26

2 After verifying that each and every one of your address pools is network-aligned, you must enter a static route for them. These static routes handle all IP address that have not been given to users; specifically, when the MAX receives a packet whose IP address matches an unused IP address in a pool, it either returns the packet to the sender with an ICMP reject or simply discards the packet. Two new internal interfaces have been added for that purpose.

- The reject interface (rj0)

  The reject interface has an IP address of 127.0.0.2. Packets routed to this interface are sent back to the source address with an ICMP "host unreachable" message.

- The black-hole interface (bh0)

The black-hole interface has an IP address of 127.0.0.3. Packets routed to this interface are discarded silently.

For example, the following static route, silently discards all packets whose destination falls in the pool's subnet. In addition to the Dest and Gateway parameters that define the pool, be sure you have set parameters Metric=0, Preference=0, Cost=0, and Private=No:

```
Edit
90-401 pool-net
>Name=pool-net
 Active=Yes
 Dest=10.12.253.0/26
 Gateway=127.0.0.3
 Metric=0
 Preference=0
 Cost=0
 Private=No
```

Note: Since the MAX creates a host route for every assigned address from the pools and since host routes override subnet routes, packets whose destination matches an assigned IP address from the pool are properly routed and not discarded or bounced. Because the MAX advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network might improperly send the MAX a packet to an inactive IP address. Depending on the above static route, these packets are either bounced with an ICMP unreachable or silently discarded.

3 Make the Connection profiles that assign IP addresses from the pool private.

For example, the following Connection profile is configured for assigning IP addresses has Private=Yes:

```
Edit
90-110 p75-home
 Ip options...
  LAN Adrs=0.0.0.0/0
  WAN Alias=0.0.0.0
  IF Adrs=0.0.0.0/0
  Preference=100
  Cost=0
  Private=Yes
```

4 Set the parameter Pool Summary = Yes to enable pool summarization as in the following example.

```
Edit
90-800 Mod Config
 WAN options..
  Pool#A start=0.0.0.0
  Pool#A count=0
  Pool only=Yes
  Pool Summary=Yes
```

This is the new Pool Summary parameter:

Table 8. Pool summary parameter

Location	Parameters with example values
Ethernet > Mod Config > WAN Options...> (Ethernet Profile)	Pool Summary=Yes

In the example above with its route and pool configuration, the terminal server IPROUTE SHOW command contained the following lines:

```
Destination         Gateway     IF      Flg       Pref    Met     Use     Age
10.12.253.0/26      -           bh0     C         0       0       0    172162
127.0.0.1/32        -           lo0     CP        0       0       0    172163
127.0.0.2/32        -           rj0     CP        0       0       0    172163
127.0.0.3/32        -           bh0     CP        0       0       0    172163
```

The following is the only information that applies to Pipelines:

Two new interfaces have been added to the Pipeline's routing table. These interfaces perform the following functions:

- The reject interface (rj0)

  The reject interface has an IP address of 127.0.0.2. Packets routed to this interface are sent back to the source address with an ICMP "host unreachable" message.
- The black-hole interface (bh0)

  The black-hole interface has an IP address of 127.0.0.3. Packets routed to this interface are discarded silently.

Password implemented for immediate modem feature

A new password has been added that separately controls access to the immediate modem feature. Previously, the Telnet password controlled access to the immediate modem feature as well as to Telnet.

The immediate modem password separately governs whether a user is allowed to use the immediate modem functionality. Previously, a user who knew the Telnet password always had access to the dialout functionality of the immediate modem.

If Telnet is password-protected, a user must know the Telnet password as well as the immediate modem password in order to dial out. To use Telnet but not the dialout functionality, a user only needs to know the Telnet password.

Configuring an immediate modem password

You specify a password for access to the modem by typing the password in the Imm.Modem Pwd field of the TServ options submenu of the Ethernet profile. The maximum length of the password is 64 characters.

Note: By default there is no password present.

```
Edit
90-B00 Mod Config
 TServ Options...
   Silent=No
   Modem Dialout=Yes
   Immediate Modem=Yes
   Imm. Modem port=5000
   Imm. Modem Pwd=*****
```

The Imm. Modem Pwd field is N/A if any of the following are disabled:

- terminal server
- Modem Dialout
- Immediate Modem

RADIUS accounting coldstart notification

A new packet type and a new attribute have been added that allow an Ascend Network Access Server (NAS) to notify the RADIUS accounting server when the NAS comes up. The packet is analogous to the SNMP coldstart trap.

How the coldstart notification packet works

Currently the Ascend-Event packet is used to send periodic updates on the number of sessions per Class. When an NAS unit is started, it sends an Ascend-Event packet to the RADIUS accounting server. The packet contains the two new attributes:

- NAS-Identifier(4) containing the identifier for the NAS
- Ascend-Event-Type(150) indicating that the event is a coldstart

Note: The MAX issues an Ascend-Event packet *only* upon startup. Changing the RADIUS accounting server (in the Mod Config>Acct submenu) does not trigger this packet.

Ascend-Event packet structure

Table 9 lists the fields in the packet and their values in an Ascend-Event packet.

Table 9. Ascend-Event packet field values

Field	Value
Code	33 - Ascend Event Request 34 - Ascend-Event-Response (sent on the successful Ascend-Event-Request)
Identifier	Used in matching Ascend-Event-Request and Ascend-Event-Response. Composed of one octet.

Table 9. Ascend-Event packet field values

Field	Value
Length	Indicates the length of the packet including the Code, Identifier, Length, Authenticator, and Attribute fields. Octets outside the range of the Length field should be treated as padding and are ignored on reception. Composed of two octets.
Authenticator	The most significant octet is transmitted first. This value is used to authenticate the messages between the client and the RADIUS accounting server. See the Livingston RADIUS draft for more information. Composed of 16 octets.
Attributes	Variable length field, containing zero or more Attributes. In a coldstart notification package, the attributes will be NAS-Identifier (4) and Ascend-Event-Type (150). The RADIUS accounting server must send back an Ascend-Event-Response with the correct identifier to the NAS.

RADIUS attributes used

Two attributes are used for accounting coldstart notification: a new Ascend-Event-Type attribute and the existing NAS-Identifier attribute.

NAS-Identifier

Description: This attribute identifies the NAS that is sending the Ascend-Event packet to the RADIUS accounting server. The accounting server uses this identifier to match Ascend-Event-Requests and Ascend-Event-Responses.

Usage: The Identifier field is one octet.

Ascend-Event-Type

Description: Ascend-Event-Type defines the coldstart event type.

Usage: Table 10 shows the values of the fields in Ascend-Event-Type:

Table 10. Ascend-Event-Type field values

Field	Value
Type	150
Length	6

Table 10. Ascend-Event-Type field values

Field	Value
String	Composed of four octets. The contain the event type Possible values: 1 Coldstart

OSPF Equal-cost Multipath routing available

Now, a MAX running OSPF alternates between two equal cost gateways. Previously, it only used the first gateway.

When OSPF detects more than one equally good gateway, in terms of routing costs, each equal-cost gateway is put on an equal-cost list. The router will alternate between all the gateways on the list. This is called equal-cost multipath routing.

For example, if a router AA has two equal-cost routes to example.com over the top T1 via router BB or the lower T1 via router CC, the routing table could look like this:

```
AA% ipr sh

Destination        Gateway         IF       Flg   Pref Met     Use     Age
10.174.88.0/25    10.174.88.12    wan2     OGM     10  10      52      19
10.174.88.0/25    10.174.88.13    wan3     OGM     10  10      52      19
10.174.88.12/32   10.174.88.12    wan2     OG      10  10       0      28
10.174.88.13/32   10.174.88.13    wan3     OG      10  10       0      28
192.168.253.0/24   -              ie0      C        0   0       1      49
192.168.253.6/32   -              lo0      CP       0   0      53      49
223.1.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.5.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.12.9.0/24      10.174.88.12   wan2     OG      10  10       0      19
255.255.255.255/32 -              ie0      CP       0   0       0      49
```

Note that the “M” in the Flags column indicates an equal-cost multipath.

A traceroute from AA to example.com would look like this:

```
AA% traceroute -q 10 example.com
traceroute to example.com (10.174.88.1), 30 hops max, 0 byte packets
1  CC.example.com (10.174.88.13)  20 ms BB.example.com (10.174.88.12)  20 ms
CC.example.com (10.174.88.13)  20 ms BB.example.com (10.174.88.12)  20 ms  20
ms CC.example.com (10.174.88.13)  60 ms  20 ms BB.example.com (10.174.88.12)
20 ms CC.example.com (10.174.88.13)  20 ms BB.example.com (10.174.88.12)  20 ms
2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20 ms  20 ms
30 ms  20 ms  30 ms
AA%
```

Note: Notice the alternating replies. The replies are statistically dispatched to BB and CC, with roughly 50% of the packets sent through each gateway.

Defender authentication added

An Ascend unit can now authenticate terminal server users by directly contacting a Digital Pathways Defender authentication server.

This release adds the support for terminal server authentication. If an Ascend unit is configured to use Defender authentication, all authenticated users are given service only according to the parameters of the TServ Options submenu for the Ethernet profile. Figure 5 illustrates a typical Defender set up.

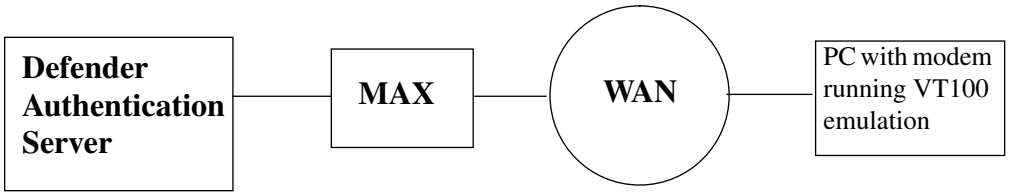


Figure 5. Example Defender set up

Configuring direct Defender authentication

1. Open the Ethernet> Mod Config>Auth menu:
2. Set Auth to the **`Defender`**.
   Auth Host #2 and Auth Host #3 are not applicable, because the Ascend unit can support only one Defender authentication server at this time.
3. Set the value of Auth Port to the TCP port number of the Defender authentication server, usually 2626.
4. Set the value of Auth Key.
   Auth Key is used as a DES secret key shared between the Ascend unit and the Defender authentication server. This key is also used for authentication by the Ascend unit in its role as a Defender authentication agent.
5. Set Auth Timeout to indicate the number of seconds the Ascend unit waits before assuming that the Defender server has become nonfunctional.

```
Edit

90-A00 Mod Config
Auth
Auth=Defender
Auth Host #1=137.175.80.24
Auth Host #2=0.0.0.0
Auth Host #3=0.0.0.0
Auth Port=2626
Auth Timeout=10
Auth Key=****************
Auth Pool=No
APP Server=No
APP Host=N/A
APP Port=N/A
SecurID DES encryption=N/A
SecurID host retries=N/A
SecurID NodeSecret=N/A
```

Logging in with Defender authentication

This section describes the process you would use to dial into an Ascend unit with Auth set to Defender:

1 Dial the number for the Ascend unit.

The banner set up by the Banner parameter appears, similar to:

```
** Ascend Pipeline Terminal Server **
```

The Defender authentication server provides the actual login request. The prompt is configured from the server side, and might appear similar to:

```
Enter ID:
```

2 Enter the ID.

The Defender server provides a numeric challenge and asks for a response from the user. The Defender authentication mechanism includes a Secure Network Key (SNK), a calculator-like device with an LCD display and keyboard. The prompt is provided again by the Defender server:

```
SNK Challenge: 01742975

Enter Response:
```

3 Enter a PIN and press Enter on the SNK keypad followed by the challenge number just displayed, and presses Enter on the keypad again. (In the example above, the challenge is 01742975.)

The SNK displays a response on its LCD screen, for example:

```
Enter Response: 123435678
```

4 Copy this response at the Ascend unit's login prompt.

If you enter the number incorrectly, or if the SNK has been improperly configured, the Defender server displays a message and another prompt for input, for example:

```
Invalid SNK Response

SNK Challenge: 39823805

Enter Response:
```

If you enter the correct response, the approval message is displayed, along with the Ascend prompt:

```
Access Approved

ascend%
```

Terminating a login before authentication completes

A user can break out of the authentication session before authentication has completed, for example, by dropping the dial-up line. In this case, the server still has a record of the user's name.

Retrying a failed login

If a login fails, the user must wait until the server's timeout period has expired. If the user makes an attempt to retry his or her login before the server's timeout period (between 30 and 120 seconds) the following message appears:

```
Your ID is already active on another channel.

Enter ID:
```

After the server's timeout period, the user can attempt to log in again.

Failed login with Defender authentication

When the Ascend unit loses contact with the Defender server, the Ascend unit terminates the TCP session, causing all authentication attempts currently in progress to be terminated on the next user input. Any sessions that are already authenticated remain active.

Subsequent attempts by any user to connect to the Ascend unit with Defender authentication cause the Ascend unit to attempt a connection to the server. If the Ascend unit cannot contact the server, authentication is impossible and all remote authentication attempts that depend on Defender are refused.

SecurID ACE authentication support added

An Ascend unit can now authenticate users by directly contacting a SecurID ACE server. Although SecurID ACE authentication was already indirectly supported via RADIUS, direct support for the SecurID ACE server was needed for two main reasons:

1) For those installations where other RADIUS features are not required, having direct SecurID ACE support on the Ascend unit decreases the complexity of the system, making the system easier to configure and maintain.

2) The SecurID ACE support via RADIUS does not support the "New PIN Mode" feature, which allows a dial-in user to change the personal identifying number (PIN).

Direct SecurID ACE support (using the App Server on the client side) for PPP dial-in users will be implemented in an upcoming release; this release adds the support for terminal server authentication only. Figure 6 illustrates a typical SecurID ACE set up.

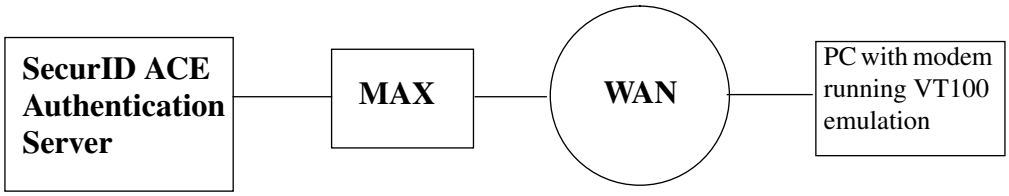


Figure 6. Example SecurID ACE set up

User Interface Changes

The Ethernet>Mod Config>Auth menu has changed to accommodate the new SecurID ACE authentication method. When you use this authentication method, existing parameters are affected in these ways:

- Auth must be set to the new value "SECURID."
- Auth Host #2 and Auth Host #3 are not applicable, because the Ascend unit can support only one SecurID ACE authentication server at this time.
- Auth Key is not applicable.
- Auth Pool is not applicable.
- Auth Port is the TCP port number of the SecurID ACE authentication server, usually 5500.
- Auth Timeout is the number of seconds the Ascend unit waits before assuming that the SecurID ACE server has become nonfunctional.
- Three new parameters have been added. The sections below describe each parameter.

SecurID DES Encryption

Description: This parameter specifies whether the server uses standard DES or the native encryption provided by SecurID.

Usage: You can specify one of these values:

- Yes specifies that the server uses standard DES encryption.
- No specifies that the server uses the native encryption provided by SecurID.

No is the default.

Dependencies: For the SecurID DES Encryption parameter to apply, you must set Auth=SECURID.

Parameter Location: Ethernet Profile: Ethernet/Mod Config/Auth

See Also: SecurID Host Retries, SecurID NodeSecret

SecurID Host Retries

Description: This parameter specifies the number of times the Ascend unit attempts to contact the SecurID host before timing out.

Usage: Specify an integer. The default value is 3.

Dependencies: For the SecurID Host Retries parameter to apply, you must set Auth=SECURID.

Parameter Location: Ethernet Profile: Ethernet/Mod Config/Auth

See Also: SecurID DES Encryption, SecurID NodeSecret

SecurID NodeSecret

Description: On the first successful authentication attempt, the SecurID host informs the Ascend unit of a secret value, theoretically only known to the Ascend unit, to be used in subsequent interactions between the Ascend unit and the SecurID host. This value appears in the SecurID NodeSecret parameter.

Usage: The parameter value is *Secure* unless the LCD user has "Edit System" security privileges. You should set this value to null (its default) before using the Ascend unit to authenticate a user. If you later reset the value of the parameter to null, you must inform the server that the node whose NodeSecret was changed must have its interface re-initialized using the "Client Edit" menu selection in the ACE server's "sdadmin" utility. Then, the server sends a new NodeSecret the next time a user successfully authenticates.

Dependencies: For the SecurID NodeSecret parameter to apply, you must set Auth=SECURID.

Parameter Location: Ethernet Profile: Ethernet/Mod Config/Auth

See Also: SecurID Host Retries, SecurID NodeSecret

Note: If an Ascend unit is configured to use SecurID ACE authentication, all authenticated users are given service only according to the parameters of the TServ Options submenu for the Ethernet profile. There currently is no way to get user-specific configuration information from the SecurID ACE server, except by using RADIUS.

SecurID ACE operation

When Auth=SECURID, the newly dialed-in user is greeted with the familiar banner and prompt:

```
** Ascend Pipeline Terminal Server **

Login:
```

When the user enters a name, the screen prompts for a password, just as for a normal login:

```
Password:
```

At this point, the user must enter his or her PIN, followed by the numbers currently being displayed on the SecurID token card.

Note: Unlike the SecurID ACE support in RADIUS, which ignores the input to "Password:" and asks for a "Passcode," this direct implementation does not take the extra step. The Ascend unit sends the input to the Password prompt to the ACE server as the passcode. If you want the Ascend unit to ask for a passcode, you can change the password prompt using the Password Prompt parameter in the TServ Options submenu of the Ethernet Profile.

If the login is correct, the terminal server prompt appears:

```
ascend%
```

If the login is incorrect, this message appears:

```
** Bad Password
```

The Ascend unit requests another login. This process repeats three times, or until the user enters a valid login name/password (or passcode) combination.

NextCode Mode

If a particular user has three or more consecutive incorrect logins, the server marks that user's token card as being in "NextCode" mode. When the user finally logs in successfully, he or she must enter in an extra passcode from his or her token to verify actual possession of the token card. When the user has sent his or her first correct PIN + passcode to the Ascend unit, this message appears:

```
Wait for the code on your token to change, then enter the new code
(without PIN).

Passcode:
```

The user must then wait until the number displayed on the token card changes, and then type in that number without the PIN. If the user enters a correct code, the terminal server command prompt or menu appears. If the user enters an incorrect code, the Ascend unit displays a "**Bad Password" message and the user's token remains in "NextCode" mode.

New PIN Mode

The ACE server system administrator can place particular tokens in "New PIN" mode. The next time the user successfully authenticates and wants access to the system, he or she must choose a new PIN or allows the server to generate one.

After the normal authentication, the Ascend unit displays one of the following three messages.

1 If the server was configured to allow the user to choose a new PIN or request one from the server, this 5-line message displays:

```
Enter your new PIN, containing 4 to 8 digits:

             or

<Return> to generate a new PIN and display it on the screen:

             or

<Ctrl C> to cancel the New PIN procedure:
```

Note: The number of allowed digits may change according to the server configuration; the server can also be configured to allow alphabetic characters in the PIN, in which case the word "characters" appears in place of "digits" in the first message.

2 If the server was configured to force the user to choose his or her own PIN, this message displays:

```
Enter your new PIN, containing 4 to 8 digits:
```

3 If the server was configured to restrict the user from choosing a PIN, and to always generate a random PIN for the user, this message displays:

```
Press <Return> to generate a new PIN and display it on the screen:
```

User-chosen PIN

In cases 1 and 2, when the user enters a new PIN, the server checks the PIN. If the new PIN has the appropriate number of characters or digits, the Ascend unit asks the user to retype the same PIN for verification:

```
Please re-enter new PIN:
```

The user types in the new PIN. If the PINs match, the new PIN is sent to the server, and the user is informed that the PIN has changed:

```
Wait for the code on your token to change, then log in with the new PIN

Login:
```

If, after the second verifying PIN entry, the Ascend unit sees that the user entered two different PINs, this message appears:

```
PINs do not match. Please try again.

Login:
```

The user must log in again. The server then asks the user to choose a new PIN.

Server-chosen PIN

In cases 1 and 3, when the server generates a PIN for the user, the user simply presses Enter in response to the initial "New PIN" prompt. The server then displays this question:

```
ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE A PIN? (y or n) [n]:
```

If the user presses "y" or "Y", the screen displays a new PIN chosen by the ACE server:

```
Your new PIN: 6467

Press Enter to clear screen:
```

The user must immediately memorize the PIN, and then press Enter. The screen clears, the PIN is sent back to the Ascend unit for confirmation, and if the ACE server accepts the PIN, the Ascend unit displays this message:

```
Wait for the code on your token to change, then log in with the new PIN

Login:
```

Note: Changing your PIN counts as one of the three allowed logins per dialup, so a correct PIN change followed by a login counts as two attempts. Therefore, if you fail twice, you need to redial and connect in order to complete authentication.

DNIS enables TCP between MAX units

Enhanced DNIS support enables ISPs to receive TCP connections instead of switched calls. Using DNIS, a local MAX creates a TCP connection to port 150 on a second MAX. The second MAX handles the TCP call as a modem connection and authenticates the call. The user appears to be connected to the second MAX. This has the advantage of bypassing the telco PSTN. It also has the advantage of concentrating phone calls; for example, if the local MAX

receives two async calls, each of which use 32K of bandwidth, both calls can be handled on one T1/PRI channel. Figure 7 provides an example TCP connection between MAX units.

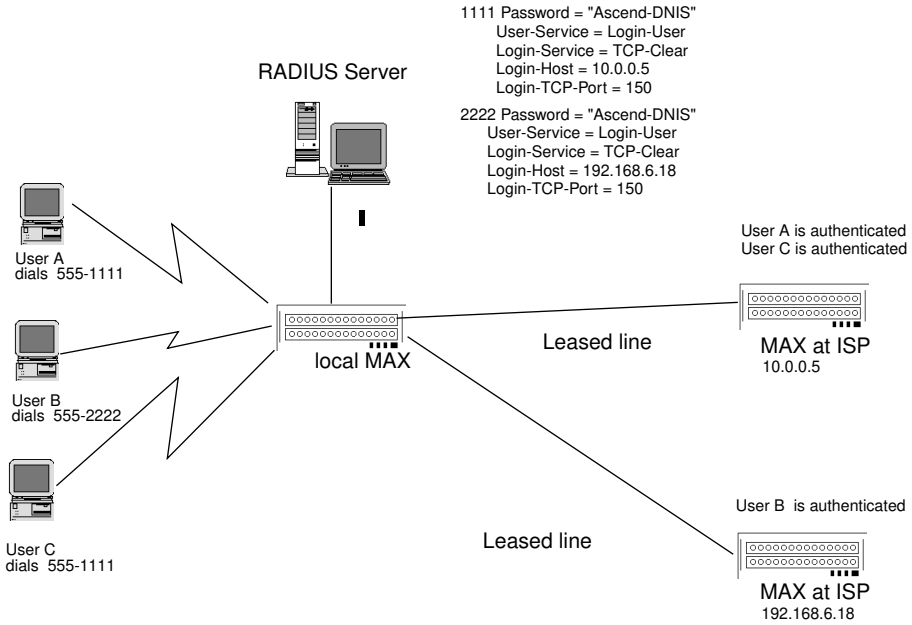


Figure 7. Example TCP connection between MAX units

This feature requires two MAX units (any of the MAX 4000 platforms). One unit is at the telco central site and is configured to use RADIUS authentication. Another unit is at an ISP and is configured with RADIUS or local profiles that authenticate callers and route modem calls to the terminal server.

The first MAX must have RADIUS user entries that specify DNIS and TCP-Clear. This unit uses DNIS to recognize that a TCP connection is required to the second MAX, whose IP address is specified in the Login-Host attribute. This first MAX is simply used to route the call to the MAX at the ISP. For example, this is a sample RADIUS entry that would work:

```
2222 Password = "Ascend-DNIS"
       User-Service = Login-User
       Login-Service = TCP-Clear
       Login-Host = 192.168.6.18
        Login-TCP-Port = 150
```

The following settings are required:

- The number shown in the sample entry as 2222 must be the DNIS number.
- User-Service must be set to Login-User.
- Login-Service must be set to TCP-Clear.
- Login-Host must be set to the IP address of the second MAX.
- Login-TCP-Port must be set to 150.

When this MAX receives a connection with the proper DNIS, it opens a TCP connection to the specified IP address.

The second MAX receives an incoming TCP connection on port 150 and treats that connection like a modem connection. This MAX authenticates the call and routes it to the terminal server interface or handles it as an async PPP session.

Note: The local MAX units must have Connection profiles to the MAX units at the ISP in order to establish a connection.

Terminal server access using the X.75 protocol

Now, you can access the terminal server using the X.75 protocol. Full technical specifications for X.75 can be found in the CCITT Blue Book Recommendation X series 1988.

User interface changes

You can configure the MAX for X.75 protocol by setting five new parameters. The sections that follow describe each parameter.

Frame Length

Description: This parameter sets the maximum number of bytes allowed in the information field by the X.75 TAs (Terminal Adapters) that might call this unit.

Usage: Specify a number between 128 and 2048. The default value is 2048.

Parameter Location: Answer Profile: Ethernet>Answer>X.75 Options

See Also: K Window Size, N2 Retransmission Count, T1 Retransmission Timer, X.75

K Window Size

Description: This parameter establishes the maximum number of data packets that can be outstanding in an X.75 connection before acknowledgment is required.

