MAX Cumulative Release Note 6.1.24

Ascend Communications, Inc.
Preliminary January 26, 1999

This *Cumulative Release Note* describes new features and corrections introduced in True Access™ Operating System (TAOS) releases after 6.1.0 for the MAX.

Ascend's TAOS runs on Ascend's advanced WAN Access products. These products provide modular chassis that integrate a range of technologies to enable service providers and enterprise managers to install customized network infrastructures.

TAOS consists of two major components: an embedded kernel and extensions. The kernel provides foundation features for WAN access environments. The extensions provide software solutions that extend the range and depth of WAN access support.

Caution: You must use the software loading procedure explained in "Upgrading your system software" on page 16 to load this version of software onto your system. Read the instructions carefully before upgrading your system.

What's new in 6.1.24

This *Cumulative Release Note* describes enhancements and corrections introduced in software releases after 6.1.0 for the MAX. Releases since 6.1.0 have been cumulative. This current release, 6.1.24, includes all changes in releases from 6.1.0.

The first section of the release note, "What's new in 6.1.24" on page 1, describes changes in the current release, including:

The next section, "Known issues in 6.1.24" on page 7, contains information you should review before you upgrade to the new release.

Also in these release notes

Subsequent sections of the *Cumulative Release Note* describe changes in interim releases from 6.1.0 to 6.1.24, all of which are encompassed in this cumulative release, including:

– “High-speed modem technology” on page 15

The last section, “Upgrading your system software” on page 16, describes how to upgrade or downgrade your system software.

How to use this release note

To use this release note:

1. Read through the release note to determine which software release applies to your environment.
2. Obtain the file from the Ascend anonymous FTP server (`ftp.ascend.com`). If you need Technical Assistance, see the next section.

   Note: If you are already on a 6.1.x release, you only need to load the “f” binary, as described in “Upgrading your system software” on page 16.
3. Upgrade to the new software by following the instructions in “Upgrading your system software.” Then configure the features that apply to your site.

How to obtain technical assistance

You can obtain technical assistance by telephone, email, fax, or modem, or over the Internet.

Enabling Ascend to assist you

If you need to contact Ascend for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model.
- Software and hardware options.
- Software version.
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your product.
- Your local telephone company’s switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1.
- Whether you are routing or bridging with your Ascend product.
- Type of computer you are using.
- Description of the problem.

Calling Ascend from within the United States

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

Priority Technical Assistance

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

Ascend Advantage Pak

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

Other telephone numbers

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

Contacting Ascend from outside the United States

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

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

Note: For a list of support options in the Asia Pacific Region, refer to `http://apac.ascend.com`

Obtaining assistance through correspondence

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

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

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

Finding information and software on the Internet

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

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

Contents

Upgrading your system software 16

What’s new in 6.1.24

Changes in Release 6.1.24 include:

- Enhancements described in “Enhancements in 6.1.24”
- Trouble Report (TR) corrections listed in Table 1 on page 3
- Rockwell code versions listed in “Known issues in 6.1.24” on page 7

Release 6.1.24 also includes the changes and enhancements included in the interim releases published from 6.1.0, which are documented in later sections of this release note.

Enhancements in 6.1.24

Modifications to Id Auth parameter

Ascend units affected: MAX 6000, MAX 1800, MAX 2000

Introduced in: 6.1.24

With this release, the Id Auth parameter supports two additional values: First and Called First.

Modified Parameter

Id Auth

Description: Specifies how CLID (calling line ID) or DNIS (Dial Number Information Service) should be used for authentication.

Usage: Specify one of the following values:

- Ignore (the default)

  Don't require a matching ID from incoming calls.
- Prefer

  Authenticate using the CLID if available, otherwise fall back to using PAP or CHAP authentication. If CLID is available and CLID authentication fails, the MAX clears the call.
- Require

  The CLID must be valid and match the value in a configured profile. If the profile also requires password authentication, do that as well.
- Fallback

  Authenticate using the CLID when RADIUS is available, otherwise fall back to using password authentication.
- Called Require

  The called number must be valid and match the Calling # value in a configured profile. If the profile also requires password authentication, do that as well.

- Called Prefer

  Authenticate using the Calling # value in a configured profile if available, otherwise fall back to using password authentication.
- First

  Authenticate using the CLID if available, otherwise fall back to using PAP or CHAP authentication. The MAX clears the call if both CLID authentication and PAP or CHAP authentication fail, or if CLID is not available and PAP or CHAP authentication fails.
- Called First

  Authenticate using the Called # if available, otherwise fall back to using PAP or CHAP authentication. The MAX clears the call if both Called # authentication and PAP or CHAP authentication fail, or if Called # is not available and PAP or CHAP authentication fails.

Location: Ethernet > Answer

See Also: AnsOrig, Calling #, Called #

A "don't fragment" ping option

Ascend units affected: MAX 6000, MAX 1800, MAX 2000

Introduced in: 6.1.24

Release 6.1.24 includes an additional option for the ping command. The option -f can be used to set the DON'T_FRAGMENT bit on ping packets.

Transmitting a Telnet break in immediate modem service

Ascend units affected: MAX 6000, MAX 4000, MAX 2000, MAX 1800, MAX 200

Introduced in: 6.1.24

In previous releases, transmitting a Telnet break was not possible in immediate modem service. In this release, you can transmit a Telnet break on 56 k modem cards by:

1. Telnet in a MAX using the immediate Telnet port.
2. Interrupt the Telnet connection by pressing Ctrl-].
3. Type:

   `send break`

Change in the minimum legal value of PPP Delay

Ascend units affected: MAX 6000, MAX 4000, MAX 2000, MAX 1800, MAX 200

Introduced in: 6.1.24

Point of sales terminals were losing data when dialing into a MAX because they were sending asynchronous data as soon as the modems connected. To correct this, the minimum legal value of PPP Delay has been changed from 1 (in a range of 1 to 60) to 0 (in a range of 0 to 60). This results in all data being sent to the Terminal Server.

Corrections in 6.1.24

A variety of corrections were included in release 6.1.24. The TR number and problem corrected are listed in numerical order in Table 1.

Table 1. Problems corrected in Release 6.1.24 for the MAX

TR	Problem corrected
TR 1412	The range of IP filter port numbers was 0 to 35565 instead of 0 to 65535.
TR 3075	A PIAFS client could not connect to a PPTP Network Server through a MAX 4000.
TR 3162	When shared profiles were in use, the MAX was not performing callbacks successfully to all calls on the same Connection profile.
TR 3163	The MAX was not handling finger requests correctly from devices running FreeBSD with the long TCP option.
TR 3245	Rather than send a busy signal when a seventeenth PIAFS call was placed to a MAX 4000, the Ascend unit accepted the call and did not process it.
TR 3301	MAX units were sending SNMP responses with unknown values.
TR 3351	A MAX 4000 with IPX enabled flooded a network with a level of IPX-SAP activity that a high-capacity router (not an Ascend router) could not process.
TR 3380	After running for up to one month, a MAX 4000 refused any sync call and the console menu did allow the user to open menu of K56-Modem cards.
TR 3384	A MAX 200Plus failed to stop sending RADIUS requests for routes, bridges, and pools to a server that was not responding to the requests.
TR 3387	Remote login (rlogin) users were receiving inaccurate disconnect-cause-codes on MAX 2000 units.
TR 3416	A rare problem with a channel restart message was occasionally resulting in a fast busy signal on ISDN connections.
TR 3425	Parallel dial on outbound calls was failing intermittently on some of the channels.
TR 3433	With extremely heavy loads on WAN lines, MAX 200 units were dropping ISDN BRI B channels, resulting in failed connections.
TR 3456	The Domain Name System (DNS) table on a MAX 4000 displayed only one IP address on a multiserver host when responding to a ping.
TR 3515	TACACS authentication began to fail on a MAX, requiring that the unit be reset.
TR 3556	A MAX 6000 was occasionally flooding an SNMP manager with MAX down traps.