Usage: Specify a number between 2 and 7. The default is 7.

Parameter Location: Answer Profile: Ethernet>Answer>X.75 Options

See Also: Frame Length, N2 Retransmission Count, T1 Retransmission Timer, X.75

N2 Retransmission Count

Description: This parameter indicates the retry limit—the maximum number of times the MAX can resend a frame on an X.75 connection when the T1 Retransmission Timer expires.

Usage: Specify a number between 2 and 15. The default value is 10. A higher value increases the probability of a correct transfer of data. A lower value allows for quicker detection of a permanent error condition.

Parameter Location: Answer Profile: Ethernet>Answer>X.75 Options

See Also: Frame Length, K Window Size, T1 Retransmission Timer, X.75

T1 Retransmission Timer

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

Usage: Specify a number between 500 and 2000. The default value is 1000 (1 second).

Parameter Location: Answer Profile: Ethernet>Answer>X.75 Options

See Also: Frame Length, K Window Size, N2 Retransmission Count, X.75

X.75

Description: This parameter specifies whether the MAX accepts incoming calls that use X.75 encapsulation.

Usage: You can specify one of these settings:

- Yes indicates that the MAX accepts incoming X.75 calls.
  The default value is Yes.
- No indicates that the MAX does not accept incoming X.75 calls.

Parameter Location: Answer Profile: Ethernet>Answer>Encaps

See Also: Frame Length, K Window Size, N2 Retransmission Count, T1 Retransmission Timer

RADIUS IP Address Allocation

The RADIUS daemon is a database server that provides user profiles to MAX products. The RADIUS database can specify pools of IP addresses that a MAX can use to dynamically allocate IP addresses to incoming callers. Formerly, dynamic IP address allocation to callers was handled by each MAX individually, from a pool of addresses pre-assigned to each MAX. This new feature adds a radipad (RADIUS IP address) daemon that allows MAX units to allocate IP addresses to callers from a global pool of addresses that is shared among many units.

Format of RADIUS global pools

Use the following format to set the Ascend-IP-Global-Pool attribute (146):

```
global-pool-zzz
```

where zzz specifies from which global pool the user gets an IP address. For example, global-pool-9 and global-pool-south are valid settings.

The format of the Ascend-IP-Pool-Definition attribute is a string containing:

```
h.h.h.h n
```

where:

h.h.h.h is the base IP address. This is the first address in a contiguous range of addresses.

n is the number of contiguous addresses formed by simple addition to the base address.

The following is an example of global address pools. This pseudo-user profile appears in the RADIUS users file on the RADIUS authentication server.

```
global-pool-9 Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-IP-Pool-Definition = "10.3.0.1 7",
        Ascend-IP-Pool-Definition = "10.4.0.1 48"
```

The pool in the above example provides a total of 55 host addresses (7 for the first pool plus 48 for the second pool) to those users whose Ascend-IP-Global-Pool attribute has been set to global-pool-9.

Format of the Pseudo-user profiles

In addition to the global pool definitions, the users file on the RADIUS server must contain a pseudo-user profile that defines which host is running radipad as well as which client MAX units are allowed to request IP addresses from global pools:

```
rapida-hosts Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-Assign-IP-Server = "10.12.253.7",
        Ascend-Assign-IP-Client = "10.0.7.18",
        Ascend-Assign-IP-Client = "10.113.0.99"
```

Configuring RADIUS IP address allocation from Global Pools

1. Add the following line to /etc/services on the hosts where the radipad daemon runs. Note that the RADIUS authentication daemon (radiusd) and radipad can be on the same host, or different hosts:

   ```
   radipa    9992/tcp#RADIUS IP address allocation from global pools
   ```

   The port number 9992 is the default. You can change it as required.

2. Install radipad in the same directory as radiusd.

3. Make sure the users file on the RADIUS server contains a “radipa-hosts” pseudo-user profile that defines which host is running radipad as well as which client MAX units are allowed to request IP addresses from global pools

```
rapida-hosts Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-Assign-IP-Server = "10.12.253.7",
        Ascend-Assign-IP-Client = "10.0.7.18",
        Ascend-Assign-IP-Client = "10.113.0.99"
```

4. Define the global address pool.

   For example:

   ```
   global-pool-zzz Password = “ascend”, User-Service = Dialout-Framed-
   User
           Ascend-IP-Pool-Definition = “10.3.0.1 7",
           Ascend-IP-Pool-Definition = “10.4.0.1 48"
   ```

   Note: For more information see the file users.example.

5. Modify your startup scripts (for example, /etc/rc.local for Sun OS 4.1.x) to start radipad when the system comes up. For example:

   ```
    #
   # Start up radipad for remote users
   #
   ```

```
if [ -f /usr/local/bin/radipad ]; then
        /usr/local/bin/radipad; echo -n ' radipad'
fi
```

Only one host on the network should run radipad. Radipad is the central manger for global IP address pools on a network and is not designed to be replicated.

6 For each user profile that will be getting an IP address from a global pool, set the Ascend-IP-Global-Pool (146) attribute.

For example:

```
Jane Smith Password = "mz9", User-Service = Framed-Protocol
    Framed-Protocol=PPP
    Ascend-Assign-IP-Global-Pool = "global-pool-zzz"
    ...
```

7 Start radipad manually the first time. To do this you must be root.

New RADIUS attributes

These attributes now appear in the RADIUS dictionary:

- Ascend-Assign-IP-Client (144)
- Ascend-Assign-IP-Server (145)
- Ascend-Assign-IP-Global-Pool (146)

Each attribute is described in the sections that follow.

Ascend-Assign-IP-Client (144)

Description: This attribute can appear in the pseudo-user profile "radipa-hosts" and specifies the IP address of an Ascend unit that can use global IP pools.

The radiusd daemon reads "radipa-hosts" prior to connecting to radipad.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

You can specify multiple instances of this attribute; at present, the list of radipad client units generated is unused. In the future, the attribute might be used to implement a recovery mechanism in which radipad starts up and polls every client asking for a complete accounting of global pool-allocated addresses it holds. If no Ascend-Assign-IP-Client attribute is present, the list of client units defaults to those present in the RADIUS clients file.

Ascend-Assign-IP-Server (145)

Description: This attribute appears in the pseudo-user profile "radipa-hosts" and specifies the IP address of the host containing radipad. The radiusd daemon reads "radipa-hosts" prior to connecting to radipad.

Note: Ascend-Assign-IP-Server must be present and must contain a valid IP address for radipad to operate.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. Only one instance of this attribute should appear in the profile. The default value is a place-holder only; you must specify a valid IP address for radipad to work.

Ascend-Assign-IP-Global-Pool (146)

Description: This attribute appears in a RADIUS user profile, and specifies that the Ascend unit should allocate an IP address to the calling device from a global IP pool.

Usage: Specify the name of the pseudo-user profile containing global IP pool definitions. The definitions are specified by the Ascend-IP-Pool-Definition attribute. You can specify multiple instances of Ascend-Assign-IP-Global-Pool. The Ascend unit tries to allocate an address from the pools in order, and chooses an address from the pool with the first available IP address.

X.25 support for reverse charge request

This new feature enables you to configure a Connection Profile to request reverse charge through the X.25 facility field. This feature is provided for situations in which you do not wish the user to type the request reverse charge string at the PAD prompt, or in which the user is in immediate PAD mode and therefore cannot type the string.

New Reverse Charge parameter

Reverse Charge

Description: This parameter specifies whether the X.25 facility field indicates "reverse charge request" when the X.25 user calls a host.

Usage: You can specify either Yes or No.

- Yes specifies that the X.25 facility field indicates "reverse charge request." This setting is equivalent to the user typing fac 0101 at the PAD prompt.
- No specifies that the X.25 facility field does not indicate "reverse charge request". The default value is No.

Parameter Location: Connection Profile: Connections/Any Connection Profile/Encaps Options/X.25 Prof

Show system version command added

A show revision command has been added to the terminal server command line options for the show command.

The Show Revisions command

The show revision command displays system type and version information for the system currently running on the MAX, including:

- system name
- build name
- release number of the loaded software

For example, typing

```
show revision
```

at the command line prompt would display information similar to:

```
MAX system revision: mhpt1bip 4.6Bp10
```

HELP for Show command includes show revision

You can display a list of the options available for the show command. When you request help for the show command by typing

```
show ?
```

at the command line, the list of options that appears now includes the new Show system revision command:

```
show revision       Display system revision.
```

Additional information for system resets now provided

The fatal error log now details the reason for a system reset and no longer describes a reset as a fatal error. Normal OSPF exits (those due to OSPF not being configured) are no longer entered in the fatal error log.

Reset descriptions

Previously, the fatal error log listed system resets as fatal errors, rather than resets, and did not give a reason for the reset. The fatal error log now lists a reset specifically as a reset and gives the reason for the reset.

Example: Reset from an NVRAM command

For example, if you use the debugger's NVRAMCLEAR command to reset a unit, you would see something like the following:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:31:19
        NVRAMCLEAR Reset from unknown in security profile 1.
OPERATOR RESET:  Index: 99   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:32:23
        NVRAM was rebuilt
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Example: RESET from the debugger

If you use the debugger RESET command, you might see the following:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
```

```
        Date: 08/04/1996.       Time: 22:32:23
        DEBUG Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Example: Reset from Sys Reset

If you select Sys Reset from the Sys Diag submenu of the System profile, you might see the following:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:32:23
        MENU Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Example: Reset from MIF

If you select Use MIF from the Sys Diag menu and reset from MIF, you might see the following:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:32:23
        MIF Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Exceptions to how messages appear

If only one message is allowed in NVRAM, the "SYSTEM IS UP" message will not appear. This applies to all Ascend units that support only one message in NVRAM, such as the 25 with a 0273 or 0269-002 board. On the 25 with an 0265 or 0269-001 board, none of these messages can be displayed.

CLID authentication can return User Busy

You can now configure CLID authentication failures to return User Busy. Two different conditions can be returned in the DISCONNECT message.

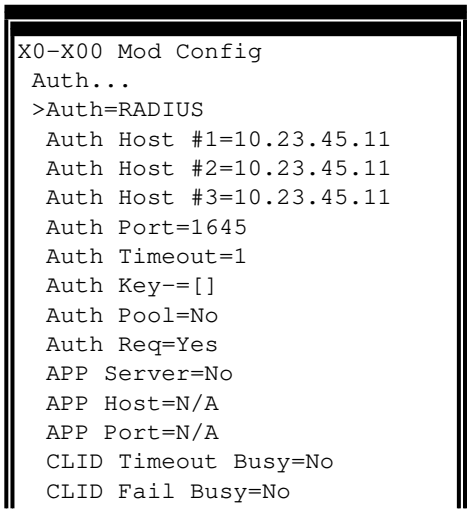
When Caller ID authentication fails in an ISDN connection, the MAX sends a DISCONNECT message. The Cause Element in the DISCONNECT message can give an idea of why the CLID authentication failed.

You can specify two values as the Cause Element value in ISDN DISCONNECT packets:

Cause Element	Description
CLID Timeout Busy	The CLID Timeout Busy specifies whether to return User Busy when Caller ID authentication fails due to a Radius timeout. The default value for CLID Timeout Busy is No (Normal Call Clearing). **Note:** This field is `N/A` if `Auth=None` or `Auth=TACACS` in the same profile.
CLID Fail Busy	CLID Fail Busy specifies whether to return User Busy when Caller ID authentication fails for reasons other than a RADIUS timeout. The default value for CLID Fail Busy is No (Normal Call Clearing). You can choose the value for this field regardless of the Server setting, since the occurrence of this failure does not depend upon using a RADIUS server.

Setting the DISCONNECT Cause value

Select the DISCONNECT Cause value in the Auth submenu of the MAX Ethernet Profile:



Ascend SNMP MIB additions

Two new disconnect codes have been added to the values for **eventDisconnectReason** OBJECT-TYPE (eventEntry 15) in the Ascend SNMP MIB:

Value	Description
clid_auth_serv_timeout (5)	Indicates that the RADIUS server, could not be reached and the MAX is configured to require `auth` failure.
clid_auth_failed (4)	Indicates that the CLID value did not match `a profile.`

User-defined message for assigned IP address

A field has been added to the Ethernet>Mod Config>TServ submenu that allows you to define a message that indicates the IP address the terminal server has assigned. This message appears when a you select PPP from the terminal server prompt, or any time a PPP connection is made from the terminal server.

Specifying a IP address assignment message

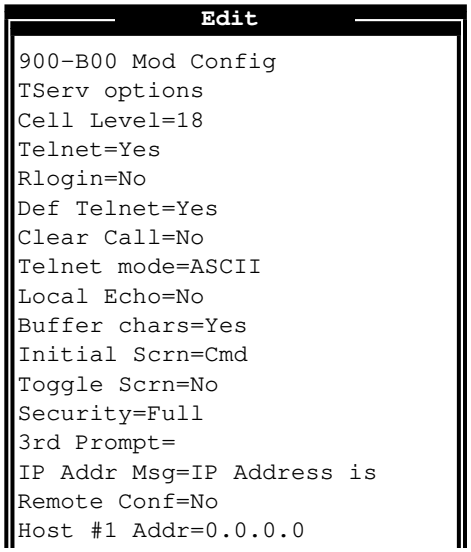
Previously, you could not modify or specify the message, which was always “IP address is x.x.x.x.” With the new field, you can specify a character string of up to 64 characters. For example, you might want to modify the message to read “Your IP address is:x.x.x.x”.

You can now specify the message that appears at the beginning of a PPP session telling the terminal server user what IP address has been assigned to the session. To do so, define a message in the Ethernet>Mod Config>TServ submenu.

Note: The IP Addr Msg field will be N/A if TS Enabled=No or PPP=No.

To set the IP address notification message:

1 Open the Ethernet>Mod Config>TServ submenu.



2 Select IP Addr Msg and type the message (up to a maximum of 64 characters) that you want to appear in the message indicating the IP address assigned.

The message you type will appear before the IP address, with no space between what you have typed and the IP address. For example, if you type

```
You have been assigned this IP address:
```

The message appears on the terminal screen as:

```
You have been assigned this IP address:x.x.x.x
```

3 Close the Ethernet>Mod Config>TServ submenu.

Debug command to change MAX modem strings

This feature adds a debug command that allows administrator's to change the AT command strings on the MAX digital modems.

A new debug command has been added to all MAX products that support digital modems. This command allows you to modify the digital modem's default AT command strings.

Caution: Changing AT command strings should only be done by experienced engineers familiar with modem technology.

1 Enter the debug mode by quickly typing:

```
Esc [ Esc =
```

or pressing Ctrl-D, then selecting D=Diagnostics.

2 At the ">" prompt type:

```
mdbstr [ 0 | 1 | 2 ] AT string
```

where

- 0 deletes any user-defined command strings and causes the modem to revert to the original command string.
- 1 overrides the internal first portion of the AT command with the specified AT command.

– 2 overrides the internal second portion of the AT command with the specified AT command.

Typing `mdbstr` without any arguments prints out the user-defined command strings (if any).

To exit the debug mode and return to the VT-100 interface, type `quit`.

Ascend Session Events sent in RADIUS-LOGOUT mode

Ascend units can now report the number of sessions by Class to a RADIUS authentication server using RADIUS -LOGOUT. Previously, this report could only be sent to a RADIUS accounting server using RADIUS-ACCOUNTING.

Previously MAX units reported the number of sessions by Class to the RADIUS Accounting server by sending an Ascend-Event(33) packet type with one or more Ascend-Number-Sessions(202) attribute(s) at a user-defined interval. This functionality is now available using RADIUS-LOGOUT to send the same type of packets to a RADIUS authentication server.

The packets are sent to the first Authentication Host in the Auth submenu at a user-defined interval. The MAX retries until the limit is reached or the Authentication Server sends a correct Event-Response. If the retry limit is exceeded then the Session Event is sent to the second Auth Host and so on. The Session Event is discarded after the MAX has attempted and failed to send the packet to all hosts in the Auth submenu.

Configuring RADIUS-LOGOUT mode session events reporting

The Sess Timer field has been added to the RADIUS Authentication submenu of Mod Config:

```
40-900 Mod Config...
 Auth...
  Auth=RADIUS/LOGOUT
  Auth Host #1=0.0.0.0
  Auth Host #1=0.0.0.0
  Auth Host #1=0.0.0.0
  Auth Port=
  Auth Timeout=1
  Auth Key=
    . . .
  Sess Timer=0
```

The numeric value in seconds in the Sess Timer field specifies the interval at which session reports will be sent. The maximum is 65535.The default is 0, which means that no Session Events will be sent. For example, if you wish the MAX to send Session Events at one-minute (60-second) intervals, set Auth to RADIUS/LOGOUT and Sess Timer to 60.

The Sess Timer field will be N/A if Auth= is not set to RADIUS/LOGOUT.

Ascend-Event packet

The Ascend-Event packet contains the session events information. The attributes sent with the version that goes to a RADIUS authentication server (the RADIUS/LOGOUT version) is slightly different from the version of the packet sent to a RADIUS accounting server, as shown in Table 11.

Table 11. Attributes sent with RADIUS/LOGOUT

	Value or Description
Password(2)	well-known password of "event"
NAS-Identifier(4)	identifier of the NAS that is sending the Session Event packet
Ascend-Event-Type(150)	value of Ascend-Session-Event
Ascend-Number-Sessions(202)	the number of active sessions

Ascend-Event packet structure

Table 12 lists the fields in the Ascend-Event packet and their values in an Ascend-Event packet.

Table 12. Ascend-Event packet field values

Field	**Value**
Code	33 - Ascend Event Request 34 - Ascend-Event-Response (sent on the successful Ascend-Event-Request)
Identifier	Used in matching Ascend-Event-Request and Ascend-Event-Response. Composed of one octet.
Length	Indicates the length of the packet including the Code, Identifier, Length, Authenticator, and Attribute fields. Octets outside the range of the Length field should be treated as padding and are ignored on reception. Composed of two octets.

Table 12. Ascend-Event packet field values

Field	Value
Authenticator	The most significant octet is transmitted first. This value is used to authenticate the messages between the client and the RADIUS accounting server. See the Livingston RADIUS draft for more information. Composed of 16 octets. **Note:** The authenticator method is different between the RADIUS accounting and authentication. This is due to using the Password as part of the Authentication authenticator.
Attributes	Variable length field, containing zero or more Attributes. If Auth=RADIUS/LOGOUT and a number greater than 0 is specified for the Sess Timer field, one of the attributes will be Ascend-Number-Sessions(202).

Ascend-Number-Sessions

Description: Ascend-Number-Sessions is a RADIUS Attribute to indicate the number of active sessions per Class a RADIUS client has. Each Attribute contains information for 1 Class/session pair. This information is then sent from the Ascend client to the RADIUS Authentication server in a Ascend-Event packet type.

Note: A session may have multiple connections. Each connection is counted.

Usage: Table 13 shows the fields in Ascend-Number-Sessions.

Table 13. Ascend-Number-Sessions field values

Field	Value
Type	202
Length	Less than or equal to 6. Length of the attribute including the type, length, value, and the length of Class. Sessions that do not have a Class have a length of 6. If there are no sessions the value of this field is 0.
String	The number of sessions that are up per Class. This is not a readable ASCII string. It is the numeric number of sessions for the Class

Table 13. Ascend-Number-Sessions field values

Field	Value
Class	The Class string

Ascend Event-Type values

Ascend-Event-Type(150) is an Attribute that describes the type of event. It is an integer with the possible values:

- Ascend-Coldstart(1)
- Ascend-Session-Event(2)

Example 1

For example, to send an Ascend-Number-Session attribute (in a Session Event packet) to the RADIUS authentication server at one-minute intervals, assuming there are three classes of users:

- Class 1 has 3 sessions,
- Class 2 has 4 sessions
- Class 3 has 1 session

The steps below outline what happens:

1 In the Auth submenu of the Mod Config menu, you set Sess Timer=60

2 The Ascend client sends a Ascend-Event-Request Packet with:

- Password
- NAS-Identifier
- Ascend-Event-Type
- the three Ascend-Number-Sessions Attributes
- no class with 0 sessions
- class 1 with 3 sessions, class 2 with 4, class 3 with 1

3 The RADIUS Authentication server sends back an Ascend-Event-Response packet.

Example 2

To send an Ascend-Number-Sessions attribute to the RADIUS authentication server at one-minute intervals, assuming there are no active connections:

1 In the Auth submenu of the Mod Config menu, you set Sess Timer=60

2 The Ascend client sends a Ascend-Event-Request Packet with:

- Password
- NAS-Identifier
- Ascend-Event-Type
- one Ascend-Number-Sessions Attributes (the number of sessions is 0)

3 The RADIUS Authentication server will send back an Ascend-Event-Response packet.

Define RIP-v2 values in RADIUS dictionary

The RADIUS daemon is a database server that provides user profiles to MAX products. RADIUS uses the Framed-Routing attribute to indicate whether the user sends RIP (Routing Information Protocol) packets, receives RIP packets, or both. Formerly, only the RIP version 1 values were specified; this release adds the RIP version 2 settings for the attribute.

New Framed-Routing description

Framed-Routing (10)

Description: This attribute specifies RIP (Routing Information Protocol) behavior for the user profile.

Usage: You can specify one of these values:

- None indicates that the MAX does not send or receive RIP updates.

None is the default. Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables. If you turn off RIP, the MAX does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX must rely on static routes specified in a pseudo-user profile.

- Broadcast indicates that the MAX sends RIP version 1 updates, but does not receive them.
- Listen indicates that the MAX receives RIP version 1 updates, but does not send them.
- Broadcast-Listen indicates that the MAX both sends and receives RIP version 1 updates.
- Broadcast-v2 indicates that the MAX sends RIP version 2 updates, but does not receive them.
- Listen-v2 indicates that the MAX receives RIP version 2 updates, but does not send them.
- Broadcast-Listen-v2 indicates that the MAX both sends and receives RIP version 2 updates.

Dependencies: If RIP is enabled to both send and receive RIP updates on the WAN interface, the MAX broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

DNS list size increased

You can allow up to 35 DNS list addresses. The number of DNS addresses listed for terminal server logins was previously limited to six. You can configure a number of addresses up to 35, which is the maximum supported by BSD.

The new List parameters

If the DNS system is set up to return lists of host addresses in response to a query, the List Attempt parameter enables a terminal server user to attempt a login to one entry in the DNS list

of hosts, and if that connection fails, to try the next entry, and so on. This helps to avoid tearing down physical links when a host is unavailable, which is especially important for immediate services such as immediate telnet or rlogin.

The new List Size parameter specifies a number of addresses that will be listed. The maximum number is 35. To use this feature, the List Attempt feature must be enabled, as shown below:

```
Edit
90-900 Mod Config
DNS...
>Domain Name=abc.com
 Pri DNS=10.2.3.4
 Sec DNS=0.0.0.0
 Pri WINS=0.0.0.0
 Sec WINS=0.0.0.0
 List Attempt=Yes
 List Size=6
```

This is the new List Size parameter:

Location	Parameters with example values
Ethernet, Mod Config/DNS... (Ethernet Profile)	List Size=6

List Size

Description: This parameter specifies a number of DNS addresses that will be made accessible to terminal server users in response to a DNS query. The maximum is 35 because BSD has a limit of 35.

Usage: Press Enter to open a text field, and then specify a number between 0 and 35. The default value is 6.

Dependencies: This parameter is N/A if the List Attempt feature is disabled.

Parameter Location: Ethernet, Mod Config/DNS...

See Also: List Attempt

Flexible RADIUS user pools

Prior to this release, when you set the Ascend-Assign-IP-Pool (218) attribute to 0, users would get an IP address from the last defined IP address pool. Now, when you set this attribute to 0, users will get an IP address from any pool.

Terminal server login timeout added

This feature adds options for configuring the timeout value for inactivity at a login prompt. Previously the MAX waited five minutes before disconnecting the call.

How it works

Users will be disconnected if they have not completed logging in when the number of seconds set in the Login Timeout field has elapsed. A user has the total number of seconds indicated in the Login Timeout field to attempt a successful login. This means that the timer begins when the login prompt appears on the terminal server screen, and continues (is not reset) when the user makes unsuccessful login attempts.

Configuring the login timeout value

The new configuration option is in the TServe submenu of the Ethernet Configuration profile:

1. Open the Ethernet profile.
2. Open the TServ Options submenu.
3. Select Login Timeout= and enter a value.
   This value can be an integer between 0 and 300 seconds. The default value is 300 seconds.
4. Close the Ethernet Profile.

Profile- or User-level DNS servers

IP address for the Domain name servers can now be set for an individual Ascend client in the IP Connection profile. Previously, the two DNS server addresses that were configured on the MAX were given to all users during IPCP negotiation.

This feature allows you to specify the IP addresses for 2 DNS servers that a user/profile can obtain during IPCP negotiations. If DNS servers are not specified for the profile or for the user, the MAX hands out the IP addresses for the two DNS servers for which it is configured. This allows you to assign specific DNS servers to “outside” users, for example, while setting a different default for “inside” users.

When negotiating DNS information to a user through PPP options, the MAX checks to see whether a DNS profile is defined in the Connection profile. If DNS information is specified at the profile level, that information is passed to the user.

If a DNS profile is not defined, the MAX checks to see if at the user level in the Ethernet profile. If the DNS information is defined in the Ethernet profile, the MAX passes that information to the user.

If no DNS information is defined either at the Connection or Ethernet profile level, the MAX passes the default DNS information defined for the MAX if the Allow As Client DNS=Yes.

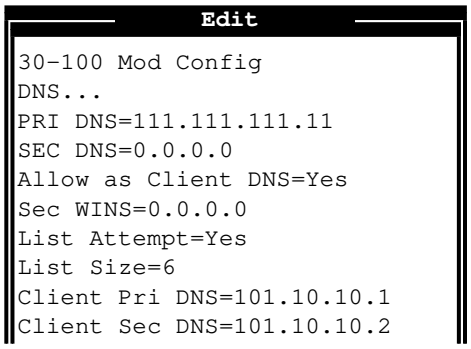
Note: There is no Radius support for this field.

You can also prevent the default MAX-level DNS information from being sent to a user when all other IPCP DNS negotiation fails.

Configuring DNS servers in the Ethernet profile

To configure user-level DNS servers in the Ethernet profile:

1 Open the Ethernet>Mod Config>DNS menu.



2 Set the PRI DNS and SEC DNS as the MAX-level defaults.

3 Select a value for Allow As Client DNS.

Allow As Client DNS is a boolean value which controls whether MAX DNS info should be passed to users if the default and profile level DNS info are not defined. The default for this field is Yes to permit backward compatibility. Select Allow As Client DNS=No to avoid sending MAX level DNS Info to user when all other IPCP DNS negotiation fails.

4 Select values for Sec WINS, List Attempt, and List Size as usual (refer to the documentation that came with your MAX).

5 Type the IP address of primary DNS server for this profile in the Client Pri DNS field.

This address will be passed to a user if the per user level DNS server is not defined. It is assumed as not defined if set to 0.0.0.0.

6 Type the IP address of secondary DNS server for all profile in the Client Pri DNS field.Client Sec DNS:

This is the IP address of secondary DNS server for all profile and it will be passed to a user if the per user level DNS server is not defined. It is assumed as not defined if set to 0.0.0.0.

Note: There is no Radius support for this field.

Configuring DNS servers in the Connection profile

To configure DNS servers in the Connection profile:

1 Open the IP submenu of the Connection profile.

```
Edit
30-100 Connections
IP Options...
LAN Adrs=0.0.0.0/0
WAN Adrs=0.0.0.0
IP Adrs=0.0.0.0/0
Metric=7
Preference=100
Private=No
RIP=Off
Pool=0
Multicast Client=No
Multicast Rate Limit=5
Client Pri DNS=111.11.11.1
Client Sec DNS=111.11.11.2
Client Assign DNS=Yes
```

2 Type the IP address of the primary DNS server for this profile in the Client Pri DNS field.

This is the IP address that will be passed to the user when logged in using a profile. It is supported in Radius with attribute Ascend-Client-Primary-DNS and is considered not defined if set to 0.0.0.0.

3 Type the IP address of the secondary DNS server for this profile in the Client Sec DNS field.

This is the second IP address that will be passed to the user when logged in using profile. It is supported in Radius with attribute Ascend-Client-Secondary-DNS and is assumed as not defined if set to 0.0.0.0.

4 Select Yes or No for Client Assign DNS.

This value controls whether DNS information should be passed to the user or not. The default is Yes.

It is supported through Radius as Ascend-Client-Assign-DNS and can be set to DNS-Assign-No or DNS-Assign-Yes. If it is not set in Radius, the value is assumed to be Yes.

Fixed interfaces appear first in SNMP IfTable

Fixed interfaces, such as ports or lines on the motherboard, now appear at the top of the SNMP IfTable before software entities. Previously, fixed interfaces appeared below software interfaces in the IfTable.

Organization of IfTable

Fixed entities, such as hardware entities, now appear in the IfTable before software entities. As removable interfaces are added, they appear after the fixed interfaces in the IfTable.

This ensures that interface numbers remain relatively fixed with the addition of slot cards. Also, since IfNumber is referenced in many places in the MIB, this change helps to make other tables appear more consistent than previously.

For example, on a MAX 4000 with a Net/BRI card the interface table would look something like this:

```
1. console
2. T1 line 1 slot 1
3. T1 line 2 slot 1
4. T1 line 1 slot 2
5. T1 line 2 slot 2
6. Serial WAN
7. Net/BRI line 1
8. Net/BRI line 2
.
.
.
13. Net/BRI line 8
14. Ethernet port
15. wan0 - wan??
16. loopback
17. atmp??
18. rj0
19. bh0
```

In the example above, interfaces 1-14 correspond to hardware/physical entities, while 15-19 correspond to software interfaces. 15 is associated with Ethernet and digital modem-related interfaces. 16-19 are software interfaces.

Units with no removable interfaces

Units with no removable interface slots might also see an ordering change of the interface. The new order will be as above.

Previously, the order was:

```
1. Ethernet
2. wan0-wan>>
3. loopback
4. atmp
5. rj0
6. console
7. T1 line 1 slot 1
8. T1 line 2 slot 1
9. T1 line 1 slot 2
10. T1 line 2 slot 2
11. Serial WAN
12. Net/BRI line 1
13. Net/BRI line 2
```

Note: If the cards in a unit do not move, the interfaces in the MIB should not move either. Only the MAX 4000, MAX 2000, and MAX 1800 have removable slot cards.

Compatibility with MIB

This change should be compatible with previous MIB releases, since they are static information. This change does not require any change to the structure of information that the MIB imposes.

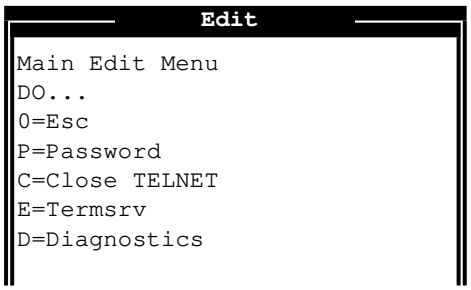
Terminal server and diagnostic functions

Termsrv and Diagnostics options have been added to the Do menu. Previously, these functions could be not be accessed through the menu interface.

Accessing the new parameters

Two menu items, E=Termsrv and D=Diagnostics, were added to the Do menu. The permissions set in a user's profile determine whether these options are available to that user.

To display the DO menu, press Ctrl-D:



Accessing the terminal server in other menus

For all MAX and Pipeline models except the Pipeline 25 models, the DO E option in the Main Edit DO menu has the same function as the Term Serv option in the Sys Diag menu.

In the Pipeline 25-FX, the DO E option in the Main Edit DO menu has exactly the same function as the Cmd Mode option in the Sys Diag menu.

Accessing the terminal server using keystrokes

You can also use the following keystroke sequence (Escape key, left square bracket, Escape key, zero) on a Pipeline to access the Terminal Server

<Esc> [<Esc> 0

Note: This keystroke sequence does not apply to the Pipeline 25PX.

Support for OSPF in MIB II

Ascend MAX products that support OSPF now support SNMP MIB II support for OSPF (Group 13). For more information refer to RFC 1253. OSPF support for MIB II does not include SNMP SET of OSPF tables or virtual interfaces for point-to-point links without an IP address.

OSPF can advertise a static route

A MAX running OSPF can now advertise routes to external destinations on behalf of another gateway (a “third-party”). This is commonly known as advertising a forwarding address.

Previously, the MAX advertised itself as the forwarding address to the external destination. When the third-party feature is enabled, the MAX advertises the IP address of another gateway.

Depending on the exact topology of the network, it may be possible for other routers to use this type of LSA and route directly to the forwarding address without involving the advertising MAX, increasing the total network throughput.

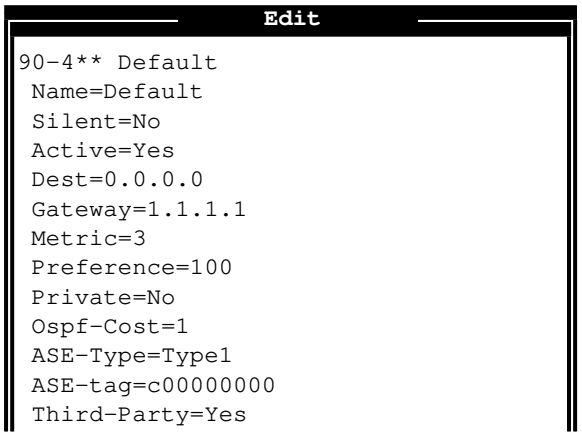
This feature can only be used if all OSPF routers know how to route to the forwarding address. This will usually mean that the forwarding address must

- be on an Ethernet that has an OSPF router acting as the forwarding router
- that designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding address LSAs

Configuring OSPF to advertise a static route

To configure a static route for OSPF to advertise a “third-party” gateway:

1. Open the static route you want to use to advertise a forwarding address using the Ethernet > Static Rtes > *static route profile* menu.
2. Set Third-Party to Yes.
3. Set the Gateway to the forwarding address.



Debug option to display unwanted dial-outs packets

Display packets as an aid to writing filters. A new debug option captures and displays packets that cause the Ascend unit to dial out when a connection is not needed. You can then get the information you need to write a filter that prevents the packet from bringing up a connection.

This enhancement adds the wan-data dial-out (wdDialout) option to the debug monitor. This option enables you to display a packet that caused an unwanted dial-out session.

When packets are not captured

If a dial-out is initiated for any of the following reasons, the wdDialout option does *not* capture a packet:

- Dial-out caused by the Ctrl-D user command
- Dial-out caused by callback security
- Dial-out on nailed channels
- Dial-out caused by NAT (Network Access Translation) acquiring an IP address
- Dial-out initiated for IP over X.25, when the X.25 internet profile changes to active and there is data waiting for X.25 to bring up the connection
- Dial-out caused by IGMP (Internet Group Management Protocol) multicast forwarding
- Dial-out to acquire a DNS address during PPP negotiations
- Dial-out in response to a DHCP Discover message
- Dial-out caused by the Ascend unit sending a DHCP packet for DHCP client processing
- Dial-out caused in response to an APP (Ascend Password Protocol) Connect Request message

Turning on the debug option

1 Enter the debug mode by quickly typing:
Esc [Esc =
or press Control-D and select D=Diagnostic.

2 At the ">" prompt type:

```
help ascend
```

you should see the wdDialout option listed. By default, the option is turned off.

3 To turn the option on, type:

```
wdDialout
```

```
WANDATA dialout display is ON
```

This is a toggle command. Typing it again turns the option off. See the next section for details on how packets are displayed in the debug monitor.

4 To exit the debug mode and return to the VT-100 interface, type quit.

Displaying packets

You can view wdDialout displays in the debug monitor. This section shows several examples.

Example 1

In the following example, the Ascend unit's time and date have not been explicitly set, either by user command or SNTP server. So, the date and time in the captured packet is invalid. The phone number dialed on receipt of this packet is 92233002.

```
  Date: 01/01/1990.          Time: 00:00:53
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 42 octets @ 2C6950
  [0000]: ff ff ff ff ff ff 00 c0 7b 61 44 fe 08 06 00 01
  [0010]: 08 00 06 04 00 01 00 c0 7b 61 44 fe cc b2 d7 7b
  [0020]: 00 00 00 00 00 00 cc b2 d7 13

  [0000]: ff ff ff ff ff ff 00 80 c7 5b e9 5b 08 06 00 01
  [0010]: 08 00 06 04 00 01 00 80 c7 5b e9 5b cc b2 d7 13
  [0020]: 00 00 00 00 00 00 cc b2 d7 16 00 00 00 00 00 00
  [0030]: 00 00 00 00 00 00 00 00 00 00 00 00
```

The type OLD-STYLE-PADDED means that the packet has a 14-byte MAC (Ethernet) header + datagram (ARP request message). The packet contents provide the following information:

```
destination MAC address   ff:ff:ff:ff:ff:ff
source MAC address        00:c0:7b:61:44:fe   /* 123 */
arp packet type           08:06
arp_hrd                   00:01               /* Ethernet 1 */
arp_prot                  08:00               /* IP=0x800 */
arp_hlen                  06                  /* hlen = 6 */
arp_plen                  04                  /* plen = 4 */
arp_op                 00:01             /* arp operation ARP_REQ
*/
arp_sha                   00:c0:7b:61:44:fe   /* 123 */
arp_spa                   cc:b2:d7:7b         /* 123 */
arp_tha                   00:00:00:00:00:00
arp_tpa                   cc:b2:d7:13         /* 19 */
```

Example 2

In this example, the phone number dialed on receipt of this packet is 92233002. The type OLD-STYLE-PADDED means that the packet has a 14-byte MAC (Ethernet) header + datagram. This is a broadcast IP RWHO message.

```
  Date: 01/01/1990.  Time: 00:00:56
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 198 octets @ 296810
  [0000]: ff ff ff ff ff ff 00 80 c7 5b e9 5b 08 00 45 00
  [0010]: 00 b8 0d c3 00 00 3f 11 24 fa cc b2 d7 13 cc b2
  [0020]: d7 ff 02 01 02 01 00 a4 e5 8a 01 01 00 00 32 46
  [0030]: 5e 26 00 00 00 00 63 6d 61 72 69 6e 65 72 00 00
  [0040]: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  [0050]: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  [0060]: 00 00 32 46 4a e3 74 74 79 63 32 00 00 00 72 79
  [0070]: 75 00 00 00 00 00 32 46 4b 35 00 00 02 59 74 74
  [0080]: 79 63 33 00 00 00 72 79 75 00 00 00 00 00 32 46
  [0090]: 4b 39 00 00 00 3d 74 74 79 63 34 00 00 00 72 79
  [00a0]: 75 00 00 00 00 00 32 46 4b 3e 00 00 00 97 74 74
  [00b0]: 79 70 30 00 00 00 72 79 75 00 00 00 00 00 32 46
  [00c0]: 5e 00 00 00 00 01
```

The packet contents provide the following information:

```
destination MAC address   ff:ff:ff:ff:ff:ff
source MAC address        00:80:c7:5b:e9:5b
source IP adddress        cc:b2:d7:13       /* 204.178.215.19 */
destination IP address    cc:b2:d7:ff       /* 204.178.215.255 sub-
network broadcast */
```

Example 3

In this example, the phone number dialed on receipt of this packet is 92233002. The type OLD-STYLE-PADDED means that the packet has a 14-byte MAC header + datagram. This is a unicast IP ICMP echo packet message.

```
  Date: 01/01/1990.     Time: 00:01:13
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 98 octets @ 291EC8
  [0000]: 08 00 20 1f 5b ce 00 80 c7 5b e9 5b 08 00 45 00
  [0010]: 00 54 0e 09 00 00 ff 01 66 10 cc b2 d7 13 cc b2
  [0020]: d7 16 08 00 f5 1b bb 07 98 00 37 5e 46 32 3a 48
  [0030]: 0d 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
  [0040]: 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
  [0050]: 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
  [0060]: 36 37
```

The packet contents provide the following information:

```
destination MAC address   08:00:20:1f:5b:ce
source MAC address        00:80:c7:5b:e9:5b
source IP address        cc:b2:d7:13       /* 204.178.215.19 */
destination IP address    cc:b2:d7:ff       /* 204.178.215.22 */
```

Example 4

In this example, the phone number dialed on receipt of this packet is 917007337921. Note that there is no MAC header. This is an IPX packet: a Get Nearest Server Request with service type File Server (0004).

```
  Date: 01/01/1990.        Time: 00:01:43
Cause an attempt to place call to 917007337921
WD_DIALOUT_DISP: chunk 261022 type IPX.
: 34 octets @ 2C6AA0
  [0000]: ff ff 00 22 00 11 00 00 00 00 ff ff ff ff ff ff
  [0010]: 04 52 00 00 00 00 00 a0 24 be d5 84 40 09 00 03
  [0020]: 00 04
```

The packet contents provide the following information:

```
chksum            ff:ff
packet len        00:22              /* 34 */
Transport Control 00                 /* 0 */
packet type       11                 /* 17 NetWare Core Protocol
Packet */
dest network      00:00:00:00
dest Node         ff:ff:ff:ff:ff:ff
dest Socket       04:52             /* Service Advertising Protocol
(SAP Packet)*/
source network    00:00:00:00:00
source Node       00:a0:24:be:d5:84  /* physical address of source
Node */
Source Socket     40:09              /*4000h-7fffh Dynamic socket*/
Sap operation     00:03             /* Get Nearest Server Request */
Sap Service Type  0:04                /* File Server */
```

Example 5

In this example, the phone number dialed on receipt of this packet is 92233002. The type OLD-STYLE-PADDED means that the packet has a 14-byte MAC header + datagram.

```
  Date: 01/01/1990.  Time: 02:40:35
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 60 octets @ 2AE950
  [0000]: 00 80 5f 74 93 d5 00 80 c7 2f 32 4c 00 2a ff ff
  [0010]: 00 29 00 11 30 6c 6b 00 00 00 00 00 00 01 04 51
  [0020]: 82 c1 b6 bf 00 80 c7 2f 32 4c 40 03 22 22 3f 03
  [0030]: 01 00 16 00 02 15 01 ff ff ff ff ff
```

The packet contents provide the following information:

```
destination MAC address   00:80:5f:74:93:d5
source MAC address        00:80:c7:2f:32:4c
chksum            ff:ff
packet len        00:29              /* 41 */
packet type       11                 /* 17 NetWare Core Protocol
Packet */
dest network      30:6c:6b:00
dest Node         00:00:00:00:00:01
dest Socket       04:51              /* NetWare Core Protocol (NCP
Packet)*/
source network    82:c1:b6:bf
```

```
source Node       00:80:c7:2f:32:4c  /* physical address of source
Node */
Source Socket     40:03              /*4000h-7fffh Dynamic socket*/
```

Add template feature in Name/Passwords profile

This feature adds a new parameter that allows you to specify which Connection Profile to use as a template. Previously, the Name/Password profiles always used the Answer Profile as a template.

How it works

This change works in two different ways depending on the Template Connection # specified in the Name/Password Profile, depending upon which profiles are active.

- A Name/Password Profile that uses a Connection profile template is active if *both* of the following are true:
  - the Active flag is set to Yes in the Name/Password Profile
  - the Active flag is set to Yes in the Connection Profile

Note: The Answer Profile is always active (always has the Active flag set to Yes).

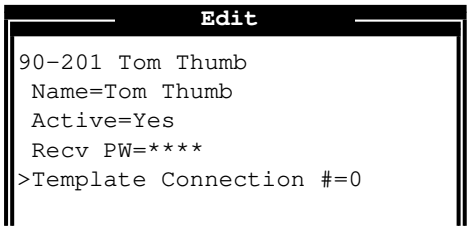
For example, you may set up a Connection Profile for the Sales group to use when dialing in, then set up a Name/Password Profile for each individual salesperson. You can prevent a user (or users) from dialing in using one of the two following methods:

- De-activate the Name/Password profile for a single salesperson to prevent that salesperson from dialing in by setting the Name/Password Active flag for the user's profile to No.
- De-activate the entire Sales group (by setting the Connection Profile Active flag for the Sales group to No).

Configuring a Name/Password template

1 Open the Names/Passwords menu.

The new Template Connection # parameter appears on the Name/Password Profile screen.



2 Set the value for Template Connection #.

- Use the default, Template Connection=#0 (the Answer profile), to specify that the Name/Password Profile will work as it always has.

  This mode supports clients dialing in over PPP and ARA, but does not support a router dialing in.

– Specify a profile number between 1 and 31 to use the Connection Profile to which the number refers.

  In this mode the Name/Password Profile functions as an alias for the Connection Profile.

3 Make sure Active=Yes.

Connection Profile call time limit

You can now specify the maximum duration of an incoming call. Previously there was no limit on an incoming call duration.

Configuring a maximum call duration

You can set the maximum duration of an incoming call in the Connection profile (in the Session Options submenu) and in the Answer Profile. To do this, specify a value for the Max Call Duration parameter in the appropriate profile (some calls are handled by their own Connection Profile, and some are handled by the Answer Profile for the duration of the call).

You can specify any value from 1-1440 minutes. The connection is checked once per minute, so the actual time of the call will be slightly longer (usually less than a minute longer) than the actual time you set.

The default is Max Call Duration=0. This means that incoming calls will not be timed and can be of unlimited duration.

New RADIUS field added

Ascend-Maximum-Call-Duration will be added to the RADIUS dictionary. It will be an integer with a value between 1 and 1440. The new RADIUS field, Ascend-Maximum-Call-Duration, is the equivalent of Max Call Duration in the local profile.

Note: Ascend-Maximum-Call-Duration applies only to incoming calls and will not affect dialout profiles.

Increase dial-out digits to 24

The maximum phone number length has been increased to 24 digits.

The following phone number fields are now 24 digits:

- Ethernet > Connections > *any profile* > Dial #
- Ethernet > Connections > *any profile* > Telco Options > Bill #
- Ethernet > Mod Config > WAN Options > Ans 1#
- Ethernet > Mod Config > WAN Options > Ans 2#
- Ethernet > Mod Config > WAN Options > Ans 3#
- Ethernet > Mod Config > WAN Options > Ans 4#
- Host/Dual > Port# Menu > Directory > *any profile* > Dial #

- Host/Dual > Port# Menu > Directory > *any profile* > Bill #
- Host/Dual > Port# Menu > Port Config > Ans 1#
- Host/Dual > Port# Menu > Port Config > Ans 2#
- Host/Dual > Port# Menu > Port Config > Ans 3#
- Host/Dual > Port# Menu > Port Config > Ans 4#
- System > Destinations > *any profile* > Dial 1#
- System > Destinations > *any profile* > Dial 2#
- System > Destinations > *any profile* > Dial 3#
- System > Destinations > *any profile* > Dial 4#
- System > Destinations > *any profile* > Dial 5#
- System > Destinations > *any profile* > Dial 6#

BACP support over MP added

Support for Bandwidth Allocation Control Protocol (BACP) has been added.BACP is the Internet standard equivalent to Ascend Multilink Protocol Plus (MP+). All platforms that support MP+ will also support BACP.

How BACP works

BACP is the Internet standard protocol equivalent to the Ascend MP+ bandwidth allocation schema that runs over MP and enables a unit from any vendor supporting MP to add or remove bandwidth based upon demand. BACP functions similarly to MP+ and uses the same menu items as for MP+. Since BACP does not support Idle Percent and this field is always N/A for MP, the Idle Percent field has been removed from the Encaps submenu of the Ethernet Connections profile.

Configuring BACP

To configure an Ascend unit to use BACP for sending or receiving, set the BACP= parameters for the Connections and Answer profiles as in Table 14.

Table 14. BACP configuration parameters

Purpose	Parameter Value	Location	Description
Send	BACP=Yes	Encaps submenu of the Ethernet Connections profile.	Enables BACP for sending. BACP=NO is the default. **Note:** The Idle Percent field has been removed from this menu since it is always N/A for MP and is not supported by BACP.

Table 14. BACP configuration parameters

Purpose	Parameter Value	Location	Description
Receive	BACP=Yes	PPP Options submenu of the Answer Profile.	Enables BACP for receiving. BACP=NO is the default.

RADIUS changes

A new attribute, Ascend-BACP-Enable, has been added to the RADIUS dictionary. See Table 15 for a description.

Note: This attribute is valid only if the framed protocol is MP.

Table 15. Ascend-BACP-Enable

Attribute Name	Ascend-BACP-Enable
Type	Value
Description	Possible attribute values: BACP--Yes enables BACP functionality for the current connection profile. BACP-No disables BACP functionality. BACP-No is the default value.

MS-CHAP support

Support for the Microsoft - Challenge Handshake Authentication Protocol (MS-CHAP) format supported by Windows NT systems has been added to all Ascend platforms except the Pipeline 25.

How it works

You can now configure an Ascend unit to send or receive MS-CHAP authentication. MS_CHAP authentication is described in detail at Microsoft's Web site:

`ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt`

Note: The 4.6Donly MS-CHAP format Ascend units support is the Windows NT version, DES and MD4 encryption. An Ascend unit can authenticate a Windows NT system and a Windows NT system can authenticate an Ascend unit.

Configuring an Ascend unit for MS-CHAP authentication

The options available for the Recv Auth parameters in the PPP Options submenu of the Answer Profile have been changed. Recv Auth=Either now enables the Ascend unit to authenticate using any of the authentication protocols (PAP, CHAP, or MS-CHAP) when communicating with Windows NT systems.

To configure an Ascend unit to authenticate using MS-CHAP, select one of the following options for Recv Auth shown in Table 16.

Table 16. MS-CHAP Receive Authentication

Value for Recv Auth=	Description
Either	The Ascend unit will allow authentication if the remote peer can authenticate using any of the designated authentication schemes.
MS-CHAP	The Ascend unit will allow authentication only if the remote peer uses MS-CHAP for authentication.

To configure an Ascend unit to send MS-CHAP authentication, select Send Auth=MS-CHAP in the Encaps options submenu of the Connection Profile. With this option selected, the Ascend unit will only continue authentication if the remote peer also supports MS-CHAP authentication.

Special handling for packetizing data from modems

We can now provide a way to control the manner in which we packetize data received from our modems. The data can be accumulated for a maximum number of milliseconds or a minimum number of bytes before being passed up to the encapsulation layer. Two new parameters have been implemented to facilitate this feature.

Special Handling

If you have a very specialized application, you can now finetune the exchange of packets between the MAX and host when working with packets received from remote modems. Two new parameters in the TServ Options menu of the Ethernet Profile enable packetization control: Packet Wait Time and Packet Characters. Each new parameter is explained in the sections that follow.

Packet Wait time

Description: This parameter specifies the maximum amount of time in milliseconds that any received data can wait before being passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 600 milliseconds. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to take into account your modem speeds when calculating its value.

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

See Also: Packet Characters

Packet characters

Description: This parameter specifies the minimum number of bytes of received data that should accumulate before the data is passed up the protocol stack for encapsulation.

Usage: Specify an integer between 0 and 500. The default value is 0 (zero).

Dependencies: If your application is so specialized that it demands you use this parameter, be sure to set the Packet Wait Time parameter to an appropriate value.