Table 1. Problems corrected in Release 6.1.24 for the MAX (continued)

TR	Problem corrected
TR 3597	In the event of a CHAP authentication failure, the link was left to time out.
TR 3643	MAX 4002 in a light call-load environment exhibited FE36.
TR 3659	Zmodem transfers from immediate Telnet connections on MAX 200 units were not working properly.
TR 3693	Customers with NI-2 circuits were unable to select the call-by-call service options for the outbound voice call initiated through the Terminal Server or DeskDial via modems.
TR 3752	The Ascend-Maximum-Time attribute was not taking effect for CBCP sessions even though the time limit defined with the attribute had been exceeded.
TR 3766	The Ascend-Xmit-Rate and Ascend-Data-Rate were being reported incorrectly as zero in RADIUS accounting STOP records for CBCP sessions.
TR 3772	Establishing more than one nailed connection on a net BRI card was not working.
TR 3784	On the MAX 1800, stacking was failing with Calling-Line Identification (CLID)-authenticated MP calls.
TR 3820	When a MAX 6000 had a video connection to another IMUX via WAN port 1, the Ascend unit terminated the video call whenever the user disabled or enabled a second WAN port.
TR 3826	No software load was available for the MAX 2000 to support Network Address Translation (NAT) for LAN and KFlex modems.
TR 3845	When dialing out to a busy line through an immediate modem connection, a MAX 4000 did not report busy, and instead reported "no carrier."
TR 3873	Some static Ascend Inverse Multiplexing (AIM) calls were failing on MAX 6000 units.
TR 3876	A user session still appeared to be active when the user had terminated the session.
TR 3889	When IPX header compression was in use, the MAX reset, logging a Fatal Error 2.
TR 3933	When PIAFS v.32 cards were used, upgrading from a 6.x release to a 7.0 release caused a fatal error.
TR 3966	When the MAX 4000's Ethernet > Connections menu was accessed from the Control Port as soon as the Power-On Self Test was completed, the MAX 4000 reset, logging no fatal error.

Table 1. Problems corrected in Release 6.1.24 for the MAX (continued)

TR	Problem corrected
TR 3975	MAX 6000 units were failing to report as busy when no modem was available for BRI line modem calls.
TR 4034	Although Mod Config > WAN options > Pool Summary was set to yes, the routes generated were not marked private for MP/MPP calls assigned from a pool.
TR 4040	MAX units crashed with FE1 errors with incorrectly encrypted tunnel passwords.
TR 4044	Transmitting a Telnet break to a modem was not possible in immediate modem service.
TR 4061	When the MP+ minimum channel counts (Min Channel Count) were set to different values at the two endpoints of a connection, outgoing calls from a MAX were not completing properly.
TR 4096	Cyclical redundancy check (CRC) errors caused MAX 6000 software uploads to fail occasionally.
TR 4097	When an external flash card was installed, progress indicators did not display.
TR 4169	MAX units were experiencing fatal errors when using immediate modem service.
TR 4191	The MAX occasionally reboots during file transfers, resulting in no fatal error.
TR 4197	OSPF was unsupported in an earlier release for the MAX 2000.
TR 250025	When configuring a new profile for EU-RAW or EU-UI encapsulation on a MAX 4000, the profile could not be saved because the MAX requested a password.
TR 250094	RADIUS accounting records for X.75 calls on a MAX 1800 was missing byte counts and packets.
TR 250187	MPP calls were being reported as PPP on the RADIUS accounting start and stop messages.
TR 250228	Callbacks using the V.110 protocol were not working consistently because some values for the RADIUS attribute Ascend-Data-Svc (247) were missing.
TR 250296	An ISDN problem resulted in inappropriate disconnects for customers using the T-ONLINE features.
TR 258589	Some dialing and dialed numbers were being omitted from PPTP incoming call request messages.

Table 1. Problems corrected in Release 6.1.24 for the MAX (continued)