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

See Also: Packet Wait Time

Multicast tree monitoring added

This feature adds a mechanism that allows the MAX to monitor whether it is able to receive multicast packets at its Internet interface. It also provides quick feedback to network operations if the MAX fails to receive regularly scheduled multicast traffic ("heartbeat" packets) on a specified multicast group address.

Monitoring multicast traffic

When the MAX is a member of a multicast group address, multicast packets should continually arrive at the MAX and can be forwarded immediately to a dialup client. The MAX can now monitor whether it can receive heartbeat packets at its Internet interface, and provides notification when the MAX fails to receive regularly scheduled multicast traffic.

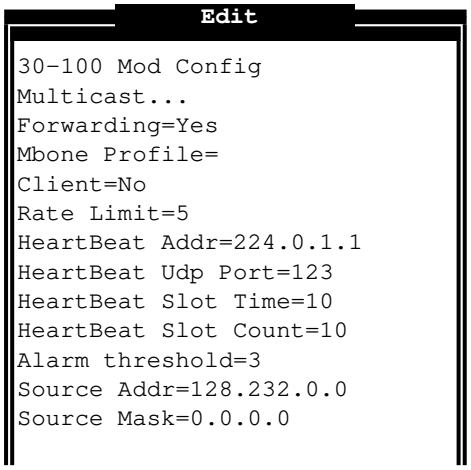
Checking the multicast heartbeat

The MAX will poll for heartbeat packets at the interval specified in Heartbeat Slot Time. Each time it polls, the MAX will add the number of heartbeat packets present to a running total. After the number of polls indicated in the Heartbeat Slot Count are completed, the MAX compares the total number of heartbeat packets received to the Alarm Threshold. If the total received is less than the Alarm Threshold, the MAX will start sending an SNMP alarm.

Note: There is no RADIUS support for this feature.

Configuring multicast monitoring

The Multicast submenu has been added to the Configuration profile. The parameters necessary for configuring the multicast tree monitoring feature are grouped under this submenu:



The possible values for the parameters in the Multicast submenu are described in the following table.

Table 17. Multicast submenu parameters

Parameter	Description
Forwarding	Select Forwarding=Yes. This is the same parameter as Multicast Forwarding in the Configuration profile.
Mbone Profile	This is the same as Mbone Profile in the Configuration profile.
Client	Select Client=No. This is same as Multicast Client in the Configuration profile
Rate Limit	Select Rate Limit=5. This is same as Multicast Rate Limit in the Configuration profile.
HeartBeat Addr	A multicast IP address. The MAX joins this multicast group to monitor heartbeat packets.
HeartBeat Udp Port	A UDP port number. The MAX accepts heartbeat packets addressed to this port and the multicast address specified above. If HeartBeat Udp Port=0, the MAX does not use the port for accepting heartbeat packets.
HeartBeat Slot Time	The time in seconds for the interval at the end of which the MAX will look for the presence of heartbeat packets. For example, if Heartbeat Slot Time=10, the MAX will check for heartbeat packets every 10 seconds.

Table 17. Multicast submenu parameters

Parameter	Description
HeartBeat Slot Count	An integer indicating number of times to poll the for heartbeat packets. For example, if Heartbeat Slot Time=10 and Heartbeat Slot Count=10, the MAX will poll every 10 seconds for a total of 10 times, or 100 seconds total elapsed time. At the end of the last poll, the MAX compares the total number of heartbeat packets received and compares that total to the Alarm Threshold.
Alarm threshold	An integer indicating the number of heartbeat packets expected in samples. If the number of packets received is less than Alarm threshold value, an SNMP alarm is sent (SNMP trap added for multicast tree heartbeat, below).
Source Addr	IP address used to filter heartbeat packets from unwanted sources. If this field is not defined (is zero) the filter is not applied, and will allow any source to send heartbeat packets.
Source Mask	Mask used to filter heartbeat packets from unwanted sources.

SNMP trap added for multicast tree heartbeat

A new SNMP trap has been added indicating that the number of heartbeat packets received is less than the Alarm threshold set in the Multicast submenu (see Alarm threshold, in Table 17).

Trap type:TRAP_ENTERPRISE

Code:TRAP_MULTICAST_TREE_BROKEN (19)

Arguments:

1) Multicast group address being monitored (4 bytes),

2) Source address of last heartbeat packet received (4 bytes)

3) Slot time interval configured in seconds (4 bytes),

4) Number of slots configured (4 bytes).

5) Total number of heartbeat packets received before the MAX started sending SNMP Alarms (4 bytes).

Change to SHOW commands

In the `show igmp groups` command, the addresses that the heartbeat monitoring feature listens to are marked with * meaning that this address is joined by local application.

DEBUGGING support

In the standard debug screen, there is a debug command `heartbeat` to debug heartbeat.

Auth TS Secure added

This feature enables you to configure the MAX using RADIUS authentication to accept a remote dial-in call to the terminal server or to drop the call if a Login-Host was not specified in the RADIUS users file. Previously, the MAX always dropped the call if no Login-Host was specified.

How it works

Previously, the MAX dropped the call when the RADIUS user file included Login-Service=TCP-Clear or Login-Service=Telnet and no Login Host was specified.

This feature adds an Auth TS Secure option that enables you to configure the MAX either to accept the call and allow access to the terminal server or to drop the call, regardless of whether a Login Host is specified in the RADIUS users file.

Note: This feature does not apply to PPP encapsulated calls, since the MAX does not accept dial-in PPP calls with the Login Service set to either Telnet or TCP-Clear.

Configuring Auth TS Secure

1. Make sure that the Login Service attribute in the RADIUS user file specifies either TCP-Clear or Telnet.
2. In the Auth submenu of the Ethernet Profile, set Auth=RADIUS or Auth=RADIUS/LOGOUT.

   For other Auth types, the Auth TS Secure option is N/A.
3. Set Auth TS Secure= to Yes or No, as shown in Table 18.

Table 18. Auth TS Secure options

Option	Description
Yes (the default).	Remote Dalian callers will be dropped if Login-Service = TCP-Clear or Login-Service = Telnet and Login-Host is not specified in the RADIUS users file.

Table 18. Auth TS Secure options

Option	Description
No	Remote Dalian callers will not be dropped if Login-Host is not specified in the RADIUS users file, but will be allowed access to the terminal server.

MAX authentication of calls via serial AIM ports

You can now specify a password for calls placed across the Host serial inverse multiplexing ports. Previously, all such calls did not undergo any form of authentication.

This feature allows you to configure a password in the Call profile for outgoing calls and in the Port configuration profile for incoming calls. Two new parameters have been added:

- Call Password in the Call profile (Host/Dual (or Host/6) >Port N Menu>Directory> *any Call profile*).
- Port Password in the Port profile (Host/Dual (or Host/6) >Port N Menu>Port Config).

Authentication is used only if the receiving unit has a password defined in the Port profile. If the Port profile in the receiving unit doesn't have a password defined, the units connect without authentication even though the originating unit may have sent parameters. Note that the MAX only authenticates AIM and BONDING calls; dual-port calls are not authenticated.

Upon initial connection of the first channel, the originating unit passes the Call profile a password to the authenticating unit. The authenticating unit compares the password received with that stored in the Port configuration profile. If the password received matches the stored password, the session is established normally for the remainder of the call. If there is no match, the authenticating unit sends a message back to the originator and drops the session. The port status screen will indicate that the call failed authentication.

Configuring serial port passwords

For you to configure a serial (Port or Call) password, your Security profile must have Edit System=Yes.

To set the passwords, do the following:

1. For outgoing AIM or BONDING calls, enter the DBA call password at Call Password in the Host/Dual (or Host/6) >Port N Menu>Directory> *any Call profile*.
2. For incoming AIM and BONDING calls, enter the Port password at Port Password in Host/Dual (or Host/6) >Port N Menu>Port Config (the Port profile).

Authentication failure status display

If a DBA call fails authentication the caller's Message Log (in the path Host>Dual>portname>Message Log) reflects the error as shown:

```
61-200  time
>M30  Line    Ch
 Password Mismatch
```

Parameter reference

Two new parameters have been added for password protecting AIM and BONDING calls. This section explains the new parameters.

Call Password

Description: This specifies the password for outgoing AIM or BONDING calls. Authentication is used only if the receiving unit has a password defined in the Port profile. If the Port profile in the receiving unit doesn't have a password defined, the units connect without authentication even though the originating unit may have sent parameters. Note that the MAX only authenticates AIM and BONDING calls; dual-port calls are not authenticated.

Usage: Enter a password of nine characters or less.

Parameter Location: Host/Dual (or Host/6) >Port N Menu>Directory> *any Call profile*

See Also: Port Password

Port Password

Description: This specifies the password for incoming AIM or BONDING calls. Authentication is used only if the calling unit has a password defined in the Call profile. If the Call profile in the calling unit doesn't have a password defined, the units connect without authentication even though the originating unit may have sent parameters. Note that the MAX only authenticates AIM and BONDING calls; dual-port calls are not authenticated.

Usage: Enter a password of nine characters or less.

Parameter Location: Host/Dual (or Host/6 >Port N Menu>Port Config

See Also: Call Password

Name/Password profile includes terminal server users

Name/Password profiles are now recognized for terminal server authentication. Previously this profile was recognized only by PPP authentication.

Using the Simple Name/Password profile

This feature supports authenticating with the name and password from Simple Name/Password profiles when connecting to the terminal server. When a terminal server user included in the Names/Passwords profile list attempts to connect, the MAX uses a profile constructed of the Answer Profile with name and password from the Name/Password profile (the result is just as if the user had a full connection profile with all settings equal to what is in the Answer profile).

Configuring a Simple Name/Password profile

There are no changes to the user interface itself. To use Name/Password profile authentication for terminal server users you can now add these users to the Name/Passwords profile list in the same way you add other users.

Address expansion of RADIUS Server Clients list

When the MAX performs RADIUS server functions, it maintains a list of clients that are allowed to make RADIUS requests. The client address list has been expanded to support a range of addresses instead of a single client IP address. Previously, a maximum of three clients with one common secret key was supported.

Client addresses changes

The number of client addresses has been increased to nine entries. In addition, the client address has been expanded to support a range of addresses instead of a single client IP address (Table 19). This means the addresses given will consist of a 32-bit value and a netmask. The number of secret (Server Key) has been changed from one key over all to one key per IP address (Table 20).

For example:

Table 19. Client IP address ranges

Entry	Description
Client #1= 125.65.5.0/24	Client #1 would be any addresses from 125.65.5 subnet.
Client #2= 125.5.0.0/16	Client #2 would be any addresses from 125.5 subnet.
Client #3= 135.50.248.76/32	Client #3 would be the single address for 138.50.248.76.
Client #4= 198.5.248.76/29	Client #4 would be the single address from 198.5.248.72 subnet.

The number of secrets (Server Key) has also been changed from one key overall to one key per address entry. For example:

Table 20. Server Keys assigned to Clients

Entry	Server Key	Description
Client #1= 125.65.5.0/ 24	Server Key #1=bob	Client#1 will allow any host in the 125.65.5.0 net.
Client #2= 125.5.0.0/16	Server Key #2=bob	Client#2 will allow any host in the 125.5.0.0 net.
Client #3= 135.50.248.76/32	Server Key #3=sue	Client#3 will allow only 1 host, 135.50.248.76.

Table 20. Server Keys assigned to Clients

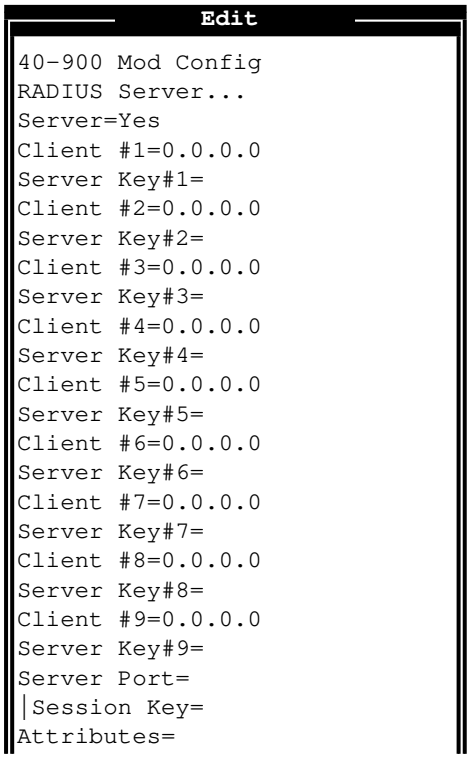
Entry	Server Key	Description
Client #4= 198.5.248.76/29	Server Key #4=george	Client#4 will allow hosts in the 198.5.248.72 net. (198.5.248.73-198.5.248.78)

Note: Client#1 and Client#2 share the same secret.

Configuring RADIUS server clients

To configure RADIUS server clients:

1 Open the RADIUS Server... submenu in the Ethernet profile.



2 Specify the parameter values as defined above and in Table 21.

Table 21. RADIUS server client parameters

Entry	Values	Description
Server	Yes - enables function No - disables function	An option that toggles the RADIUS server functionality on and off.

Table 21. RADIUS server client parameters

Entry	Values	Description
Client #n	The format of the address is a.b.c.d[/x] where a.b.c.d is the IP address and /x is for the optional mask bits. This field is N/A if Server=No	The address or range of addresses. **Note:** If no mask bits are supplied, the software supplies default ones.
Server Key #n	String up to 20 characters. This field is N/A if Server=No.	Secret required for Client #n. Restoring a configuration with old clients requires manual configuration. See Restoring configurations with the new Client list from a backup in this note for more information.
Server Port	UDP port number. This field is N/A if Server=No.	UDP port number for receiving the RADIUS requests.
Session Key	Yes or No. This field is N/A if Server=No.	Indicates whether the MAX should generate a unique session key per connection.
Attributes	Any - (default) match by IP address, name, session id, or session key. Session - match by Session key only. All - match by all applicable values. This field is N/A if Server=No.	Indicates what type of keys are required for matching RADIUS requests with sessions.

Restoring configurations with the new Client list from a backup

The RADIUS Server submenu used to consist of 3 clients (specific host addresses) and 1 Server Key for all 3 clients. If the MAX supports the new RADIUS Server, the restoration of the MAX configuration will cause a problem because the new RADIUS Server allows up to 9 addresses (host or net) and a Server Key for each address. When you restore configurations with the old Client Address list, the netmask assigned to the clients will be the default netmask of the address type given (ex: 128.50.1.1 will get a netmask of 16) and not the previous 32-bit

(i.e. single host) address. In addition, the Server Key will not automatically be set. You must set the Server Key manually for each client in the RADIUS Server submenu.

Forward multicast trace packets

This feature allows multicast clients to MTRACE (multicast trace) the path taken by multicast traffic. The MAX can now pass IGMP MTRACE packets from multicast clients to Mbone and MTRACE RESPONSE packets back to clients from MBone. Previously, a MAX user or other MBONE router user could not use MTRACE on multicast connections to Pipelines.

DBA RADIUS attribute names changed

This change gives the values used by the Ascend-DBA-Monitor attribute a set of unique names based upon the attribute name to eliminate any conflicts. Previously, a conflict in the RADIUS value None caused the Framed-Routing attribute, when configured as None, to use the value of 2, which means Listen, instead of zero when sending profile information to the MAX.

How it works

The normal mode of an MPP call is for both sides of the MPP session to monitor the transmit data from their own perspectives and add or delete bandwidth based on the results of that monitoring. This is called Dynamic Bandwidth Allocation (DBA). In an earlier release, the option to choose which side should add or delete bandwidth was added in the Connection profile.

RADIUS uses the Ascend-DBA-Monitor attribute to indicate which direction(s), if any, should be monitored. When the Ascend-DBA-Monitor attribute was added to the RADIUS dictionary three valid values were defined for the new attribute:

- Transmit
- Transmit-Recv
- None

The value name None was already in use by other attributes, but with a value different from that used by Ascend-DBA-Monitor. Since RADIUS value names are global (shared among all the entries in the RADIUS dictionary) the value of None was changed for all attributes that use it.

This caused the attribute Framed-Routing, when assigned the value of None in the RADIUS server, to use the numeric value 2 (Listen) instead of 0.

RADIUS dictionary changes

The three values for the Ascend-DBA-Monitor have been renamed to be unique, as shown in Table 22:

Table 22. New values for VALUE

Type	Attribute	New Name	Old Name	Value

Table 22. New values for VALUE

VALUE	Ascend-DBA-Monitor	DBA-Transmit	Transmit	0
VALUE	Ascend-DBA-Monitor	DBA-Transmit-Recv	Transmit-Recv	1
VALUE	Ascend-DBA-Monitor	DBA-None	None	2

Checksum validation and redownload for 12MOD

The MAX now downloads the 12MOD modem code, waits for the modems to checksum the downloaded code, and then verifies the checksum matches before continuing with AT POST. Previously, the MAX downloaded the modem code and immediately commence with AT POST. This feature helps to reduce the POST failure rates for the MOD12 cards.

New download process

The 12MOD digital modem slot card boots every time the MAX is power-cycled, and requires boot-up configuration data from the MAX. This feature change means the MAX makes two further attempts to download the code for the MAX's MOD12 digital 12-modem slot card if the first boot-up fails.

Previously, the MAX downloaded the required code and immediately commenced with AT POST (which sends the string "AT" to each modem and waits for the modem to respond with "OK"). Now the MAX downloads the modem code, waits for the modems to checksum the downloaded code, and then verifies that the checksum matches before continuing. If the checksum does not match, the MAX will download the code again, up to 2 more times.

If the checksum still doesn't match after three download attempts, the MAX will fail the entire slot card.

There are no user interface changes and no configuration required to implement this change. The only change in operation that you might notice is that the unit may take slightly longer (~30 secs) to complete POST depending on how many redownloads are performed.

Specifying default routes on a per-user basis

You can now specify a default route on a per-user basis in a Connection Profile or a RADIUS user profile. If an operator is using a particular service, you can cause the Ascend unit to send traffic to the router that service uses, even if the router is not the default gateway shown in the system-wide routing table.

Overview

If you specify a default route in a Connection Profile or RADIUS user profile, the Ascend unit routes IP packets in this way:

1. The Ascend unit consults its routing table to find a next-hop address.
2. If the next hop is the default route for the system (destination 0.0.0.0), the Ascend unit uses the per-user default address as a next hop instead of the system-wide default route.

The unit also uses the per-user default if the normal routing logic fails to find a route and there is no system-wide default route.

This feature applies to routing all packets received on an interface using a given profile, regardless of the specific IP source address; therefore, you can use this feature when the profile belongs to another access router and all hosts behind that router use the default gateway. While all packets arriving on the interface using the given profile are affected, the MAX unit handles packets from other users or from the Ethernet normally. In addition, this feature does not alter the global routing table.

MAX configuration interface changes

To configure a per-user route in the MAX configuration interface, you must set the Client Gateway parameter in the IP Options menu of the Connection Profile.

Client Gateway

Description: This parameter specifies the default route for IP packets coming from the user on this connection.

Usage: Specify the IP address of the next hop router in dotted decimal notation. The default value is 0.0.0.0; if you accept this value, the Ascend unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

The Ascend unit must have a direct route to the address you specify; the direct route can take place via a profile or an Ethernet connection. If the Ascend unit does not have a direct route, it drops the packets on the connection. When you diagnose routing problems with a profile using this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

Example: If you specify Client Gateway=10.0.0.3 in the profile "Berkeley," IP packets from the user with destinations through the default route will be routed through the gateway at 10.0.0.3.

Parameter Location: Connection Profile: Ethernet>Connections>Any Connection Profile>IP Options

RADIUS changes

To configure a per-user route in RADIUS, you must set the Ascend-Client-Gateway attribute in a RADIUS user profile.

Ascend-Client-Gateway (132)

Description: The attribute specifies the default route for IP packets coming from the user on this connection.

Usage: Specify the IP address of the next hop router in dotted decimal notation. The default value is 0.0.0.0; if you accept this value, the Ascend unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

The Ascend unit must have a direct route to the address you specify; the direct route can take place via a profile or an Ethernet connection. If the Ascend unit does not have a direct route, it drops the packets on the connection. When you diagnose routing problems with a profile using this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

Example: If you specify Client Gateway=10.0.0.3 in the profile "Berkeley," IP packets from the user with destinations through the default route will be routed through the gateway at 10.0.0.3.

MAXDial support for Microsoft Fax added

Support for Microsoft Fax has been added to MAXDial with this release. Previously, there was no way to set Microsoft Fax to use hardware flow control (which was required). This release includes utilities to allow the use of Microsoft Fax with MAXDial.

Configuring Microsoft Fax for use with MAXDial

Configuring Microsoft Fax for to work with MAXDial is different on the MAX 200Plus, which uses a PCMCIA modem, and bigger MAX units, which use Ascend modems. This note includes procedures for both types of configurations, as follows:

- Changes affecting the MAX 200Plus
- Changes affecting the MAX 1800, MAX 2000, and MAX 4000

Changes to the files included in the release

The files FIXMSFAX.EXE and MDMASCN2.INF (Ascend digital modem definition file) have been added to the release to allow all MAX users to configure Microsoft Fax for use with MAXDial.

Configuring Microsoft Fax on the MAX 200Plus

You must use the utility in FIXMSFAX.EXE to set up Microsoft Fax correctly. The MAXDial README.TXT file has been updated to describe this process. On the MAX 200Plus, the configuration is not done at install time and is thus not covered in the installation help file. Perform the following procedure after you have correctly installed the MAXDial software.

1 Make sure Microsoft Fax is installed on your computer.
Microsoft Fax is installed as part of Microsoft Exchange under Windows 95.

2 Start Microsoft Exchange by double-clicking on the Inbox icon in the Windows 95 desktop.

3 Click on Settings, and then click on Fax Settings in Microsoft Exchange.

4 Select the Modem page of the Microsoft Fax properties notebook.

5 Select the Modem page of the notebook, then select the Properties page for your modem.

6 On the Modem Properties page for your modem, click Advanced.

7 Enable the Use Class 2 if available setting.

8 Exit Microsoft Fax.

9 Restart Microsoft Fax and immediately exit again.

10 Finally, start Microsoft Fax again.
This ensures that Microsoft Fax is fully configured to use the modem.

11 After Microsoft Fax starts up (which may take some time), run the FIXMSFAX utility from a Windows 95 DOS command prompt.

This alters the modem setup strings used by Microsoft Fax to include the required hardware flow control command.

Note: If you do not follow the above procedure for running FIXMSFAX (including exiting and restarting Microsoft Fax twice), FIXMSFAX may report errors regarding missing registry entries. This occurs when Microsoft Fax has not fully configured itself to use a modem. If you see such error messages, fax operation may be impaired.

Configuring Microsoft Fax with MAX units other than the MAX 200Plus

You must use the Ascend digital modem type when you install MAXDial. This automatically configures Microsoft Fax to operate in hardware flow control mode, with no further user interaction required. Since the MAXDial installation coach help file helps you correctly set up the modem when using MAX 4000, MAX 2000, MAX 1800.

Defining an Ascend digital modem for the serial port

1. Pull down Start>Settings>Control Panel and click Modems to start the Modems control panel.
2. At the first screen, select Add.

   A dialog box appears saying “Windows will try to detect your modem...”.

   If you are using a portable computer, Windows may present a screen offering a choice between PCMCIA modems and Other. If this appears, select Other and click Next; otherwise go on to the next step.
3. Click on the checkbox labelled “Don’t detect my modem. I will select it from a list” and then click Next.

   A list of modem manufacturers appears.
4. Click on the Have Disk button.
5. Insert the MAXDial 32 installation disk into any drive.
6. Enter the drive letter if it differs from the default shown and click OK.
7. Select Ascend digital modem from the list of models that appears (this should be the only choice) and click Next.
8. Select the MAXDial port you are configuring from the list of ports that appears and click Next.
9. Click Finish when the dialog box saying “Your modem has been set up successfully...” appears.
10. Pull down Start>Shut Down>Restart the computer and select Yes.

Multi-line terminal server prompt

You can now configure a terminal server prompt of up to 80 characters and consisting of more than one line. Previously, the prompt could only consist of one line and was limited to 15 characters.

How it works

The Login Prompt parameter specifies the prompt the terminal server displays when asking the user for his or her login name. To specify a multi-line prompt, you can now use two special character combinations that are interpreted as a carriage return/line feed and a tab. These character combinations enable you to specify a prompt that appears as a multi-line prompt on the user's terminal server screen.

Note: Login Prompt applies only to a user starting a remote terminal server session.

Configuring a multi-line prompt

1 Open the Ethernet profile.

2 Open the TServ options submenu.

```
Edit
90-B00 Mod Config
TServ options
TS Enabled=Yes
Passwd=
Banner=**Ascend Pipeline**
Login Prompt=Login:
Passwd Prompt=Password:
Prompt=ascend%
>Prompt Format=No
Term Type=vt100‘
PPP=Yes
SLIP=No
SLIP BOOTP=N/A
V42/MNP=Will
Max Baud=33600
MDM Trn Level=-13
Cell First=No
```

3 Make sure TS Enabled=Yes.
The Login Prompt parameter is N/A if TS Enabled=No

4 Select Login Prompt= and press Enter to open a text field.

5 Type up to 80 characters. The default value is "Login:"

Character combination	Description
\n	carriage return/line feed
\t	tab
\\	displays "\" on the screen

Note: Any characters that are not specified that have a'\' in front of them are removed. For example, you could enter

```
Welcome to\n\t\\Ascend Remote Server\\\nEnter your user
name:
```

to display the following on the terminal server screen:

```
Welcome to
       \\Ascend Remote Server\\
Enter your user name:
```

6 Press Enter again to close the text field.

7 Set Prompt Format=Yes

This is the field that determines whether you are able to use the multi-line format for the terminal server prompt. If Prompt Format=No, the MAX does not interpret the line feed/ carriage return character or the tab character.

Two DNS domains configurable

You can now specify a second domain name server to be searched when making a connection that looks for a DNS host. Previously, you could specify only one domain name server.

How it works

If the MAX is informed about DNS, dial-in users can TELNET into the local network using hostnames instead of IP addresses. This feature adds a field to the DNS submenu of the Ethernet Profile that enables you to configure two DNS domains. The MAX will search for the DNS Server(s) in the domain configured in Domain Name= first, and then in the domain configured in Sec Domain Name=.

Configuring a second domain:

1 Open the Ethernet Profile.

2 Open the DNS submenu.

You can enter up to 63 characters. By default the field is empty.

```
Edit
90-B00 Mod Config
DNS...
Domain Name=newtek.com
Sec Domain Name=ascend.com
Pri DNS=192.168.1.1
Sec DNS=0.0.0.0
Allow as client DNS=Yes
Pri WINS=0.0.0.0
Sec WINS=0.0.0.0
List Attempt=No
List Size=N/A
Client Pri DNS=0.0.0.0
Client Sec DNS=0.0.0.0
```

3 Close the Ethernet Profile.

Configurable source port for remote authentication and accounting

You can now specify the source port used to send remote authentication requests for all external authentication services the MAX supports, including RADIUS, TACACS, and Defender. You can also specify the source port used to send RADIUS or TACACS+ accounting requests. This new feature meets the needs of those users needing to specify the source port for various uses, including filtering.

User interface changes on MAX

This release includes two new parameters: Auth Src Port and Acct Src Port. The Auth Src Port parameter appears in the Auth submenu of the Ethernet Profile, and specifies the source port for remote authentication requests. The Acct Src Port parameter appears in the Accounting submenu of the Ethernet Profile, and specifies the source port for RADIUS or TACACS+ accounting requests.

Each new parameter is described in the sections that follow.

Auth Src Port

Description: This parameter specifies the source port used to send a remote authentication requests. You can define a source port for all the external authentication services the MAX supports.

Usage: Press Enter to open a text field. Then, type a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the Ascend unit can use any port number between 1024 and 2000.

Dependencies: You can specify the same source port for authentication and accounting requests.

Parameter Location: Ethernet Profile: Ethernet/Mod Config/Auth

See Also: Acct Src Port

Acct Src Port

Description: This parameter specifies the source port used to send a RADIUS or TACACS+ accounting request.

Usage: Press Enter to open a text field. Then, type a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the Ascend unit can use any port number between 1024 and 2000.

Dependencies: You can specify the same source port for authentication and accounting requests.

Parameter Location: Ethernet Profile: Ethernet>Mod Config>Accounting

See Also: Auth Src Port

Modification of RADIUS messages during MAX boot up

The MAX boot-up message warning of timeout of a null user name was misleading and has been rewritten. It now more accurately reports the event as a normal occurrence that releases global IP address pools.

At startup, the MAX syslog notes RADIUS requests intended to release any RADIUS-allocated IP addresses. Some versions of the RADIUS server (960916) timeout the request, which previously resulted in a log message reporting a timeout on a null user name. Now, instead of the null user name, one of these strings appears:

```
RADIUS release global-pool address
RADIUS release all global-pool addresses
```

New maximum lengths for login and password

prompts

In this release, the Login Prompt and Password Prompt parameters now allow you to specify a greater number of characters. This feature was implemented to accommodate existing user scripts.

The Login Prompt parameter specifies the prompt the terminal server displays when asking the user for his or her login name. The Password Prompt parameter specifies the prompt the terminal server displays when asking for a password. You can now specify up to 31 characters for both Login Prompt and Password Prompt.

Ascend X.25 PAD now sends no banner message

This feature sets the terminal server to display no banner when a terminal connects to the MAX over X.25. Previously, when a terminal connected to the MAX, the terminal received an X.25 banner message

How it works

This features changes the MAX default behavior so that no banner appears. When an X.25 PAD user logs in, they see only the X.25 PAD prompt and an asterisk.

Rate Limit default changed for receiving multicast packets

The default rate limit for multicast/Mbone packets has been increased to 100 seconds, which prevents the MAX from accepting packets from multicast clients. This change reverses effect of the previous default, 5 seconds, a fairly short interval that could result in excessive multicast traffic for some networks.

What was changed

The Multicast Rate Limit specifies how many seconds the MAX waits before accepting another packet from a multicast client. To prevent multicast clients from creating response storms to multicast transmissions, you can configure the Ethernet profile and the Connection profile to limit the rate at which the MAX accepts packets from clients.

Previously, the default Rate Limit was 5 seconds. A period this short could result in excessive multicast traffic for some networks. The new default is 100 seconds, which prevents the MAX from accepting any packets from multicast clients.

The Rate Limit parameter appears in two menus: the Multicast submenu of the Ethernet Profile (Figure 8) and the IP Options submenu of the Connection Profile (Figure 9).

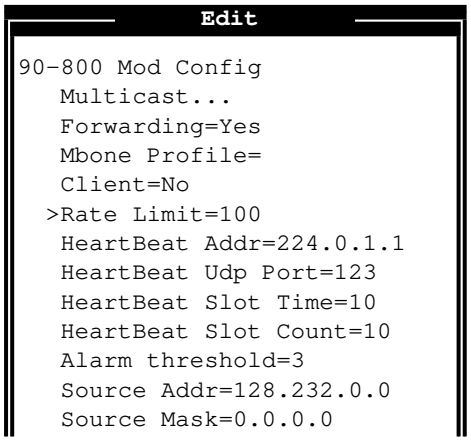


Figure 8. Ethernet > Mod Config submenu

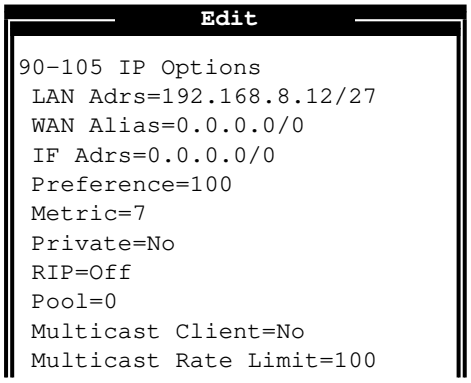


Figure 9. Connection profile > IP Options submenu

Multicast rate limit in RADIUS

You can set this parameter using the RADIUS attribute "Ascend-Multicast-Rate-Limit". If you do not set the Rate Limit parameter through RADIUS, the MAX assumes it to be 100 (the default).

Terminal server kill command

The new terminal server kill command enables you to disconnect a user who establishes a connection with the Ascend unit via Telnet. You can disconnect the user by session ID. The disconnect code that results is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects.

Command-line syntax

To terminate a Telnet session, enter this command line at the terminal server prompt:

```
kill <session ID>
```

For the <session ID> argument, specify the session ID as displayed by the terminal server "show users" command. The disconnect reason for the session is reported as DIS_LOCAL_ADMIN.

The active Security Profile must have Edit All Calls=Yes. If Edit All Calls=No, this message displays when you issue the kill command:

```
Insufficient security level for that operation.
```

If you issue the kill command without the <session ID> argument, this message displays:

```
kill command requires an argument
```

When the session is properly terminated, a message like this one displays:

```
Session 216747095 killed.
```

When the session is not terminated, a caution like this one displays:

```
Unable to kill session 216747095.
```

Per-user control and accounting for immediate modem and MAXDial

This feature adds per-user control of users accessing the MAX unit's modems through immediate modem or MAXDial. This feature also adds accounting to keep track of the calls made through immediate modem or MAXDial.

The details of the MAXDial interface changes are not described in this release note.

Introduction

The Immediate Modem feature allows users to Telnet to a MAX to access the MAX unit's modems, so that they can place outgoing calls without going through MAX terminal server interface. The MAXDial software offers the same outgoing call ability, but through a GUI interface. Now the MAX provides per-user control and accounting for both the Immediate Modem feature and MAXDial to control access to the modems.

When per-user Immediate Modem is enabled, the MAX will request a login name before allowing any user access to the Immediate Modem feature. The MAX will attempt to find a profile with the name provided by the user, looking first for a local Connection profile, then for a simple Name/Password profile, and finally for a RADIUS profile. If no profile matching the name provided by the user can be found, the MAX will reject the user and close the Telnet session. Otherwise, it will prompt the user for the password (if any) associated with the profile and verify that the user enters the correct password. If the user enters the correct password, the MAX then checks that the Dialout-OK parameter of the appropriate profile. If Dialout OK is set to Yes, the user will be allowed access to the immediate modem feature. Otherwise, if the

user gets the password wrong or the Dialout OK parameter is set to No, the MAX rejects the user (with an appropriate message) and closes the telnet session.

MAX configuration interface changes

Two new parameters support immediate modem and MAXDial call restriction and accounting:

- Imm. Modem Auth in the Ethernet>Mod Config>TServ Options menu
- Dialout OK in the Telco Options submenu of the Connection Profile

Note: The Immediate Modem parameter is an existing parameter in the Ethernet > Mod Config > TServ Options submenu.

The following sections describe these new parameters.

Imm. Modem Auth

Description: This parameter enables you to specify the type of call restriction in use.

Usage: You can specify one of these settings:

- None

  This setting indicates that call restriction is disabled, and that all users can place outgoing calls.
- Global

  This setting indicates that a single password exists for dialout. Anyone who knows that password can place outgoing calls. The Imm. Modem Pwd parameter specifies the password.
- User

  This setting indicates the MAX requires a login before any user can access the Immediate Modem's dialout feature. The MAX attempts to match the user's name and password to a name and receive password in a Connection profile, Name/Password profile, or RADIUS users profile. If the user is authenticated by matching a Password profile, the Password profile must point to a Connection profile for the setting of the Dialout OK parameter.

  This is the default.

Dependencies: Keep this additional information in mind:

- When Imm. Modem Auth=None or User, Imm.Modem Pwd is not applicable.
- Previously, you could set the Imm. Modem Pwd parameter to null in order to allow unlimited access to the immediate modem feature; now, however, you should set Imm. Modem Auth=None.

  Note that for compatibility reasons, the system still treats the combination of Imm. Modem Auth=Global and a blank Imm. Modem Pwd parameter as if Imm. Modem Auth were set to None.

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

See Also: Dialout OK, Imm. Modem Pwd

Dialout OK

Description: This parameter specifies whether the user associated with an outgoing Connection Profile can dial out using one of the MAX unit's digital modems.

Usage: You can specify Yes or No.

- Yes indicates that the Connection Profile allows modem dialout.
- No indicates that the Connection Profile does not allow modem dialout.
  The default value is No.

Dependencies: For the Dialout OK parameter to apply, Imm. Modem Auth must be set to User.

See Also: Imm. Modem Auth

New RADIUS attribute

When Imm. Modem Auth=User, you can configure individual RADIUS profiles to allow or disallow dialout. A new RADIUS attribute, Ascend-Dialout-Allowed, will appear in the RADIUS dictionary.

Ascend-Dialout-Allowed

Description: This attribute specifies whether the user associated with an outgoing RADIUS user profile can dial out using one of the MAX unit's digital modems.

Usage: You can specify one of these settings:

- Dialout-Allowed indicates that the RADIUS user profile allows modem dialout.
- Dialout-Not-Allowed indicates that the RADIUS user profile does not allow modem dialout.
  The default value is Dialout-Not Allowed.

Example: Here is an example of a dialout-enabled RADIUS profile:

```
#   This profile applies only to PPP sessions. It uses a local pass-
word.
fred Password="scr41"
    User-Service=Framed-User,
    Framed-Protocol=PPP,
    Framed-Address=10.0.1.1,
    Framed-Netmask=255.255.255.0,
    Ascend-Metric=2,
    Framed-Routing=None,
    Ascend-Idle-Limit=30,
    Ascend-Dialout-Allowed=Dialout-Allowed
```

Dependencies: For the Ascend-Dialout-Allowed attribute to apply, Imm. Modem Auth must be set to User in the TServ Options submenu of the Ethernet Profile.

Call accounting in RADIUS

When you configure the MAX to use RADIUS accounting, RADIUS generates the appropriate session Start and Stop records for the immediate modem dialout sessions. In the Stop record, the attribute Ascend-Connect-Progress (50) identifies a modem dialout session. The User-Name attribute contains the user name if Imm.Modem Auth=User; if Imm. Modem Auth=Global or None, the User-Name attribute is null. The Acct-Input-Octets and Acct-Output-Octets attributes specify the number of bytes received from and written to the modem, respectively.

Note: Call accounting does not record outgoing modem calls made through the terminal server interface; it only applies to immediate modem calls.

Here is an example of the two RADIUS accounting records generated by a brief modem dialout session:

```
Tue Oct 22 15:26:02 1996
   User-Name="ascend1"
   NAS-Identifier=204.253.164.62
   Acct-Status-Type=Start
   Acct-Delay-Time=0
   Acct-Session-Id="214847291"
   Acct-Authentic=Local

Tue Oct 22 15:26:15 1996
   User-Name="ascend1"
   NAS-Identifier=204.253.164.62
   Acct-Status-Type=Stop
   Acct-Delay-Time=0
   Acct-Session-Id="214847291"
   Acct-Authentic=Local
   Acct-Session-Time=12
   Acct-Input-Octets=19
   Acct-Output-Octets=6
   Acct-Input-Packets=0
   Acct-Output-Packets=0
   Ascend-Disconnect-Cause=3
   Ascend-Connect-Progress=50
   Ascend-Data-Rate=0
   Ascend-PreSession-Time=0
   Ascend-Pre-Input-Octets=0
   Ascend-Pre-Output-Octets=0
   Ascend-Pre-Input-Packets=0
   Ascend-Pre-Output-Packets=0
```

Call accounting in SNMP

When you configure the MAX to use SNMP accounting, SNMP enters appropriate event records into the Ascend events group (Ascend 10). Three events are generated:

- A call-originated event

  This event contains no information uniquely identifying the event as a dialout event.
- A name-changed event

  This event contains the user name and host IP address associated with the session. A value of 16 in the eventCurrentService field identifies this event as a dialout event.
- A call-cleared event

  A value of 50 in the eventConnectProgress field identifies this event as a dialout event.

The eventCallReferenceNum field correlates the three events, and contains the same number for all three events.

Note: Call accounting does not record outgoing calls made through the terminal server interface; it only applies to immediate modem calls.

These three SNMP event records were generated by a modem dialout session:

```
# Call-originated event
 eventIdNumber=247
  eventTimeStamp=28
  eventType=1: call originated
```

```
  eventCallReferenceNum=215369509
  eventDataRate=0
  eventSlotNumber=1
  eventSlotLineNumber=1
  eventSlotChannelNumber=0
  eventModemSlotNumber=0
  eventModemOnSlot=0
  eventCurrentService=1: none
  eventUserName=""
  eventUserIPAddress=0.0.0.0
  eventUserSubnetMask=0.0.0.0
  eventDisconnectReason=1: n/a
  eventConnectProgress=1: n/a

# Name-changed event
  eventIdNumber=248
  eventTimeStamp=28
  eventType=5: name changed
  eventCallReferenceNum=215369509
  eventDataRate=0
  eventSlotNumber=0
  eventSlotLineNumber=0
  eventSlotChannelNumber=0
  eventModemSlotNumber=0
  eventModemOnSlot=0
  eventCurrentService=16 (unknown)
  eventUserName="kevin"
  eventUserIPAddress=204.253.164.61
  eventUserSubnetMask=0.0.0.0
  eventDisconnectReason=1: n/a
  eventConnectProgress=1: n/a

# Call cleared event
  eventIdNumber=249
  eventTimeStamp=33
  eventType=3: call cleared
  eventCallReferenceNum=215369509
  eventDataRate=0
  eventSlotNumber=1
  eventSlotLineNumber=1
  eventSlotChannelNumber=0
  eventModemSlotNumber=0
  eventModemOnSlot=0
  eventCurrentService=1: none
  eventUserName=""
  eventUserIPAddress=0.0.0.0
  eventUserSubnetMask=0.0.0.0
  eventDisconnectReason=3: call disconnected
  eventConnectProgress=50 (unknown)
```

Call charge and call status for U.S. ISDN PRI lines

This feature allows SNMP managers to monitor Ascend units call charges and call status for U.S. ISDN PRI lines.

SNMP managers can now gather call charge and call status information for PRI lines. Previously this information could only be gathered from German 1TR6, German Net 5 and the Japan NTT switch types.

ISDN call charge accounting

ISDN call charge accounting was previously implemented for the German 1TR6, German Net 5 and Japan NTT switch types. Now it is also implemented for the ATT, NTI, NI-2 switch types.

When an ISDN call disconnects from ATT, NTI, NI-2 switches, these switches send call billing information to the call originator as part of the call tear-down process. This information is written to the eventCallCharge (eventEntry 17) SNMP object in the Ascend Enterprise MIB events group (10). An SNMP manager can then read this object to determine the cost of the call.

eventCallCharge is a read-only integer and is applicable only if eventType is callCleared (3). Otherwise, 0 is returned.

Call status information

Ascend units currently report such standard information elements as phone number, bearer capability, and cause codes. However, there are some information elements that are very useful and sometimes necessary for debugging a failed connection.

These values can be displayed using SNMP.

Four SNMP objects were added to the eventGroup table to support call status information:

- eventInOctets
- eventOutOctets
- eventCalledPartyID
- eventCallingPartyID

eventInOctets (eventEntry 20)

This object records the total number of octets received by the user from the moment the call begins until it is cleared. It is only applicable if the eventType is callCleared (3), otherwise, 0 is returned.

eventOutOctets (eventEntry 21)

This object records the total number of octets sent by the user from the moment the call begins until it is cleared. It is only applicable if the eventType is callCleared (3), otherwise, 0 is returned.

eventCalledPartyID (eventEntry 18)

This object records the telephone number of the answering device (that is, this unit). This ID is obtained from layer 3 protocol messages during call setup. It is only applicable when the eventType is callOriginated (1), callAnswered (2), or callCleared (3). If the called party ID is unknown or not applicable, a null string is returned.

eventCallingPartyID (eventEntry 19)

This object records the telephone number of the caller. This ID is obtained from layer 3 protocol messages during call setup. It is only applicable when the eventType is callOriginated (1), callAnswered (2), or callCleared (3). If calling party ID is unknown or not applicable, a null string is returned.

New RADIUS attribute for controlling service

For RADIUS-authenticated clients, you can now use the type of connection (ISDN or modem) to prevent them from using a capability to which they have not subscribed. When MAX forwards an Access-Request packet to the RADIUS server, it now includes the NAS-Port-Type attribute. This attribute indicates the type of the physical port of the NAS (Network Authentication Server) that is authenticating the client.

Some Internet Service Providers offer different levels of service based on connection type (modem or ISDN). To prevent a client from using a capability to which they have not subscribed, the capability of limiting the access based on the type of connection is required.

The NAS-Port-Type attribute indicates the type of the physical port of the NAS authenticating the client. When it can be determined, it may be included in addition to the NAS-Port attribute. It is only used in Access-Request packets. To use this feature, you must download the most recent RADIUS dictionary and daemon from the Ascend FTP site. The RADIUS dictionary includes the NAS-Port-Type attribute, which is defined as follows:

```
ATTRIBUTENAS-Port-Type61integer
    VALUENAS-Port-TypeAsync0
    VALUENAS-Port-TypeSync1
    VALUENAS-Port-TypeISDN-Sync2
    VALUENAS-Port-TypeISDN-Async-V1203
    VALUENAS-Port-TypeISDN-Async-V1104
    VALUENAS-Port-TypeVirtual5
```

These are the supported NAS port types:

- Async refers to a call routed to a digital modem.
- Sync refers to a non-ISDN synchronous connection such as a switched-56K connection.
- ISDN-Sync refers to a synchronous ISDN connection
- ISDN-Async-v120 refers to an ISDN connection using the V.120 asynchronous rate adaptation.
- ISDN-Async-v110 refers to an ISDN connection using the V.110 asynchronous rate adaptation.

- Virtual refers to a connection to the NAS via some transport protocol, instead of through a physical port.

The following a sample user's entry makes use of the NAS-Port-Type feature:

```
# Restrict the user to async modem calls only
# Do not allow ISDN or other connections
ascend1 Password = "pipeline", NAS-Port-Type = Async
        User-Service = Framed-User,
        Framed-Protocol = PPP,
        Framed-Address = 10.0.1.1,
        Framed-Netmask = 255.255.255.0
```

Separate modem-user and digital-user profiles

This feature allows users dialing into a MAX authenticating with in SecurID ACE direct mode to specify one of the MAX unit's local profiles to be used for session parameters. The previous implementation of SecurID ACE always used the RADIUS default profile for all users who authenticated with a SecurID token card. It also enables an optional Lan Address setting to override the Lan Address in the specified profile (or in the default profile, if no specific profile is given). This feature also enables you to specify different profiles/addresses for each user, based on whether the user has dialed in with a modem (analog call) or ISDN (digital call). This means a single token card can be used for authenticating from two different remote setups (for example, a Pipeline 50 + desktop at home or a laptop and modem while travelling). This feature also changes slightly the way that quotations are done for password (rp) strings given in the ACE server shell strings.

How it works

The previous implementation of direct SecurID ACE authentication on the MAX product line always used the RADIUS default profile for all users who authenticated with a SecurID token card. This limited the functionality of the feature, since all users had to be satisfied with a standard limited set of parameters.

The default profile is one you create with the username DEFAULT and place as the *last profile* of the RADIUS users file. The ACE server will use that profile to determine what to do with users who are not contained in the users file.

This new implementation uses each user's shell setting on the ACE server to store several parameters about the user, including the name of a MAX local profile which should be used when setting up the call for that user, as well as the address and netmask to be used in place of the Lan Address in the given profile.

Shell string structure

The shell string returned by ACE is limited to 64 characters, so brevity is very important. The names of parameters are extremely short.

The basic structure of the string is:

```
<parameters> |<CallType> <parameters> |<CallType> <parameters>
...
```

Table 23. SecurID-ACE shell string structure

Parameter	Possible Values	Description
<CallType>	A	Following information is only for analog (modem) calls). See the RADIUS NAS-Port attribute for an explanation of which calls are classified as analog and which are classified as digital.
	D	Following information is only for digital (ISDN) calls. See the RADIUS NAS-Port attribute for an explanation of which calls are classified as analog and which are classified as digital.
	" " (space)	Following information is for all types of calls.
		Note: Everything from a <CallType> up to the next "|" (or the end of the string) is put into the caller's profile if and only if the call was of the given type.
<parameters>	one or more of <parameter>	
<parameter>	rp=<string>	Applies only to PAP-TOKEN-CHAP calls, since direct SecurID authentication does not support CACHE-TOKEN. This parameter is put in place of the Receive Password in the Connection Profile, and is used for authentication in subsequent calls. rp is only used to authenticate the second and subsequent calls in an MP bundle, never the first call. The first call must be authenticated by the user with a token value from the SecurID card.
	la=<address>	The IP address of the caller. This parameter functions the same as LAN Adrs in the Connection Profiles. You can use it to specify an address for the remote caller that is different from the address given in the selected (or default) Connection Profile.

Table 23. SecurID-ACE shell string structure (continued)

Parameter	Possible Values	Description
	prf=<string>	The name of the Connection Profile stored in the MAX's NVRAM; provides the configuration of the caller. If there is no profile for a call: If Use Answer as Default=Yes (from the Answer profile), the Answer profile is used as the default. If Use Answer as Default=No, the Factory Default Profile is used.
<string>	<stuff> "<stuff>" '<stuff>' [<stuff>]	<stuff>is the value of the parameter.

Conventions

The conventions in the following table apply to all strings.

Table 24. Format conventions for strings

quotes and brackets	Only needed when the value itself has a space in it. Table 23 shows the multiple types of quoting in case you need both a space and one of the other quote characters in a string.
| (vertical bar character)	Has a special meaning, and cannot appear in any string.
<address>	An <address> is a string (that is, you can quote or bracket it if you like), but it should take on the form of an IP address, (for example, 1.2.3.4) optionally followed by a netmask (for example, /24).

Examples of String Contents:

For example, the following string

```
|D prf="isdnroute" rp=[greco] la=192.0.2.1/24 |A prf=modemroute
```

specifies:

- if the caller is digital
  - use the profile called isdnroute
  - set the Receive PW to greco
  - set the Lan Addr to 192.0.2.1/24
- if the caller is analog
  - use the profile called modemroute

Shortening a string

The above string is just short enough to fit. If the string was any longer, the end of modemroute would be cut off and authentication would fail for analog calls. The same shell string could be given as:

```
|D prf=isdnroute rp=greco la=192.0.2.1|A prf=modemroute
```

Although this example specifies the same information as the previous example, it has been shortened in the following ways:

- The quotation symbols have been removed. In general, quotes are needed only if there is a space in the character string.
- The space has been removed from before the **|A** (the | character indicates the end of a string, just like a space).
- The netmask was not given (/24 is the default netmask for 192.0.2.1, a class C network address).

Setting common parameters for analog and digital calls

It is also possible to have common parameters preceding the sections specific to just analog or digital. For example:

```
prf=john |D la=135.2.2.4/24 |A la=135.2.3.20
```

In this example, the settings would always be taken from the profile john, but the address would be set differently depending on whether the call was analog or digital.

The section with common parameters can be placed after the specific sections as well as before. For example, the following string:

```
|A prf=modemroute |D prf=isdnroute | la=10.0.0.20/32
```

says to use modemroute as the profile template for analog calls, isdnroute for digital calls, and in both cases to use the address 10.0.0.20/32 as the LAN Address.