TR	Problem corrected
TR 258613	When the MAX 1800 was configured as a Dynamic Host Configuration Protocol (DHCP) server and received a DHCP discover request sent by a bootp relay agent, the response it sent contained source and destination addresses with octets reversed.
TR 258618	Incoming calls to a MAX 200 were failing when immediate service was in use.
TR 258656	MAX 6000 and MAX 4000 units were not responding to AARP packets originating from a Shiva router.
TR 258660	Unnecessary RIP update events were occurring in the MAX 4000.
TR 258662	Problems were occurring with RADIUS stop records, including missing records, records sent while sessions were still active, and username inaccuracies.
TR 258676	Continuous modem retraining was occurring when using DPNSS/DASS2 lines.
TR 258680	A customized RADIUS server on a customer site sent unacceptable external filters to the MAX, causing a fatal error. Although upgrading the RADIUS server fixed the problem, changes were made to prevent any similar problems.
TR 258688	On the MAX 6000, the E1 channel could not be nailed when signalling is set to none.
TR 258692	A MAX on an X.75 network was not processing calls consistently when v42.bis compression was in use.
TR 258694	Point of sales terminals were losing data when dialing into a MAX because they were sending asynchronous data as soon as the modems connected.
TR 258703	MAX 4000 units occasionally reset after a few days when supporting DNIS, RADIUS, PPTP, and L2TP.
TR 258722	The avm diagnostic command occasionally displayed inconsistent results.
TR 1000057	The MAX occasionally did not respond to incoming calls over R2.
TR 1000063	In heavy RAS traffic conditions, users dialed in but did not get a busy signal a ring tone, nor a connected modem tone.
TR 1000078	On a MAX 2000, SNMP suspect, disabled, and dead LANmodem Object IDs (OIDs) were not functioning.
TR 1000078	On a MAX 2000, SNMP suspect, disabled, and dead LANmodem Object IDs (OIDs) were not functioning.

Table 1. Problems corrected in Release 6.1.24 for the MAX (continued)

TR	Problem corrected
TR 1000085	Modems on MAX units randomly failed to connect, requiring a MAX reset to recover the failed modems.
TR 1000092	When an R2 CLID was requested, an incorrect tone was being returned.
TR 1000094	MAX did not operate correctly as a Home Agent running IPX.
TR 1000112	After heavy Multipoint Protocol (MP) traffic, a router would disconnect from a MAX.
TR 1000133	MAX units supporting Australian BRI lines occasionally reset logging no Fatal Error.

Rockwell code version

The following Rockwell code versions are supported in release 6.1.24:

Digital modem modules	Rockwell code versions
K56	2.084
V.34 Modem-12	1.610G24
V.34 Modem-8	1.610G19

Rockwell 2.084 firmware supports v.90, K56flex, K56plus, and all slower, standard modem speeds.

Known issues in 6.1.24

The known issues associated with 6.1.24 are as follows:

- Incoming calls are not properly routing through PBX-T1 conversion when pbx type=data and answer service = none.
- The following multimedia features are not supported in this release. Customers using these features should not upgrade to 6.1.x:
  - AIM/BONDING
  - BERT (Bit Error Rate Test)
  - Time-of-day calling
  - Backup and Overflow

Corrections since release 6.1.0

Releases from 6.1.0 to 6.1.24 have included corrections. Corrected problems are listed in numerical order in this section.

Table 2. Problems corrected from Release 6.1.0 to 6.1.24

TR	Problem corrected	Correction introduced in release
TR 1412	The range of IP filter port numbers was 0 to 35565 instead of 0 to 65535.	6.1.24
TR 1486	MAX 4000-NFAS Line Quiesce did not work.	6.1.7
TR 3075	A PIAFS client could not connect to a PPTP Network Server through a MAX 4000.	6.1.24
TR 3162	When shared profiles were in use, the MAX was not performing callbacks successfully to all calls on the same Connection profile.	6.1.24
TR 3163	The MAX was not handling finger requests correctly from devices running FreeBSD with the long TCP option.	6.1.24
TR 3227	A MAX 4000, with ARA enabled, assigned two IP addresses to each connection and released only one IP address when the connection ended.	6.1.7
TR 3245	Rather than send a busy signal when a seventeenth PIAFS call was placed to a MAX 4000, the Ascend unit accepted the call and did not process it.	6.1.24
TR 3301	MAX units were sending SNMP responses with unknown values.	6.1.24
TR 3351	A MAX 4000 with IPX enabled flooded a network with a level of IPX-SAP activity that a high-capacity router (not an Ascend router) could not process.	6.1.24
TR 3358	MAX 4000 delivered packets through a static ISDN route when more efficient routes were available.	6.1.7
TR 3367	A MAX 4000 generated FE1 and FE8 messages.	6.1.7
TR 3380	After running for up to one month, a MAX 4000 refused any sync call and the console menu did allow the user to open menu of K56-Modem cards.	6.1.24