Separate sections are not required. For example:

```
prf=john la=10.0.0.20/32
```

would use the profile named john and set the Lan Address to 10.0.0.20/32 whether the call was analog or digital.

Or you can have just one or the other:

```
|D prf=isdnroute rp= "go for it"
```

In this case, an analog caller would be given the default or answer profile depending on the setting of the Use Answer as Default parameter in the answer profile.

String errors

If there is an error or unrecognized string in the shell string for a user, the authentication will fail. If you have trouble seeing what caused the failure, enter the MAX's debug mode and turn on a diagnostic display of the string interpretation using the command **`securiddebug`**. This is a toggle that turns the display on and off.

String too long

Check to see that you have not exceeded the 64 character limit (the ACE server's sdadmin program does not check for this limit). This is indicated when the final parameter is not complete. For security reasons, the password string is not displayed by this debug mode.

For security reasons, the password string is not displayed by this debug mode, so you will not be able to tell directly from the debug output whether the rp parameter is being truncated. If you encounter problems with the 2nd and subsequent channels of an MP call automatically authenticating, the problem could be that the end of the rp parameter is being cut off.

Setting overwritten

Each new parameter is copied over the current state of the caller's profile at each step. It is therefore possible to overwrite one setting with another. For example:

```
rp=joebob prf=john
```

will cause the Receive Password joebob to be overwritten by the Receive Password in the profile john. Be careful always to list prf's before rp's or la's.

Add PAP-TOKEN-CHAP to ACE authentication

This feature enables user dialing into a MAX authenticating with direct SecurID ACE to bring up additional channels without the repeating the interaction required for the first token authentication.

How it works

The original implementation of direct SecurID ACE authentication on the MAX product line did not support PAP-TOKEN-CHAP (as is supported when using token cards through RADIUS), because the MAX needed to have a per-user password that did not change over time, such as the Recv Password in a local profile, and the ACE server only used a time-based, changing password.

PAP-TOKEN-CHAP is implemented in this feature by storing a static password in the user's shell setting on the ACE server and sending it back to the MAX when the user first connects. Aside from this, PAP-TOKEN-CHAP configuration on the calling router is identical to configuring PAP-TOKEN-CHAP for any other type of token card authentication.

Configuring PAP-TOKEN-CHAP on the ACE server

This feature implementation makes no changes on the MAX user interface. There is a difference in the setup of the ACE server itself.

To set the static password to use during PAP-TOKEN-CHAP for a particular user:

1. Run the sdadmin program on the ACE server machine.
2. From the Client menu, select Edit.
3. Pick the MAX from the list of clients and click OK.
4. Click User Activations.
5. From the Directly Activated Users list, select the user that will be using PAP-TOKEN-CHAP, then click Edit Activation Data.
6. In the Activation Data window, delete any existing text in the Shell field, and replace it with:

   `rp="<password>"`

   where `<password>` is the password to be configured as the Aux Send PW on the calling router (usually a Pipeline). This is done in Step 8.

   For example, if the password is to be Little Big (without quotation marks), then the Shell field should contain: `rp="Little Big"`

   (with quotation marks). In this example, the quotes are delimiters for the password. Different delimiters are allowed is so that the user can have a password containing those delimiters, for example:

   `rp='Quote"quote'`

   which contains a double quote in the middle of the password.

   You can use any character you like for the delimiters in place of the double quotes except the vertical bar ("|"), which has a special meaning in the shell field. For example, the following entry would produce the same Receive Password setting as `rp="Little Big"`:

   `rp=/Little Big/`

   However, `rp=[Little Big]` is not identical and would an error, since the left bracket and right bracket are different characters.
7. Press OK to clear the Activation Data dialog, and Exit to clear the Edit Client dialog
8. Configure the calling router (usually a Pipeline) to use PAP-TOKEN-CHAP authentication, and set Aux Send PW in the Connection profile Encaps options to be identical to the string you entered in the ACE server as rp (Receive Password) in Step 6.
9. Assuming all other configuration was already done (configuring the answering MAX to use SecurID authentication, and configuring the calling router to use the App Server, for example), you should now be able to bring up a multi-channel call, while only performing a single token authentication.

Host BRI U-Interface slot card offered

The Host/BRI slot card for the MAX is now available with a U interface. The card functions similarly to the BRI 8S-Interface slot card already available. This note describes the differences and specifications of the new BRI/LT card.

Ascend units affected: MAX 4000, MAX 1600

BRI-8U/LT card specifications

The Multiband BRI-8 U/LT slot card (called the BRI/LT card in this document) is a new slot card in the MAX family of BRI cards. It shares many of the features familiar to Host/BRI and Net/BRI slot card users.

This document describes user interface details for the BRI/LT. Since many of the parameters and functionality of the BRI/LT card are similar to those of existing cards, you can find additional information on features and configuration in the MAX 4000 Reference Guide.

Functional specifications

The Multiband BRI-8U/LT slot card (BRI/LT in short) provides the following features:

- ISDN BRI signalling
- 8 ports, BRI U-interface (2B+D)
- 144kbit/s user bit rate over a two-wire subscriber loop
- 2B1Q block code (2 binary, 1 quaternary)
- Line Termination (LT) mode
- Switch-Less (replaces the switch)
- Data calls only (the BRI/LT replaces the switch, no voice calls are possible)
- point to point
- supports switched channels
- supports nailed channels (including Ascend's superDigital 128)
- supports all of the applications that were going over the BRI-8 S/T slot card except for voice calls
- supports maintenance functions (BRI-U interface monitoring commands), out of band (for example, the monitoring functions are using the M1, M2, M3 positions of an U superframe and do not steal any bits from the B nor the D channel, 2 monitor commands can be carried per U super frame)

The BRI/LT provides a separate network that does not congest the “voice network” with data traffic. Data traffic is not presented to a switch, since the MAX replaces the switch for data-only traffic. In this way the BRI/LT provides some of the functionality of a switch for monitoring line quality and troubleshooting the line. See Diagnostic Functions for more information on troubleshooting a line, and Status screens for more information on monitoring a line.

Configuring the BRI/LT card

Configuration parameters for the BRI/LT card are similar to those for the Host/BRI card described in the MAX 4000 Reference Guide. If a BRI/LT slot card is installed in a MAX and passes POST, the Main Edit Menu shows a X0-000 BRI/LT option, indicating that a BRI/LT card was detected on slot X, as shown below.

```
Edit

Main Edit Menu
   00-000 System
   10-000 Net/T1
   20-000 Net/T1
   30-000 V.34 Modem
  >40-000 BRI/LT
   50-000 Empty
   60-000 Empty
   70-000 Empty
   90-000 Ethernet
   A0-000 Ether Data
   B0-000 Serial WAN
```

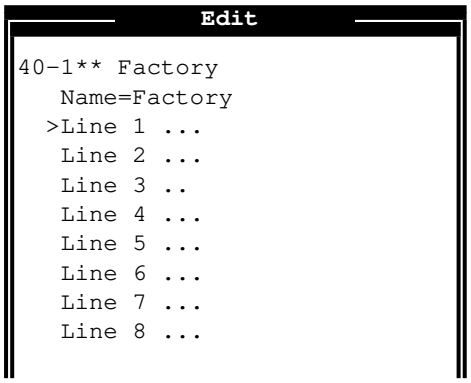
1 Select the BRI/LTcard to configure the BRI/LT card. The example shows a BRI/LT card in slot 4.

```
Edit

40-000 BRI/LT
  >40-100 Line Config
   40-200 Line Diag
```

2 Define up to five profiles for the BRI/LT card.

```
Edit

40-100 Line Config
  >40-1** Factory
   40-101
   40-102
   40-103
   40-104
```

3 Select the line to configure each port.



4 To configure a specific port, select the port (slot/line/port), and configure the fields. Table 25 describes the options available.

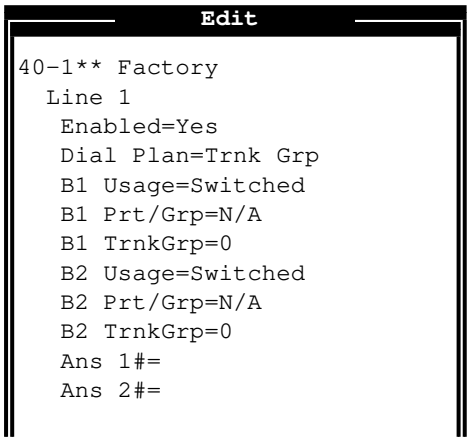


Table 25. BRI/LT line configuration parameters

Parameter	Description	Values
Enabled=	Specifies whether this port is enabled or not.	N/A: Never Range: yes/no Default: yes
Dial Plan=	Defines the dial plan for this port.	N/A: This parameter is N/A when Use Trunk Group=No in the System Configuration Profile. Range: Trnk Grp/Extended Default: Trnk Grp
B1 Usage=	Selects the call type for this channel: switched, nailed or unused.	N/A: Never Range: Switched/Nailed/Unused Default: Switched

Table 25. BRI/LT line configuration parameters

Parameter	Description	Values
B1 Prt/Grp=	Nailed group number when nailed channel selected for this channel.	N/A: When B1 usage=unused or =switched. Range: 1-64 Default: 1 (if nailed) N/A if Switched or Unused
B1 TrnkGrp=	The trunk group number when dialing out on this channel. Used to identify the port/channel for an outgoing call.	N/A: NA if B1 Usage=Nailed or =Unused Default: 0 Range: 4-9 2 indicates a call placed on a BRI line provided by a BRI/LT card placed between serial host ports.
B2 Usage=	Selects the call type for this channel: switched, nailed or unused	N/A: Never Range: Switched/Nailed/Unused Default: Switched
B2 Prt/Grp=	Nailed group number when nailed channel selected for this channel	N/A: When B2 Usage=unused or =switched. Range: 1-64 Default: 1 (if nailed) N/A if Switched or Unused
B2 TrnkGrp=	The trunk group number when dialing out this channel. Used to identify the port/channel for an outgoing call.	NA: NA if B1 Usage=Nailed or =Unused Default: 0 Range: 4-9 **Note:** 2 indicates a call placed on a BRI line provided by a BRI/LT card placed between serial host ports.
Ans 1#=	Answer number 1. Phone number assigned to the WAN line to receive calls from remote device.	Not applicable to outgoing calls, to local calling (calling between local BRI lines provided by the MAX), or to calls received with no called party information.
Ans 2#=	Answer number 2. Phone number assigned to the WAN line to receive calls from remote device.	Not applicable to outgoing calls, to local calling (calling between local BRI lines provided by the MAX), or to calls received with no called party information.

Configuring a remote TA with the BRI/LT

When configuring a remote TA (for example, a Pipeline 50 U-interface) to attach to the BRI/LT, always select ATT 5ESS Point-to-point as the switch type. The BRI/LT card can only emulate the ATT 5ESS point-to-point switch.

Diagnostic Functions

Maintenance functions for the BRI/LT include test loopbacks, statistics (block error counters), and error generation (to check that the counters work).

Maintenance functions supported by the BRI/LT driver use the BRI-U interface's embedded operations channel (EOC). The EOC transfers data from the exchange to the terminal side and vice versa without occupying either the B- or the D-channel. It is used to transmit diagnostic function and signaling information, for example:

- obtaining the block errors in close to real time.
- diagnostic functions to diagnose a line (for example, loopback, corrupt CRC)

The EOC monitor commands are sent in the M1, M2, and M3 bits of the U-superframe (refer to ANSI T1-601, from ANSI 1991 for more information about usage of the M1, M2, and M3 bits of the superframe).

Block error counters

The remote U interface/echo canceller provides internal counters for far-end and near-end block errors. A near-end block error (NEBE) indicates that the error has been detected in the receive direction. A far-end block error (FEBE) identifies errors in the transmission direction. The block error totals are obtained from the remote TA. These cumulative totals are reset when you clear the block error buffer(s) from the Line diagnostics submenu, or when you restart the MAX. The totals wrap back to zero when they reach 65535.

You can use the block error counters to monitor transmission quality at the U-interface. A block error is detected each time when the calculated checksum of the received data does not correspond to the control checksum transmitted in the successive superframe. One block error indicates that one U-superframe has not been transmitted correctly. The block error count does not provide information regarding the number of bit errors in the U-superframe, only that the CRC failed in that superframe.

About every 4 seconds, a daemon running in the MAX obtains the remote block error counter values and displays their cumulative value in the block errors status screens.

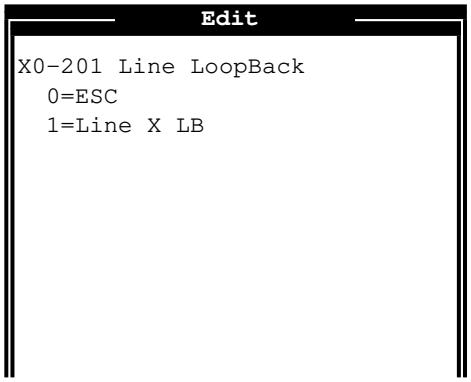
See Block Error status display for a description of the block error information displayed.

Generating errors to test the block error counters

In order to test the NEBE and FEBE counters, transmission errors can be simulated with artificially corrupted CRCs. The Corrupt CRC and Rq Corrupt CRC options request the local BRI/U interface or the remote U interface/echo canceller to invert the CRC.

Using Line Loopback

When you select Line Loopback from the Line Diagnostics submenu, an intermediate screen appears:



1 Select 1 to enable the loopback command.

When you select 1, the Line loopback command is issued, and test frames are sent continuously in the D channel until the command is cancelled. Frames transmitted have a length of 24 bytes. The frames differ in content and should cover every possible bit pattern.

Note: Only one loopback can be issued at a time on the same line. If another user attempts to invoke the loopback command for a line that is already in loopback mode, the following error message is displayed:

```
Line LB already.
Cmd ignored.
```

Because UnRq Corrupt CRC uses the same command to request that the remote cancel the loopback, UnRq Corrupt CRC is unavailable when the MAX exits loopback mode.

2 Display the LB Counters status screen to see the number of transmitted frames as opposed to the number of correctly received frames.

The MAX continuously sends frames to the remote end. This means that:

– When the MAX receives a frame that matches the transmitted frame in size (and the bytes of the received frame exactly match the bytes in transmitted frame), it sends a new frame out and increments the receive counter for that frame.

– When the MAX receives a frame that does not match the transmitted frame, it still sends out a new frame, but does not increment the receive counter for that frame.

– When the MAX does not receive a frame back, the timeout between two consecutive transmitted frames is about 4 seconds.

3 Press ESC to cancel the Loopback function.

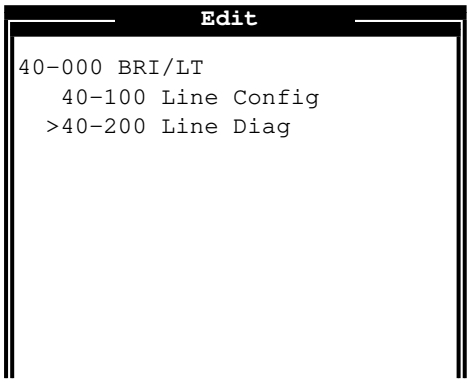
The following message appears:

```
Line loopback terminated.
```

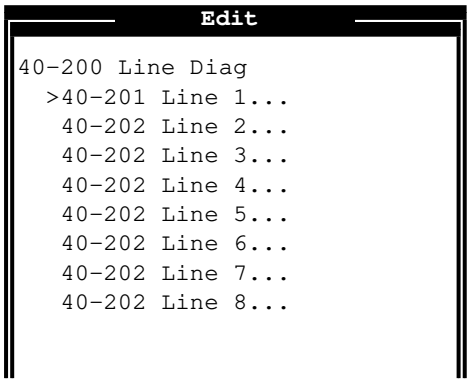
Using the diagnostic functions

All of the diagnostic functions are accessed from the Line Diag submenu of the BRI/LT Configuration Profile.

1 Select the BRI/LT card and then select Line Diag to use the diagnostic functions for this slot.



2 Select the line for which the EOC command is to be issued:



3 Select the EOC function in the Line diagnostics submenu:

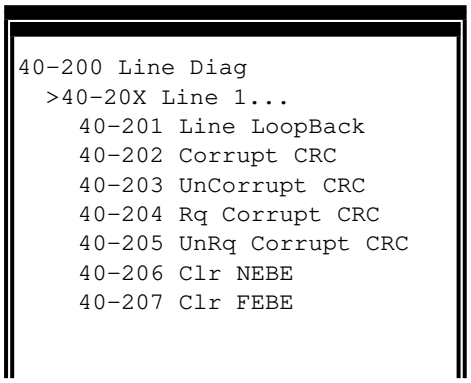


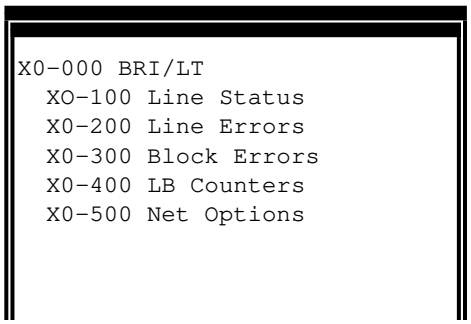
Table 26. Line Diagnostics submenu parameters

X0-201 Line Loopback (LB)	Puts line into loopback mode. Displays a menu with additional options. See Using Line Loopback, below.
X0-202 Corrupt CRC (CCRC)	Causes the BRI-U interface to permanently transmit inverted CRCs until cancelled. When this command is issued, the far-end block error should be viewed from the remote TA.
X0-203 UnCorrupt CRC	Cancels previous CCRC command.
X0-204 Rq Corrupt CRC (RCC)	Request NT1 to corrupt the CRC to artificially simulate transmission errors. It is used to verify that the block error counters are working, or providing the right information. When issued, check the near-end block error.
X0-205 UnRq Corrupt CRC	Request NT1 to return to normal.
X0-204 Clr FEBE	Clears the FEBE counter.
X0-205 Clr NEBE	Clears the NEBE counter.

Status screens

BRI/LT is a branch of the Main Status Menu that lists windows indicating the status of the ISDN BRI interfaces. The BRI/LT window appears only if a BRI/LT module is installed.

To display the BRI/LT Status menu, select BRI/LT from the Main Status Menu.



Line Status

The Line BRI/LT Status window shows the condition of the electrical link to the carrier and the status of the B1 and B2 channels.

Line errors

The Line Errors status window displays the errors recorded on all current channels in a channel-by-channel, line-by-line list. The Line Errors window displays the status of lines even if the interface is disabled in the Line Profile. This status function is the same as that for the NET/BRI module. For more information about Line Errors, refer to the MAX 4000 Reference Guide.

Block Error status display

The Block Errors status display shows the errors for near-end block errors (NEBE) and far-end block errors (FEBE). The numbers displayed are totals accumulated since the last time the block error buffers were cleared.

The FEBE and NEBE error buffers can be cleared per line and per counter (you can clear the FEBE buffer for a line without clearing the NEBE buffer). The totals for each buffer wrap back to zero after they reach 65535. Restarting the MAX clears the buffers.

X0-X00	FEBE	NEBE
1:	0	0
2:	0	0
3:	0	0
4:	0	0
5:	0	0
6:	0	0
7:	0	0
8:	0	0

Loopback (LB) counters status display

The Loopback counters status display shows the number of test frames sent and received since the Loopback command was issued (see Using Line Loopback). The numbers displayed are cumulative totals since the Line loopback command was issued; when the loopback command is started or restarted the LB counters are reset to 0.

X0-XXX	XMIT	RECV
1:	0	0
2:	0	0
3:	0	0
4:	0	0
5:	0	0
6:	0	0
7:	0	0
8:	0	0

Net options

Net Options for the BRI/LT lists the interface features with which your MAX has been equipped.

```
X0-XXX Net Option
>BRI/LT Network I/F
 8 Network I/F(s)
```

SNMP callStatusType field added to callStatus table

This new SNMP feature enables you to differentiate incoming calls from outgoing calls.

Changes to the Ascend Enterprise MIB

The new callStatusType field is defined in this way:

```
callStatusType  OBJECT-TYPE
  SYNTAX  INTEGER   {
    callOutgoing(1),    -- outgoing call
    callIncoming(2)     -- incoming call
    }
  ACCESS   read-only
  STATUS   mandatory
  DESCRIPTION   "A value of 0 is returned if entry is invalid."
    ::= { callStatusEntry 13 }
```

New lanModemGroup in the Ascend Enterprise MIB

This new feature enables you to monitor the digital modem usage for analog calls. The disabled modem list subgroup is available only on MAX units with digital modems and a T1 network interface.

Changes to the Ascend Enterprise MIB

The lanModemGroup specifies the digital modems supported by the Ascend unit and is defined as follows:

```
lanModemGroup       OBJECT IDENTIFIER ::= { ascend 15 }
availLanModem OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of lan modems in the availLanModemTable."
    ::= { lanModemGroup 1 }
availLanModemTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF AvailLanModemEntry
```

```
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The lan modems in this table are used for answering or
placing calls.
  This table is searched before the suspectLanModemTable."
    ::= { lanModemGroup 2 }
availLanModemEntry OBJECT-TYPE
  SYNTAX  AvailLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The properties associated with the entries in the avail-
LanModemTable."
  INDEX  { availLanModemSlotIndex, availLanModemPortIndex }
    ::= { availLanModemTable 1 }
  AvailLanModemEntry ::=
    SEQUENCE {
      availLanModemSlotIndex
    INTEGER,
      availLanModemPortIndex
    INTEGER,
      availLanModemUsedCount
    Counter,
      availLanModemBadCount
    Counter,
      availLanModemLast32
    INTEGER
    }
availLanModemSlotIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The slot number corresponding to the lan modem."
    ::= { availLanModemEntry 1 }
availLanModemPortIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The port number corresponding to the lan modem."
    ::= { availLanModemEntry 2 }
availLanModemUsedCount OBJECT-TYPE
```

```
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of times the lan modem was utilized."
    ::= { availLanModemEntry 3 }
availLanModemBadCount OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of times the lan modem failed."
    ::= { availLanModemEntry 4 }
availLanModemLast32 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "A 32-bit mask of the last 32 times the lan modem was
tried. A '0' in the
  bit position indicates failure while a '1' indicates success."
    ::= { availLanModemEntry 5 }
suspectLanModem OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of lan modems in the suspectLanModemTable."
    ::= { lanModemGroup 3 }
suspectLanModemTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF SuspectLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The lan modems in the suspectLanModemTable are tried
after the availLan
  ModemTable is exhausted."
    ::= { lanModemGroup 4 }
suspectLanModemEntry OBJECT-TYPE
  SYNTAX  SuspectLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The properties associated with the entries in the sus-
pectLanModemTable."
  INDEX  { suspectLanModemSlotIndex, suspectLanModemPortIndex }
   ::= { suspectLanModemTable 1 }
```

```
  SuspectLanModemEntry ::=
   SEQUENCE {
     suspectLanModemSlotIndex
   INTEGER,
     suspectLanModemPortIndex
   INTEGER,
     suspectLanModemUsedCount
   Counter,
     suspectLanModemBadCount
   Counter,
     suspectLanModemLast32
   INTEGER
   }
suspectLanModemSlotIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The slot number corresponding to the lan modem."
   ::= { suspectLanModemEntry 1 }
suspectLanModemPortIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The port number corresponding to the lan modem."
    ::= { suspectLanModemEntry 2 }
suspectLanModemUsedCount OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of times the lan modem was utilized."
    ::= { suspectLanModemEntry 3 }
suspectLanModemBadCount OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of times the lan modem failed."
    ::= { suspectLanModemEntry 4 }
suspectLanModemLast32 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
```

```
  STATUS  mandatory
  DESCRIPTION "A 32-bit mask of the last 32 times the lan modem was
tried. A '0' in the
  bit position indicates failure while a '1' indicates success."
    ::= { suspectLanModemEntry 5 }
disabledLanModem OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The number of lan modems in the disabledLanModemTable."
    ::= { lanModemGroup 5 }
disabledLanModemTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF DisabledLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The table of lan modems disabled using the console."
    ::= { lanModemGroup 6 }
disabledLanModemEntry OBJECT-TYPE
  SYNTAX  DisabledLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The properties associated with the entries in the
  disabledLanModemTable."
  INDEX  { disabledLanModemSlotIndex, disabledLanModemPortIndex }
    ::= { disabledLanModemTable 1 }
  DisabledLanModemEntry ::=
    SEQUENCE {
      disabledLanModemSlotIndex
    INTEGER,
      disabledLanModemPortIndex
    INTEGER,
     disabledLanModemUsedCount
   Counter,
     disabledLanModemBadCount
   Counter,
     disabledLanModemLast32
   INTEGER
   }
disabledLanModemSlotIndex OBJECT-TYPE
  SYNTAX  INTEGER
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The slot number corresponding to the lan modem."
      ::= { disabledLanModemEntry 1 }
  disabledLanModemPortIndex OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The port number corresponding to the lan modem."
      ::= { disabledLanModemEntry 2 }
  disabledLanModemUsedCount OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The number of times the lan modem was utilized."
      ::= { disabledLanModemEntry 3 }
  disabledLanModemBadCount OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The number of times the lan modem failed."
      ::= { disabledLanModemEntry 4 }
  disabledLanModemLast32 OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "A 32-bit mask of the last 32 times the lan modem was
  tried. A '0' in the
    bit position indicates failure while a '1' indicates success."
      ::= { disabledLanModemEntry 5 }
  deadLanModem OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION "The number of lan modems in the deadLanModemTable."
      ::= { lanModemGroup 7 }
  deadLanModemTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF DeadLanModemEntry
    ACCESS  not-accessible
    STATUS  mandatory
```

```
  DESCRIPTION "The table of lan modems which are considered as dead."
    ::= { lanModemGroup 8 }
deadLanModemEntry OBJECT-TYPE
  SYNTAX  DeadLanModemEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION "The properties associated with the entries in the dead-
LanModemTable."
  INDEX  { deadLanModemSlotIndex, deadLanModemPortIndex }
   ::= { deadLanModemTable 1 }
   DeadLanModemEntry ::=
     SEQUENCE {
       deadLanModemSlotIndex
     INTEGER,
       deadLanModemPortIndex
     INTEGER,
       deadLanModemState
     INTEGER
     }
deadLanModemSlotIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The slot number corresponding to the lan modem."
    ::= { deadLanModemEntry 1 }
deadLanModemPortIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION "The port number corresponding to the lan modem."
    ::= { deadLanModemEntry 2 }
deadLanModemState OBJECT-TYPE
  SYNTAX  INTEGER {
    other(1),
    failedPost(2),
    nonExistent(3)
    }
  ACCESS  read-only
  STATUS  mandatory
```

```
  DESCRIPTION "The reason for the lan modem to be place in the deadLan-
ModemTable."
    ::= { deadLanModemEntry 3 }
```

X. 25 Auto-call parameter name and field changed

The name of the Immed X.121 Addr field in the Encaps submenu of the PAD Connection Profile has been changed to Auto-Call X.121 field. The size of this field has been enlarged to permit 48 characters to be entered. Previously, this field allowed a maximum of 15 characters. The larger field permits inclusion of Call User Data in the Auto Call X.121 Addr field, a feature required by some hosts.