Table 2. Problems corrected from Release 6.1.0 to 6.1.24 (continued)

TR	Problem corrected	Correction introduced in release
TR 3384	A MAX 200Plus failed to stop sending RADIUS requests for routes, bridges, and pools to a server that was not responding to the requests.	6.1.24
TR 3387	Remote login (rlogin) users were receiving inaccurate disconnect-cause-codes on MAX 2000 units.	6.1.24
TR 3390	FE 46 generated by MAX 4048 with Line Quality Monitoring (LQM) turned on.	6.1.3
TR 3416	A rare problem with a channel restart message was occasionally resulting in a fast busy signal on ISDN connections.	6.1.24
TR 3425	Parallel dial on outbound calls was failing intermittently on some of the channels.	6.1.24
TR 3433	With extremely heavy loads on WAN lines, MAX 200 units were dropping ISDN BRI B channels, resulting in failed connections.	6.1.24
TR 3456	The Domain Name System (DNS) table on a MAX 4000 displayed only one IP address on a multiserver host when responding to a ping.	6.1.24
TR 3460	MAX 4000 accounting log incorrectly reported the framed address parameter when the MAX set up or tore down an MP connection.	6.1.7
TR 3474	MAX handling MP calls exhibited IP Pool leak.	6.1.3
TR 3486	Telnet sessions to MAX 4000 generated FE 140 and FE 175 immediately after the password was successfully entered.	6.1.3
TR 3515	TACACS authentication began to fail on a MAX, requiring that the unit be reset.	6.1.24
TR 3549	RIP2 Use Multicast Parameter changed when upgrading to 6.1.0 from 5.0ap48.	6.1.7
TR 3556	A MAX 6000 was occasionally flooding an SNMP manager with MAX down traps.	6.1.24
TR 3557	SNMP resets placed a warning 176 before reset h.	6.1.7
TR 3558	SNMP WAN trap variable was not correct.	6.1.7
TR 3567	SNMP Reboot Trap logged misleading information.	6.1.7

Table 2. Problems corrected from Release 6.1.0 to 6.1.24 (continued)

TR	Problem corrected	Correction introduced in release
TR 3597	In the event of a CHAP authentication failure, the link was left to time out.	6.1.24
TR 3643	MAX 4002 in a light call-load environment exhibited FE36.	6.1.24
TR 3659	Zmodem transfers from immediate Telnet connections on MAX 200 units were not working properly.	6.1.24
TR 3693	Customers with NI-2 circuits were unable to select the call-by-call service options for the outbound voice call initiated through the Terminal Server or DeskDial via modems.	6.1.24
TR 3752	The Ascend-Maximum-Time attribute was not taking effect for CBCP sessions even though the time limit defined with the attribute had been exceeded.	6.1.24
TR 3766	The Ascend-Xmit-Rate and Ascend-Data-Rate were being reported incorrectly as zero in RADIUS accounting STOP records for CBCP sessions.	6.1.24
TR 3772	Establishing more than one nailed connection on a net BRI card was not working.	6.1.24
TR 3784	On the MAX 1800, stacking was failing with Calling-Line Identification (CLID)-authenticated MP calls.	6.1.24
TR 3820	When a MAX 6000 had a video connection to another IMUX via WAN port 1, the Ascend unit terminated the video call whenever the user disabled or enabled a second WAN port.	6.1.24
TR 3826	No software load was available for the MAX 2000 to support Network Address Translation (NAT) for LAN and KFlex modems.	6.1.3
TR 3845	When dialing out to a busy line through an immediate modem connection, a MAX 4000 did not report busy, and instead reported “no carrier.”	6.1.24
TR 3873	Some static Ascend Inverse Multiplexing (AIM) calls were failing on MAX 6000 units.	6.1.24
TR 3876	A user session still appeared to be active when the user had terminated the session.	6.1.24
TR 3889	When IPX header compression was in use, the MAX reset, logging a Fatal Error 2.	6.1.24

Table 2. Problems corrected from Release 6.1.0 to 6.1.24 (continued)