How it works

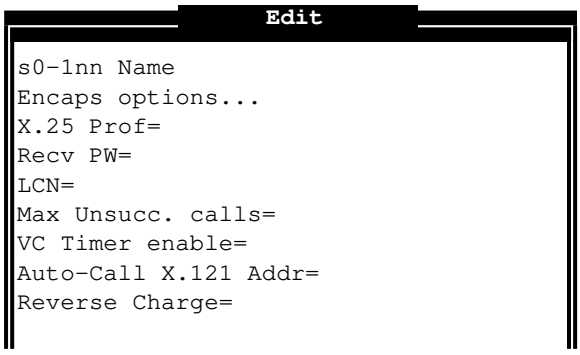
When a user calls the X.25/PAD through a modem, the MAX normally performs authentication during which it selects a local Connection profile matching the callers' login name and password. The matching profile provides a setting for the Auto-Call X.121 Adr parameter.

If the MAX unit's terminal server has been set Immed Service=X.25/PAD, then depending on how the user has set the Auto-Call X.121 Adr parameter, the X.25 session might automatically begin, or the MAX would present the user with the X.25/PAD prompt, an asterisk (*). The syntax for setting the Auto-Call X.121 Adr parameter is given in the "Configuring X.25 Autocall," below.

Configuring X.25 Auto-call

In the Encapsulation submenu of a user's Connection Profile, you can use the Auto-call X.121 Addr field to specify that the PAD call an X.121 address immediately after the PAD session starts for that user.

When Encaps=X.25/PAD, the Encaps submenu looks like the following:



To enable the Auto-Call feature, enter the CUD in the Auto-Call X.121 Addr field when you configure the PAD. Use the format

```
CALL [?] | [[<address>][*P|*D|*F <data>]]
```

Table 27 shows the arguments for the call command.

Note: The <data> following the *P and *D keywords is inserted into the last 12 bytes of the user data field.

Table 27. X.25/PAD terminal server commands

Argument	Meaning
<address>	The X.121 address to which the call is made. The address can contain up to 15 characters.
*P	Do not echo what is entered at the keyboard after the *P command, even if you set X.3 parameter number 2 to Echo. This is to protect passwords that are carried with the call user data. While you are entering text in the auto-call field, this input will be echoed regardless of whether you have issued a *D command.
*D	Echo what is entered at the keyboard after the *D command. This is the opposite of *P.
*F	What follows the *F command is fast-select data.

New trap for suspect modems

A new SNMP trap is generated when a modem moves to the suspect list. Ascend units create a "suspect" list for digital modems based on failed connection attempts and other factors. In this release, SNMP trap is generated and sent to the alarm filter group when a modem is placed on the suspect list.

In this release, an SNMP trap is generated carrying information pertaining to a modem that has moved to the suspect list. This trap is sent to the alarm filter group. The following item has been added to ascend.trp:

-- lan modem moved to the suspect list

```
  lanModemMovedToSuspectList  TRAP-TYPE
        ENTERPRISE      ascend
--      VARIABLES       { slot, port, usedCount, badCount, last32  }
        DESCRIPTION     "This trap is sent to all the managers in the
                          alarm group when a lan modem (digital modem)
                      is moved to the suspect list.Refer to the
                      lanModemGroup.suspectLanModemTable description."
        ::= 20
```

Terminal server show users command added

A terminal server command has been added that displays a list of user sessions active on a system. Each user session is identified by the sessionID, with additional information about the session. The show users command has also been added to the online help for the show command.

How the show users command works

To display a list of active user session on an Ascend MAX, type

```
show users
```

at the terminal server prompt. The following table shows the information the show users command will return..

Show user fields	Field description
IO	O (outgoing call) I (incoming call)
Session ID	Session identifier for the session. This number can be cross- referenced to other system functions that also use the sessionID. It is the same as Acct-Session-ID in RADIUS.
Line Channel	The WAN line and channel associated with the session.
Slot Port	The slot and port of the service being used by the session. This can be: • the number of a slot containing a modem card and the modem on that card • the virtual slot of the MAX's bridge/router, with port giving the virtual interfaces to MAX's bridge/router starting with 1 for the first session of a multichannel session
Data Rate	The bearer capacity or modem speed as appropriate to the session type.

Show user fields	Field description
Service Type	The type of session. This can be Termsrv or a protocol name. For MP and MPP sessions the ID of the session is listed following the encapsulation protocol name to allow identification of the MP bundle to which a session belongs. The special values Initial and Login document the progress of a session: • Initially identifies sessions that do not yet have a protocol assigned. • Login identifies Termsrv sessions during the login process.
Host Address	The network address of the host originating the session. For some sessions this field is N/A. F For outgoing MPP sessions only the first connection has a valid network address associated with it. All other connections in the bundle have the network address as listed as MPP Bundle.
User Name	The name associated with the session. Initially this value is Answer. This is usually replaced with the name of the remote host. For terminal server sessions this is the login name. Prior to login completion this field will show the string “modem x:y” where x and y are the slot and port of them modem servicing the session.

Example data displayed by show users

In the example shown in Figure 10 three sessions are indicated:

- outgoing MPP bundle of two connections on the channel two of the first T1 line
- outgoing MPP bundle of two connections on the channel six of the first T1 line
- incoming async PPP session on the first channel of the same T1 being serviced at 28.8K by the first modem on the modem card in slot three

Note: mpID is the bundle ID the calls in the multiband bundle (on MP or MPP+) have in common.

The Pipeline 50 name is `arwp50` and the user logged onto the terminal server as `trmhavnor`.

```
** Ascend Pipeline Terminal Server **
ascend% show users

I Session     Line:    Slot:  Data    Service     Host           User
O ID          Channel  Port   Rate    Type[mpID]  Address        Name
O 214933581   1:2      9:1    56K     MPP[1]      192.168.4.9    arwp50
O 214933582   1:6      9:2    56K     MPP[1]      MPP Bundle     arwp50
I 214933583   1:1      3:1    28800   Termsrv     N/A            trmhavnor
```

Figure 10. show users command output

Controlling whether RADIUS attributes 6 and 7 are sent

While some RADIUS servers require attributes 6 (user-service) and 7 (framed-protocol) in the authentication requests, other RADIUS servers should not receive them. You can now specify whether Ascend units send values for RADIUS attributes 6 and 7.

In this release, the Auth submenu of the Ethernet (Mod Config) profile contains a new parameter named Auth Send Attr 6, 7. This parameter can be set to Yes to generate the appropriate values for attributes 6 and 7 for an incoming call and send them in authentication requests. For example, incoming PPP calls would have attribute 6 (user-service) set to framed-user and attribute 7 (framed-protocol) set to PPP. The default value is Yes.

Set this value to No if your RADIUS server doesn't require or should not get attributes 6 and 7 in the authentication request.

Set this value to Yes if you want attributes 6 and 7 to be sent to your RADIUS Server in the authentication request, you want to control access to PPP and SLIP via the terminal server explicitly by the RADIUS response, or if you use a MERIT RADIUS server.

Optional prompt before authentication

An extra prompt has been added to the terminal server dialog before authentication that allows the Ascend unit's terminal server to mimic another terminal server's login sequence.

What it resolves

Some ISPs currently use a terminal server that follows a login sequence different from that used by Ascend. You can now configure an additional prompt to accommodate the different login sequence. This change will benefit any ISPs who want the following:

- to upgrade to Ascend from another vendor's terminal server whose dialog includes a menu-selection prior to authentication
- to retain compatibility with existing client software already in use by subscribers that depends upon the older terminal server's dialog

3rd Prompt

Description: You can configure a prompt by specifying the string that will appear with the prompt and where it will appear in the login sequence (first or last). This prompt can emulate an existing terminal server prompt, depending upon what you specify in the prompt string.

Usage: To configure the 3rd prompt:

1 Open the TServ options submenu in the Ethernet Configuration profile.

```
90-B00 Mod Config
 TServ Options
   Cell Level=18
   Telnet=Yes
   Rlogin=Yes
   Def Telnet=No
   Clear Call=No
   Telnet mode=ASCII
   Local Echo=No
   Buffer chars=Yes
   Initial Scrn=Cmd
   Toggle Scrn=Yes
   Security=Partial
   3rd Prompt=Service?
   3rd Prompt Seq=First
   IP Addr Msg=IP address is
   Remote Conf=Nov
```

2 Type a prompt string in the 3rd Prompt= field.

3 Select First or Last for 3rd Prompt Seq to determine where the additional prompt will appear in the login sequence. The default is Last.

Dependencies: The 3rd Prompt feature only works if Auth=RADIUS or Auth=RADIUS/LOGOUT in the Ethernet Configuration Profile.

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

See Also: 3rd Prompt Seq, Auth

3rd Prompt Seq

Description: This parameter specifies whether the 3rd Prompt appears before or after the login and password prompts. It has two possible settings:

- 3rd Prompt Seq=First

  If terminal server security is set to Partial or Full and 3rd Prompt Seq=First, the string specified in the Third Prompt parameter appears when the user connects and the user's input is echoed. After the user enters a Login name and Password, the input in response to the third prompt is passed to RADIUS as part of the authentication request.

  Note: This prompt appears only when the MAX authentication method in the Ethernet Profile is set to RADIUS or RADIUS/LOGOUT.

- 3rd Prompt Seq=Last

  If terminal server security is set to Partial or Full and 3rd Prompt Seq=Last, the Ascend unit sends the user's input to the additional prompt to RADIUS as a part of the authentica-

tion request. The user's input for this prompt is not echoed, since it is treated like an extra password.

Note: This prompt appears only when the MAX authentication method in the Ethernet Profile is set to RADIUS or RADIUS/LOGOUT.

Usage: To specify whether the 3rd Prompt will appear first or last:

1. Open the TServ options submenu in the Ethernet Configuration profile.
2. Type a prompt string in the 3rd Prompt= field.
3. Select First or Last for 3rd Prompt Seq to determine where the additional prompt will appear in the login sequence. The default is Last.

   This field is N/A if TS Enabled=No or 3rd Prompt= is empty. 3rd Prompt Seq=First will work with any authentication method except Auth=None.

Dependencies: The 3rd Prompt feature works slightly differently depending upon whether you specify that it appear in Last position (a prompt issued after the login and password prompts) or the First position (a prompt issued before login and password prompts).

Similarities in the way the 3rd prompt works (First or Last position):

- Both work only when Auth=RADIUS or Auth=RADIUS/LOGOUT
- User's input is passed to RADIUS with the authentication request as the value of the "Ascend-Third-Prompt" attribute.

Differences in the way the 3rd prompt works (First or Last position):

- The First prompt appears before Login & Password prompts, the Last prompt appears after Login & Password prompt

User's input is echoed in response to a First prompt and is not echoed in response to a Last prompt.

See Also: 3rd Prompt, Auth

Radius attribute

The RADIUS attribute Ascend-Third-Prompt stores the user's input in response to the third prompt. The MAX passes the information the user enters to the RADIUS server as the Ascend-Third-Prompt attribute. The Authentication-Request packet contains this attribute.

Input from the user in response to the third prompt in either the Last position (a prompt issued after the login and password prompts) or the First position (a prompt issued before login and password prompts) is sent to the RADIUS server in the Ascend-Third-Prompt attribute as part of the authentication request. This prompt appears to the user only if Auth=RADIUS or Auth=RADIUS/LOGOUT in the Ethernet Configuration Profile. For more information see the MAX Radius Guide.

SNMP variables for tracking load and capacity

SNMP eventGroup fields have been added to keep track of totals relating to call and session events. Version 2.0 of the Ascend Enterprise MIB includes new eventGroup fields that record statistics about the total numbers of calls and sessions.

The Ascend Enterprise MIB has been modified to include new variables for tracking the Ascend unit's load and capacity. This feature tracks the following totals:

- current number of active calls
- current number of active sessions
- total number of calls since system startup
- total number of sessions since system startup
- total number of calls answered since system startup
- total number of calls originated since system startup
- total number of calls cleared since system startup
- total number of data rate changes since system startup
- total number of service changes since system startup
- total number of name changes since system startup

This feature is available in the Ascend Enterprise MIB with the following SNMP version numbers:

```
sysMibVersionNum  - 2
sysMibMinorRevNum - 0
```

The following listing is excerpted from ascend.mib where the OID for the eventGroup is .1.3.6.1.4.1.529.10.

```
eventCurrentActiveCalls      OBJECT-TYPE
     SYNTAX                  INTEGER
     ACCESS                  read-only
     STATUS                  mandatory
     DESCRIPTION             "The number of calls currently
                              active."
     ::= { eventGroup 5 }

eventCurrentActiveSessions   OBJECT-TYPE
     SYNTAX                  INTEGER
     ACCESS                  read-only
     STATUS                  mandatory
     DESCRIPTION             "The number of sessions currently
                              active."
     ::= { eventGroup 6 }

eventTotalCalls              OBJECT-TYPE
     SYNTAX                  Counter
     ACCESS                  read-only
     STATUS                  mandatory
     DESCRIPTION             "The total number of active calls
                              since system startup."
```

```
        ::= { eventGroup 7 }

eventTotalSessions          OBJECT-TYPE
        SYNTAX              Counter
        ACCESS              read-only
        STATUS              mandatory
        DESCRIPTION         "The total number of active sessions
                            since system startup."
        ::= { eventGroup 8 }

eventTotalCallsAnswered     OBJECT-TYPE
        SYNTAX              Counter
        ACCESS              read-only
        STATUS              mandatory
        DESCRIPTION         "The total number of calls answered since
                           system startup."
        ::= { eventGroup 9 }

eventTotalCallsOriginated   OBJECT-TYPE
        SYNTAX              Counter
        ACCESS              read-only
        STATUS              mandatory
        DESCRIPTION         "The total number of calls originated
                            since system startup."
        ::= { eventGroup 10 }

eventTotalCallsCleared      OBJECT-TYPE
        SYNTAX              Counter
        ACCESS              read-only
        STATUS              mandatory
        DESCRIPTION         "The total number of calls cleared since
                           system startup."
        ::= { eventGroup 11 }

eventTotalBaudRateChanges   OBJECT-TYPE
        SYNTAX              Counter
        ACCESS              read-only
        STATUS              mandatory
        DESCRIPTION         "The total number of baud rate change
                            events since system startup."
```

```
        ::= { eventGroup 12 }

    eventTotalServiceChanges   OBJECT-TYPE
        SYNTAX                 Counter
        ACCESS                 read-only
        STATUS                 mandatory
        DESCRIPTION            "The total number of service change
                                events since system startup."
        ::= { eventGroup 13 }

    eventTotalNameChanges      OBJECT-TYPE
        SYNTAX                 Counter
        ACCESS                 read-only
        STATUS                 mandatory
        DESCRIPTION            "The total number of name change events
                               since system startup."
        ::= { eventGroup 14 }
```

MPP should drop newest B channel first

The order in which MPP drops channels when bandwidth is decreased has changed.

Super-Call-ID for billing of multi-channel calls

The SNMP Super-Call-ID feature keeps track of the calls associated with a multi-channel MP or MP+ session.Version 2.0 of the Ascend Enterprise MIB includes a new eventTable object that enables customers to use SNMP records to bill multi-channel sessions. This feature was available previously only in the RADIUS Accounting End Record.

Super-Call-ID adds to SNMP a feature that was previously available only in the Ascend-Multilink-ID (187) attribute. This feature enables customers to use SNMP event records to bill multi-channel sessions. It is available in the Ascend Enterprise MIB with the following SNMP version numbers:

sysMibVersionNum - 2
sysMibMinorRevNum - 0

The eventMultiLinkID object has been added to the eventTable in ascend.mib. The eventMultiLinkID object applies to sessions that are part of a multilink bundle.The object returns 0 (zero) unless eventType is one of the following types:

- callCleared(3)
- serviceChanged(4)
- NameChanged(5)

The eventMultiLinkID object is defined as follows:

Name: .iso.org.dod.internet.private.enterprises.ascend.eventGroup.

eventTable.eventEntry.eventMultiLinkID

OID: .1.3.6.1.4.1.529.10.4.1.22

Modem transmit level can now be set

This feature allows users to modify the internal transmit level of the Rockwell digital modems.

How it works

A new parameter has been added to make the transmit level seen by the codec within a digital modem be programmable. By transmitting at higher level, it helps certain modems on their near-end-echo problems.

The new parameter is MDM Trn Level parameter in Ethernet>Mod Config>Term Serv Options.

The default setting -13 (db) is the default behavior of the digital modems prior to this feature.

10 modem pools configurable from WAN Options menu

The number of static address pools you can configure from the WAN options submenu of the Ethernet Configuration Profile has been increased to a maximum of 10 pools. Previously, you could configure a maximum of two pools.

How it works

An address pool is a group of IP addresses used in dynamic IP addressing. If Assign Adrs=Yes, the MAX tries to assign an IP address to the calling device (performs dynamic IP). The MAX asks the calling device to accept an assigned address chosen from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters in the WAN Options submenu of the Ethernet Configuration Profile. If the calling end accepts the IP address, the MAX sets the LAN Adrs parameter in the Connection Profile to the assigned address.

This feature enables you to specify up to ten address pools using the Pool #n Start and Pool #n Count parameters. Previously, although you could define address pools 1 through 50 in an address pool user file downloaded from the RADIUS server, you could define only two pools using the Pool #n parameters without RADIUS.

See the *MAX Reference Guide* for more information about these parameters.

Configuring address pools

To configure an address pool without RADIUS:

1. Set Encaps=PPP in the appropriate Connection Profile.
2. Open the Ethernet Answer Profile.
3. Select Assign Adrs=Yes in the Ethernet Answer Profile.
4. Open the WAN options submenu of the Ethernet Profile.
5. Select Pool #n Start and press Enter to open a text field.
6. Type the first IP address in the pool.

   The address you specify does not ned to be on the same LAN segment as the MAX. The MAX chooses an address from the pool and assigns it to an incoming call when Assign Adrs=Yes or when the calling station requests an address assignment.

   The default is 0.0.0.0.

   If Pool is null and Assign Adrs=Yes, the MAX gets IP addresses from the first defined address pool.

   Note: You can define address pools 1 through 10 using the Pool #*n* Start and Pool #*n* Count parameters, but these pools are superseded by RADIUS pools 1 through 10, if they exist.
7. Press Enter again to close the text field.
8. Select Pool #n Count and press Enter to open a text field.
9. Enter a number between 0 and 254.

   This parameter specifies the number of IP addresses in IP address pool n.

   The default is 0 (zero).
10. Press Enter again to close the text field.
11. Repeat Step 1 through Step 10 to define up to ten starting addresses for ten different pools.

Note: If you do not set the Pool #*n* Start and Pool #*n* Count parameters, the Assign Adrs parameter is N/A.

RADIUS changes

There has been no change to the way RADIUS works with modem address pools. Pool definitions from RADIUS either override NVRAM entries (entries configured from the WAN Options submenu of the Ethernet Configuration Profile) or supplement them. For example, if you configure the following:

1-10	11, 12	1-10 (NVRAM) plus 11 and 12 (from RADIUS)

NVRAM Entries Defined	#RADIUS entries	Result after loading
1, 2	5, 6	1, 2,5,6
1, 2 1-10	2, 6	1, 2, 6 Pools 2 and 6 are configured in RADIUS.

Enhanced RADIUS support for bridging connections

RADIUS-specified dialout connections can now be brought up based on ARP requests.An earlier software release enabled RADIUS configuration of bridging table entries. However, only a resident Connection profile could bring up the required connection. In this release, the Ascend unit can download a RADIUS profile to bring up the required connection.

A previous software release enabled administrators to create pseudo-user entries to add MAC addresses and their associated IP addresses to the ARP table. When the MAX received an ARP request for one of the specified IP addresses, it responded with the corresponding MAC address and used the IP address to bring up a Connection profile to that remote address. In this release, the feature has been enhanced to enable the MAX to download a RADIUS profile if no resident Connection profile is found to bring up the required connection.

The RADIUS database entries use this format:

```
#  bridge-<unit-name>-<number> Password = "ascend", User-Service =
Dialout-Framed-User
#  Ascend-Bridge-Address = "<MAC-address> <profile-name> <IP-address>"
```

These are the related elements:

- bridge-<unit_name>-<number>
  The unit-specific bridging entry.
  - <unit_name>
    The system name of the Ascend unit—that is, the name specified by the Name parameter in the System Profile.
  - <number>
    A number in a sequential series, starting at 1. The MAX named <unit_name> queries bridge-<unit_name>-1, then bridge-<unit_name>-2, then bridge-<unit_name>-3, until it receives an authentication reject from RADIUS.
- Ascend-Bridge-Address
  The value assigned to the Ascend-Bridge-Address attribute includes these elements:
  - <MAC-address>

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".

– <profile-name>

The name of a dialout Connection profile. If this profile is not resident in the MAX, the MAX will attempt to download it from the RADIUS database of dialout profiles.

– <IP-address>

The IP address associated with the MAC address, specified in dotted decimal format. This element is optional. If it is specified, both the MAC address and this IP address are added to the ARP table.

These are some sample RADIUS dialout profiles and related RADIUS bridge-address pseudo-user entries:

```
prof2 Password="ascend"
        User-Service=Dialout-Framed-User
        Framed-Protocol = MPP,
        Ascend-Bridge = Bridge-Yes,
        Ascend-Idle-Limit = 0,
        Ascend-Dial-Number = 98797,
        Ascend-Send-Auth = Send-Auth-CHAP,
        Ascend-Send-Secret="test"


prof1 Password="ascend"
        User-Service=Dialout-Framed-User
        Framed-Protocol = MPP,
        Ascend-Bridge = Bridge-Yes,
        Ascend-Idle-Limit = 0,
        Ascend-Dial-Number = 98797,
        Ascend-Send-Auth = Send-Auth-CHAP,
        Ascend-Send-Secret="test"


bridge-maxp-1 Password = "ascend", User-Service = Dialout-Framed-User
        Ascend-Bridge-Address = "2:2:3:10:11:12 prof1 1.2.3.4"
        Ascend-Bridge-Address = "2:2:3:13:14:15 prof2 5.6.7.8"


bridge-maxp-2 Password="ascend" User-Service=Dialout-Framed-User
        Ascend-Bridge-Address = "00:80:cc:cc:cc:cc prof1 10.1.1.1"
        Ascend-Bridge-Address = "00:80:bb:bb:bb:bb prof1 20.1.1.1"
        Ascend-Bridge-Address = "00:80:dd:dd:dd:dd prof1"
        Ascend-Bridge-Address = "00:80:ee:ee:ee:ee prof1 40.1.1.1"
        Ascend-Bridge-Address = "00:80:aa:aa:aa:aa prof1 50.1.1.1"
```

Busy modem list added to SNMP

A sub-group that lists the modems currently being used for outgoing or incoming calls has been added to the Ascend MIB. This feature enables you to automate service management, including modem maintenance, to scale service and add capacity.

Ascend MIB changes

The busyLanModem subgroup has been added to the lanModemGroup in the Ascend MIB.

Note: The SNMP and LMODEM features must be enabled in order to monitor the modem usage.

```
busyLanModem       OBJECT-TYPE
    SYNTAX          INTEGER
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The number of lan modems in the
                     busyLanModemTable."
    ::= { lanModemGroup 9 }

busyLanModemTable  OBJECT-TYPE
    SYNTAX          SEQUENCE OF BusyLanModemEntry
    ACCESS          not-accessible
    STATUS          mandatory
    DESCRIPTION     "The lan modems in this table are busy
                     answering or placing calls."
    ::= { lanModemGroup 10 }

busyLanModemEntry  OBJECT-TYPE
    SYNTAX          BusyLanModemEntry
    ACCESS          not-accessible
    STATUS          mandatory
    DESCRIPTION     "The properties associated with the
                     entries in the busyLanModemTable."
    INDEX           { busyLanModemSlotIndex,
                      busyLanModemPortIndex }
    ::= { busyLanModemTable 1 }

BusyLanModemEntry ::=
    SEQUENCE {
        busyLanModemSlotIndex
            INTEGER,
        busyLanModemPortIndex
            INTEGER,
        busyLanModemUsedCount
            Counter,
        busyLanModemBadCount
```

```
            Counter,
        busyLanModemLast32
            INTEGER,
        busyDirection
            INTEGER
    }

busyLanModemSlotIndex      OBJECT-TYPE
    SYNTAX          INTEGER
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The slot number corresponding to the lan
                    modem."
    ::= { busyLanModemEntry 1 }

busyLanModemPortIndex      OBJECT-TYPE
    SYNTAX          INTEGER
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The port number corresponding to the
                     lan modem."
    ::= { busyLanModemEntry 2 }

busyLanModemUsedCount      OBJECT-TYPE
    SYNTAX          Counter
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The number of times the lan modem was
                     utilized."
    ::= { busyLanModemEntry 3 }

busyLanModemBadCount       OBJECT-TYPE
    SYNTAX          Counter
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The number of times the lan modem
                     failed."
    ::= { busyLanModemEntry 4 }

busyLanModemLast32 OBJECT-TYPE
```

```
    SYNTAX          INTEGER
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "A 32-bit mask of the last 32 times
                    the lan modem was tried. A '0' in the
                      bit position indicates failure while an '1'
                    indicates success."
    ::= { busyLanModemEntry 5 }

busyDirection      OBJECT-TYPE
    SYNTAXINTEGER {
                        callUnknown(1),
      callOriginated(2),-- unit dialed out
      callAnswered(3)-- unit answered call
    }
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "Distinguishes incoming from outgoing calls."
    ::= { busyLanModemEntry 6 }


suspectTrapState OBJECT-TYPE
    SYNTAX  INTEGER { enabled(1), disabled(2) }
    ACCESS   read-write
    STATUS   mandatory
    DESCRIPTION
             "This variable  indicates  whether  the  system
             produces the lanModemMovedToSuspectList trap. It
             will be automatically enabled after restart."
    DEFVAL { enabled }
    ::= { lanModemGroup 11 }
```

Active sessions indexed by session ID

This feature allows the MAX to determine whether more than one user is connected using the same user profile.

Active sessions indexed by the session ID

The MAX creates unique session IDs for users when they connect. This feature allows an SNMP manager to determine whether more than one user is connected to the MAX using the same session ID.

As part of the feature a sessionActiveTable has been added to the Ascend MIB. This table is similar to the sessionStatusTable but is indexed by the ssnActiveCallReferenceNum object. If the ssnActiveCallReferenceNum (in the sessionActiveTable) is the same as the ssnStatusCallReferenceNum (in the sessionStatusTable), this implies that the previous session is still active. This feature can be used to make sure that multiple users are not connected using the same user profile.

New MIB objects

The following MIB objects have been added to the Ascend MIB.

```
sessionActiveTable  OBJECT-TYPE
 STATUS mandatory
 DESCRIPTION"A list of active session entries.
                      This table is similar to sessionStatusTable
                    with invalid entries screened out and indexed
                    by ssnActiveCallReferenceNum.
                    ssnActiveCallReferenceNum tracks
                    ssnStatusCallReferenceNum of
                    sessionStatusTable."
 ::= { sessionActiveGroup 3 }


 sessionActiveEntryOBJECT-TYPE
 SYNTAX SessionActiveEntry
 ACCESS not-accessible
 STATUS mandatory
 DESCRIPTION"An entry containing object variables to describe
           an active session."
 INDEX  { ssnActiveCallReferenceNum }
 ::= { sessionActiveTable 1 }
 SessionActiveEntry ::=
 SEQUENCE {
     ssnActiveCallReferenceNum
    INTEGER,
     ssnActiveIndex
    INTEGER,
     ssnActiveValidFlag
    INTEGER,
```

```
    ssnActiveUserName
   DisplayString,
    ssnActiveUserIPAddress
   IpAddress,
    ssnActiveUserSubnetMask
   IpAddress,
    ssnActiveCurrentService
   INTEGER
}

 ssnActiveCallReferenceNum  OBJECT-TYPE
SYNTAX INTEGER (1..'7fffffff'h)
ACCESS read-only
STATUS mandatory
DESCRIPTION"A unique number identifying this active session.
            Refer to ssnStatusCallReferenceNum for more
            information."
::= { sessionActiveEntry 1 }

 ssnActiveIndexOBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION"The index number for this session status entry. Its
          value ranges from 1 to 'ssnStatusMaximumSessions'.
          Refer to ssnStatusIndex for more information."
::= { sessionActiveEntry 2 }

 ssnActiveValidFlag  OBJECT-TYPE
SYNTAX INTEGER {
          invalid(1),
          valid(2)
      }
ACCESS read-only
STATUS mandatory
DESCRIPTION"All entries will be valid(2).
           Refer to ssnStatusValidFlag for more information."
::= { sessionActiveEntry 3 }

 ssnActiveUserName   OBJECT-TYPE
```

```
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION"The name of the remote user.
          Refer to ssnStatusUserName for more information."
::= { sessionActiveEntry 4 }

 ssnActiveUserIPAddressOBJECT-TYPE
SYNTAX IpAddress
ACCESS read-only
STATUS mandatory
DESCRIPTION"The IP address of the remote user.
            Refer to ssnStatusUserIPAddress for more information."
::= { sessionActiveEntry 5 }

 ssnActiveUserSubnetMask OBJECT-TYPE
SYNTAX IpAddress
ACCESS read-only
STATUS mandatory
DESCRIPTION"The subnet mask of the remote user.
           Refer to ssnStatusUserSubnetMask for more information."
::= { sessionActiveEntry 6 }

 ssnActiveCurrentService OBJECT-TYPE
SYNTAX INTEGER {
          none(1),
          other(2), -- none of the following
          ppp(3), -- Point-To-Point Protocol
          slip(4), -- Serial Line IP
          mpp(5), -- Multichannel PPP
          x25(6), -- X.25
          combinet(7), -- Combinet
          frameRelay(8), -- Frame Relay
          euraw(9),
          euui(10),
          telnet(11), -- telnet
          telnetBinary(12), -- binary telnet
          rawTcp(13), -- raw TCP
          terminalServer(14), -- terminal server
          mp(15) -- Multilink PPP
```

```
        }
ACCESS read-only
STATUS mandatory
DESCRIPTION"The current service provided to the remote user.
        The value none(1) is returned if entry is invalid
        OR if user dials into the terminal server and is
        in midst of a login sequence.
         Refer to ssnStatusCurrentService for more information."
::= { sessionActiveEntry 7 }
```

Additional features not in the user documentation

Expect callback parameter added to dialout profile

A parameter has been added to the Telco options submenu of the Connections menu for configuring an Ascend MAX to expect a callback from the machine called. This prevents problems that arise when CLID is set to Required on the machine that is expected to callback.

How expect callback works

When an Ascend machine initiates a call and the call gets through, the called machine hangs up on the incoming caller and then immediately initiates a call to that destination (callback) before performing password authentication.

For example, in Figure 11 ping or telnet is initiated through a MAX to a Pipeline and CLID is set to Required on the Pipeline (the side that will be doing the callback), the Pipeline rejects the incoming call before answering it. To the MAX (the initiating side), it appears as if the call never got through at all.

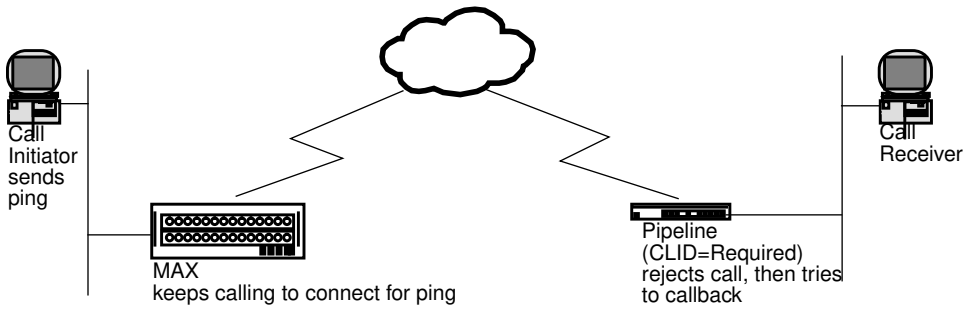


Figure 11. Callback connection failure

This is a special problem for ping and telnet, because these processes try continuously to open a connection and reject any callback because the process is already trying establish a connection.

When Expect Callback is set to Yes, calls that dialout and do not connect (for any reason) will be put on a list that disallows any further calls to that destination for 90 seconds. This gives the far end an opportunity to complete the callback.

Enabling Expect Callback on MAX

Expect Callback should only be set to Yes (TRUE) in dialout profiles, and not used for incoming calls.

To set Expect Callback to Yes:

1 Open Ethernet>Connections>Any Profile>Telco.

2 Set Exp Callback to Yes.

Note: If a call fails for any reason, regardless of whether or not the called machine requires CLID and is attempting a callback, the call initiator will still have to wait 90 seconds before attempting the call the same number again if Expect Callback is set to Yes.

New RADIUS attribute added

Ascend-Expect-Callback was added to the RADIUS dictionary to enable Expect Callback

Ascend-Expect-Callback

Description: Ascend-Expect-Callback enables or disables Expect Callback, so that a the call initiator will wait 90 seconds after placing a call, to prevent a connection failure where the called machine hangs up and tries to callback while the initiating machine continues to try to call.

Usage: The possible values for this attribute are two integers:

Expect-Callback-No =0 disables Expect Callback. The initiating machine will not wait for a callback after placing a call.

Expect-Callback-Yes =1 enables Expect Callback. The initiating machine will wait for 90 seconds after placing a call before attempting to place another call to the same number.

Additional sample available for DTMF decode

A parameter has been added to the Net/T1 Line Profile allowing the PRI-T1 conversion process to use one or two sets of Goertzel samples to do the DTMF tone detection. The MAX currently uses only one sample to decode signals from robbed-bit PBXs. The PRI-T1 conversion process is more accurate when the MAX can use two samples.

The use of only one sample supports standard tone durations and other PBXs that use a non-standard tone duration of less than 50ms. This duration is not enough for computing the Goertzel algorithm with two sample sets. Using one sample set seems to work with most PBXs, in most cases, but using two samples is more accurate. Where the tone duration is long (more than 70ms), setting the Input Sample Count to Two is recommended.

Configuring PBX-T1 to use two sample sets

To configure a PBX-T1 line to use two sample sets for DTMF tone detection:

1 Open the current Net/T1 Line Profile (Line Config menu).
The example shows part of the Line Profile with the new parameter added.

```
Edit
20-1** Factory
 >Sig Mode=PBX T1
  NFAS ID num=N/A
  Rob Ctrl=Wink-Start
     . . .
  Ans#=
  Ans Service=Voice
  Input Sample Count=One
```

2 For Input Sample Count select Two.
This field has only two possible values, one (the default) or two. Selecting two configures the MAX to use 2 sample sets for DTMF detection.

Note: The Input Sample Count parameter is set to N/A if the Sig Mode is not PBX-T1.

3 Exit the Line Profile menu.

Silent mode parameter added

Information about the Silent mode configuration option was missing from the user documentation. You can use this option to reduce the number of status messages sent to a modem caller using the Terminal Server.

How the silent option works

Previously, status messages intended to be read by a human terminal server user were sent to all modem callers, including automated applications. Enabling the Silent mode means that certain of these messages are not sent, reducing the amount of unnecessary traffic.

Currently the status messages include, but are not limited to:

- Connecting to [hostname] ...)
- Connected.
- Connection failed.
- Connection closed....logging off.)
- Not connected.
- Escape character is disabled, binary mode selected.
- Binary mode rejected, Escape character is ^].

Enabling Silent mode

You enable Silent mode operation and preventing status messages from being sent across the network connection by setting Silent=Yes in the TServ options submenu of the Ethernet Mod Config menu. The default value is No.

Problems corrected in this release

TR 918 Two MP connections to MAX caused second system to reboot.

There were conflicting endpoint identifiers in the MP calls. These identifiers were removed and now complete simultaneous MP calls can be made.

TR 1128 Removed excess trace generated by warning 182.

Occasionally, the number of channels active on the MAX did not match the number of actual active sessions.

TR 1154 X25/PAD: Enlarge auto-call field.

The MAX did not properly handle output flow control of the X.25 host with modem speeds slower than a host speed of 9600. At higher speeds (14,400 or greater) this problem was not observed. To enable the customer to supply more information about the call, the auto call field was increased to allow users to specify Call User Data (CUD) parameters (specifically, the *D and *P features of the PAD). Now the auto call input field is 48 bytes in length, which accepts a 15-byte X.121 address and the required CUD parameters.

TR 1162 User could not launch a PPP or SLIP session.

If the RADIUS user-service attribute was not specified, user could not launch a PPP or SLIP session.

TR 1168 Bad negotiation of MRRU hung Cisco, Yamaha routers.

With one-channel MP calls, pings with packets greater than 1472 time out. With two-channel MP calls, pings with packets greater than 1470 time out. When two Pipelines are involved, all pings are successful.

TR 1189 Switching from "Perm/Switched" to "Switched" cause Idle to go to 0.

Changing the Call Type setting from Perm/Switched to Switched did not change the idle parameter appropriately. The solution was to set the Idle parameter to the factory default of 120 when switching from Perm/Switched to Switched.

TR 1217 MS-Stac compression did not work.

When a Windows 95 client called a MAX (configured for MS-Stac), the Windows 95 client rejected MS-Stac and accepted a Stac request instead.

TR 1245 MAX with BRI- SNMP reports incorrect ifadmin stats.

The MAX incorrectly reported ifAdminStatus. All BRI lines would be reported to be up even if the lines were not enabled.

TR 1251 Local connection profile was WAN0 whether link was up or not.

For a MAX with frame relay connections, any locally defined Connection Profile with a different subnet class, would show up as WAN0 whether the link was up or not.

TR 1262 Working Terminal Sessions don't work after upgrade to 4.6B.

After upgrading to 4.6B, async connections would be dropped (with code 52 - invalid telnet host) after the ID and password were entered if the Login-Service specified was TCP-Clear and no TCP host (Login-Host attribute) was specified. Prior to 4.6B, Login-Host was not required. To restore the unit to pre-4.6B behavior, the Auth TS Secure parameter was added.

TR 1269 Users showed connection to a MAX but were not actually active.

The MAX was collecting phantom sessions in the Dyn Stats window even when users were no longer connected. There were conflicting endpoint identifiers in the MP calls. These identifiers were removed and now the Dyn Stats window accurately displays an active user connection.

TR 1270 Reduced incidence of type 1 disconnect records.

Running 4.6Bp6 software: Switched to a framed protocol from the terminal server and in response to a successful PPP hunt, the login prompt generated an extra RADIUS STOP record. This record contained an uninitialized Disconnect code.

TR 1289 Customer could not see any traffic over nailed link.

Using an SNMP application to monitor status and bandwidth utilization, SNMP saw the nailed link on wan0 as a Frame Relay link, but did not show packet traffic in IfOutOctets of MIB-2. Furthermore, it showed the link speed as 64k. The link speed should have been 128k.

TR 1295 Calls rejected because of CLID authentication failure did not return User Busy.

When CLID is required in a Connection profile, and a call failed to present the required CLID, the Ascend unit did not answer the call and did not give the caller a busy signal. It is now possible to configure the Ascend unit to return a busy signal or not. See the CLID Timeout Busy (MAX units only) and CLID Fail Busy (all Ascend units except the Pipeline 25 PX) parameters in this release note for further information.

TR 1324 Telnet to Unisys server fails.

Telnet from an Ascend unit to a Unisys SVR4 server did not work.

TR 1344 MAX 4.6Ct3 PPP negotiation didn't work with Trumpet Winsock.

Trumpet Winsock dialing into an Ascend unit with 4.6Ct3 software failed PPP negotiations. The problem has been corrected.

TR 1346 MAX reset with no fatal error log.

Overruns on the Ethernet flooded the system with high-priority interrupts, which slowed performance severely. This caused the watch dog to expire, resetting the Max.

TR 1365 "Ascend-Authen-Alias" attribute is not supported.

Support for "Ascend-Authen-Alias" was not included in 4.6Bi19, which is now corrected.

TR 1368 Callback stops working after several hours.

Callbacks worked normally under heavy load for about 18 hours, then failed to return calls. On some models, though, callback failed immediately.

TR 1371 When a Stack call clears, route did not age out. Subsequent calls fail.

On a MAX using Multichassis MPP, when a Pipeline with two active channels disconnected, the route associated with the Pipeline continued to be advertised long after the Pipeline had completely disconnected.

TR 1395 If pool1 is used, pool2 won't be used.

When no pool was specified via RADIUS, a pool of 1 address was defined. The first user logged in and was assigned an address. The second user would be unsuccessful. This second user was successful if he logged in first.

TR 1397 Expect callback parameter enabled.

With the Expect Callback parameter enabled, the Ascend unit waited 90 seconds to ping again before establishing another session.

TR 1405 12-mod modems stop answering calls after a while.

12-mod modem cards stop answering calls after a while. Debug message showed that modem driver ran out of transmit buffers. Now, a threshold of 18 transmit buffers can be allocated to each modem.

TR 1414 RADIUS - IPX static routes did not work.

If static routes are defined using a connection profile they work as expected, but when they need to go through RADIUS, the route is not added to the routing table. If IPX packets attempt to bring up a connection, the call is started, but it is not possible to reach the NetWare server at the other end.

TR 1422 PC dialing into Ascend unit received invalid IPX route if authentication was turned off.

Ascend units assumed incoming IPX calls were from routers, unless the authenticating Connection (or RADIUS) profile specified it was from a PC. The Connection profile parameter, Peer, has been added to the Answer profile to allow the MAX to treat incoming IPX connections as either PC calls (Client) or router calls (Dialin). See Peer in these release notes.

TR 1423 Stack problems on MAX.

With two MAX units, each with 2 PRI connections and each using a different ISDN number, calls would not be cleared from the stack properly, even though they appeared to clear gracefully. After multiple calls that should have been cleared, PRI would show Ring/Answer, but the calls crashed. In other instances IP connectivity would be lost.

TR 1425 Static bridge addresses age out from ARP table in about 10 minutes.

Static Bridge Addresses time out of the ARP table in about 10 minutes. A reset of the box brings the addresses back.

TR 1453 Max resets with fatal error 29.

If a caller hung up midway through the display of the terminal server banner, the memory pool would get corrupted. After a number of these incidents, the MAX would reset.

TR 1469 RADIUS IPX routes don't age when connection clears.

If a user profile is set up specifying both and IP and IPX routes, when a call clears, the IP route clears, but the IPX route never goes away.

TR 1499 MAX profile in RADIUS was not removing memory.

RADIUS was not deleting a defined Frame Relay profile from the MAX, even though RADIUS no longer contained that profile.

TR 1505 SNMP callStatusHighWaterMark returns wrong value.

When callStatusHighWaterMark is queried, the MAX responds with the number of calls on the system. If callStatusHighWaterMark is reset to 0 it continues to display 0 until the number of new calls answered exceed the number of calls on the MAX when callStatusHighWaterMark was reset.

TR 1513 MAX using OSPF would reset under heavy traffic.

The MAX, configured for OSPF, would run out of memory under heavy traffic.

TR 1515 3rd Prompt no longer passed to RADIUS in auth. request packet.

In 3.6Ci5, when the the 3rd Prompt Seq parameter was added, the 3rd Prompt failed to get passed to RADIUS in the authentication request packet, regardless of whether it appeared first or last.

TR 1574 MAX reset.

Running 4.6C software: Memory problems were occurring because of an invalid RADIUS configuration.

TR 1577 Login sequence has changed.

Running 4.6Ci12 software: Login sequence changed for RADIUS logins. The RADIUS challenge responses are no longer echoed as "*'". The RADIUS login sequence has been restored to the way it was in 4.6B.

TR 1587 IPX routes did not age when connection profile was deactivated.

Running 4.6Ci12 software: When deactivating a Connection Profile (by setting Active=No) the configured IP route was aged out, but for IPX, the route did not age.

TR 1618 MAX resets.

Running 4.6Cp9 software: The MAX would reset occasionally with Fatal Error 29 if encapsulation was set to TCP-Clear and Buffer Chars was set to No.

TR 1619 Turn off TRACK_DISCONNECTS debug

Running 4.6Ci10 software: At random times, users would get a busy signal, when trying to access the MAX 4004. The telephone company looked at the line condition and saw that the MAX was outputting a busy condition.

TR 1622 MAX sends wrong bearer capability for outgoing modem calls.

Running 4.6Ci14 software: In Germany, a client dialing out through the MAX using MAXDial could not connect to an ISDN network. This was due to the MAX sending the wrong bearer capability.

TR 1629 MP Stack - Second channel failed on the MAX.

Running 4.6Cp10 software: Two channel calls were established where the first channel accesses the first MAX and the second channel accesses the second MAX. If the second channel failed (on-site the customer had a second channel failing authentication), then all subsequent two-channel calls into the MAX would fail.

TR 1638 MAX occasionally resets.

Running 4.6Cp11 software: The MAX would occasionally reset with Fatal Error 29 when tearing down stack connections.

TR 1662 SNMP: ipAdEntIfIndex didn't match ifIndex.

Running 4.6Ci17 software: ipAdEntIfIndex showed the IP Address of the box pointing to 1. This was incorrect; needed to be the same value as ifIndex.

TR 1664 When CLID failed, call was not answered.

Running 4.6Ci17 software: When CLID Auth is set to Prefer or Require, the MAX would fail to answer the call.

TR 1667 MAX received a Fatal Warning 104.

Running the mhpt1 software, the MAX occasionally received a fatal warning.

TR 1684 Inactivity timer not started for CLID authentication call.

Running 4.6Ci14 software: On a MAX, the inactivity timer did not start on a call with CLID authentication.

TR 1691 MAX Call Duration could not be disabled once value was set

Running 4.6Ci17 software: The MAX Call Duration parameter could not be set and saved to zero if it had been previously set to a value in the 1 - 1440 range.

TR 1693 SNMP: MAX 4000 reported wrong ifAdminStatus.

Running 4.6Ci17 software: When a MAX with a WAN1 was configured with line 1=trunk and line 2=disabled, line 1 was disabled and should not have been.

TR 1699 New Ascend SNMP MIB variables had the same values as in 4.6Cp10.

Running 4.6Ci18 software: New Ascend SNMP MIB variables (sysMibVersionNum and sysMibMinorRevNum) did not correctly report changes in the Ascend MIB.

TR 1700 After 18-20 callers, MAX would send busy signals to subsequent callers.

Running 4.6Ci18 software: After 18-20 callers would successfully connect, the MAX would send busy signals to subsequent callers and not allow them to connect.

TR 1710 MAX reset with FE using TACACS+ accounting and WAN port.

Running 4.6Ci18 software: When the MAX was connected over a serial WAN connection to a Cisco 4500, the MAX reset immediately until the V.35 cable was disconnected. If the connection profile was turned off, the MAX was reset, everything would work out fine until the connection profile was re-enabled.

TR 1712 PPP communication failed between Netopia or WebRamp and the MAX.

Running 4.6Ci18 software: PPP negotiations between Netopia and WebRamp routers and the MAX would fail. This was caused by the inability of the Netopia and WebRamp routers to handle BACP negotiation.

TR 1714 After a period of time, the MAX would stop answering analog callers.

Running 4.6Ci18 software: After a period of time, the MAX digital modems would stop answering calls from users dialing in over analog lines. This problem did not affect users dialing in over ISDN lines.

TR 1726 OSPF routes not always deleted properly from the IP route table.

Running 4.6Ci18 software: MAX units running OSPF were not properly deleting inactive routes from their routing tables.

TR 1734 PBX-T1 conversion wasn't functioning with Data Call option installed.

Running 4.6Cp9 software: On a MAX outbound calls failed when originating from the PBX but inbound calls were normal when originating from the network side.

TR 1735 When Livingston Enterprise's PortMaster called MAX, CHAP broke

Running 4.6Ci18 software: PPP/Auth broke if peer sent any NCP before AUTH was completed, i.e., the MAX was setup for Recv Auth=CHAP, but before the MAX received a message digest from peer. The peer sent an IPCP request. In this case, the MAX would go ahead and open Auth and start NCP negotiations.

TR 1737 Large SNMP PDU size

Running 4.6Cp14 software: To support the new eventTable OIDS, there was a size limit to the SNMP request packet. Packets larger than about 480 bytes of data caused the problem.

TR 1751 MAX did not negotiate nack of telnet terminal-type option

Running 4.6Ci18 software: Telnet negotiation looped. Fujitsu's telnet server did not support the telnet terminal type option.

TR 1767 Immediate Telnet/CLID Auth-Radius not working

Running 4.6Ci22 software: The MAX 4000 answered a call and performed a RADIUS lookup. While the MAX still used the calling number, the RADIUS request used the actual called number.

TR 1780 Immediate Telnet didn't work with TACACS+ authentication.

Running 4.6Ci22 software: On a MAX 4004 - This version of code did not allow Immediate Telnet with TACACS+ authentication.

TR 1812 OSPF routes not advertised when RADIUS Route Stacking used.

Running 4.6Ci24 software: When RADIUS Route Stacking was used, OSPF did not propagate the correct routes.

TR 1817 MAX 4000 occasionally reset with fatal error.

Running 4.6Ci24 software: the MAX 4000 was resetting with a fatal error.

NA Rockwell modem code version 1.600G5+ updated.

Rockwell modem code updated to improve connectivity.

Upgrading system software

To upgrade your Ascend product 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 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 Ascend product configuration to your computer's hard disk.

Note: Uploading system software overwrites all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. At the end of this process, restore your profiles from the backup file you created. Since the backup file is readable text, you can reenter the settings through the Ascend product's user interface.

For further information, 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 Ascend product.

7 Your communications program begins sending the binary file to your Ascend product. 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 Ascend product resets itself. When the self-test is complete, the Ascend product's initial menu 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.