TR	Problem corrected	Correction introduced in release
TR 3933	When PIAFS v.32 cards were used, upgrading from a 6.x release to a 7.0 release caused a fatal error.	6.1.24
TR 3966	When the MAX 4000's Ethernet > Connections menu was accessed from the Control Port as soon as the Power-On Self Test was completed, the MAX 4000 reset, logging no fatal error.	6.1.24
TR 3975	MAX 6000 units were failing to report as busy when no modem was available for BRI line modem calls.	6.1.24
TR 4034	Although Mod Config > WAN options > Pool Summary was set to yes, the routes generated were not marked private for MP/MPP calls assigned from a pool.	6.1.24
TR 4040	MAX units crashed with FE1 errors with incorrectly encrypted tunnel passwords.	6.1.24
TR 4044	Transmitting a Telnet break to a modem was not possible in immediate modem service.	6.1.24
TR 4061	When the MP+ minimum channel counts (Min Channel Count) were set to different values at the two endpoints of a connection, outgoing calls from a MAX were not completing properly.	6.1.24
TR 4096	Cyclical redundancy check (CRC) errors caused MAX 6000 software uploads to fail occasionally.	6.1.24
TR 4097	When an external flash card was installed, progress indicators did not display.	6.1.24
TR 4169	MAX units were experiencing fatal errors when using immediate modem service.	6.1.24
TR 4191	The MAX occasionally reboots during file transfers, resulting in no fatal error.	6.1.24
TR 4197	OSPF was unsupported in an earlier release for the MAX 2000.	6.1.24
TR 250025	When configuring a new profile for EU-RAW or EU-UI encapsulation on a MAX 4000, the profile could not be saved because the MAX requested a password.	6.1.24
TR 250094	RADIUS accounting records for X.75 calls on a MAX 1800 was missing byte counts and packets.	6.1.24

Table 2. Problems corrected from Release 6.1.0 to 6.1.24 (continued)

TR	Problem corrected	Correction introduced in release
TR 250187	MPP calls were being reported as PPP on the RADIUS accounting start and stop messages.	6.1.24
TR 250228	Callbacks using the V.110 protocol were not working consistently because some values for the RADIUS attribute Ascend-Data-Svc (247) were missing.	6.1.24
TR 250276	MAX 4000 and MAX 6000 connected to E1 lines provided by a Nokia Switch did not accept traffic from the network.	6.1.1
TR 250296	An ISDN problem resulted in inappropriate disconnects for customers using the T-ONLINE features.	6.1.24
TR 250301	ATMP was not present in load ebixk.m40	6.1.7
TR 258589	Some dialing and dialed numbers were being omitted from PPTP incoming call request messages.	6.1.24
TR 258613	When the MAX 1800 was configured as a Dynamic Host Configuration Protocol (DHCP) server and received a DHCP discover request sent by a bootp relay agent, the response it sent contained source and destination addresses with octets reversed.	6.1.24
TR 258618	Incoming calls to a MAX 200 were failing when immediate service was in use.	6.1.24
TR 258656	MAX 6000 and MAX 4000 units were not responding to AARP packets originating from a Shiva router.	6.1.24
TR 258660	Unnecessary RIP update events were occurring in the MAX 4000.	6.1.24
TR 258662	Problems were occurring with RADIUS stop records, including missing records, records sent while sessions were still active, and username inaccuracies.	6.1.24
TR 258672	In a few interim releases, backup BRI Permanent Virtual Circuits (PVCs) were not functioning.	6.1.24
TR 258676	Continuous modem retraining was occurring when using DPNSS/DASS2 lines.	6.1.24
TR 258680	A customized RADIUS server on a customer site sent unacceptable external filters to the MAX, causing a fatal error. Although upgrading the RADIUS server fixed the problem, changes were made to prevent any similar problems.	6.1.24

Table 2. Problems corrected from Release 6.1.0 to 6.1.24 (continued)

TR	Problem corrected	Correction introduced in release
TR 258688	On the MAX 6000, the E1 channel could not be nailed when signalling is set to none.	6.1.24
TR 258692	A MAX on an X.75 network was not processing calls consistently when v42.bis compression was in use.	6.1.24
TR 258694	Point of sales terminals were losing data when dialing into a MAX because they were sending asynchronous data as soon as the modems connected.	6.1.24
TR 258703	MAX 4000 units occasionally reset after a few days when supporting DNIS, RADIUS, PPTP, and L2TP.	6.1.24
TR 258722	The avm diagnostic command occasionally displayed inconsistent results.	6.1.24
TR 1000057	The MAX occasionally did not respond to incoming calls over R2.	6.1.24
TR 1000063	In heavy RAS traffic conditions, users dialed in but did not get a busy signal a ring tone, nor a connected modem tone.	6.1.24
TR 1000070	100M Ethernet port on MAX 6000 did not auto-negotiate FDX.	6.1.24
TR 1000078	On a MAX 2000, SNMP suspect, disabled, and dead LANmodem Object IDs (OIDs) were not functioning.	6.1.24
TR 1000085	Modems on MAX modem cards randomly failed to connect and did not recover until they had been reset.	6.1.24
TR 1000092	When an R2 CLID was requested, an incorrect tone was being returned.	6.1.24
TR 1000094	MAX did not operate correctly as a Home Agent running IPX.	6.1.24
TR 1000112	After heavy Multipoint Protocol (MP) traffic, a router would disconnect from a MAX.	6.1.24
TR 1000133	A few BRI switch types were reported to have experienced low memory conditions.	6.1.24

Enhancements in 6.1.3

Release 6.1.3 included two enhancements, described in this section.

MultiVoice capability added to MAX 2000

MultiVoice capability is now available for your MAX 2000.

Specifying the maximum time to establish an outgoing call

You can now set the maximum time that the MAX allows for an outgoing call to connect with a remote device before disconnecting the attempt. Previously, the MAX allowed outgoing calls twenty seconds to connect.

New parameter

MAX Dialout Time

Description: Specifies the amount of seconds that the MAX waits for an outgoing call to connect before disconnecting the attempt.

Usage: Specify a number from 0 to 255. The 0 (zero) setting resets the parameter to its factory-default setting. The default is 20.

Example: `max dialout time = 120`

Location: System

Enhancements in 6.1.1

Release 6.1.1 included a new monitoring capability for the MAX 6000.

Monitoring Redundant MAX 6000 power supplies

The Redundant MAX 6000 has an extra power supply as a backup power source. The MAX 6000 checks the power supplies every 15 seconds. When either power supply fails, a Warning 400 records the condition, the Alarm Relay closes and the Alarm light goes on. When a failed power supply recovers, the MAX reopens the Alarm Relay and the Alarm light goes off.

Note: Some Redundant MAX units ship with only one power supply, in this case the feature described above would not apply.

Notice of discontinuance—v.34 slot cards

Software support for V.34 modem slot cards will be phased out of new TAOS code releases beginning with TAOS 7.1. The last TAOS release to contain software support for V.34 slot cards for the MAX family is TAOS 7.0.

The slot cards affected by this discontinuance are as follows:

8-port

- MX-SL-8MOD-V34
- MX-SL-8MOD-V34-B
- MX-SL-8MOD-V34B
- MX-SL-8MOD–V34R.

12-port

- MX-SL-12MOD
- MX-SL-12MOD-B.

Caution: If you continue to use the slot cards listed above, do not download future TAOS code releases numbered 7.1 or later. Those releases are not planned to include software support for V.34 slot cards.

High-speed modem technology

To move to higher-speed modem technologies, which support up to 56Kbps data rates, order Series56 modem slot cards. These cards support the ITU-T 56Kbps standard, known as V.90. They are backward compatible with older modem technologies, including V.34.

Upgrading your system software

Caution: Periodically the procedure for uploading new software to Ascend units changes significantly. Carefully read the new software loading procedures explained in this section before upgrading your system.

Introduction to upgrade and downgrade procedures

This section explains how to change your system software by either upgrading or downgrading it. Before you upgrade or downgrade your software, review the related terms and definitions in the following list and review the guidelines for upgrading and downgrading in the sections "Guidelines for upgrading system software" on page 17 and "Guidelines for downgrading system software" on page 18.

This document uses the following terms:

Build	The name of the software binary. For example, `ti.m40` is the MAX 4000 T1 IP-only software build. For the names of all the software builds and the features they provide see `/pub/Software-Releases/Max/Upgrade-Filenames.txt` on the Ascend FTP server. If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose its all or part of its configuration. If this happens, you must restore your configuration from a backup.
Standard load	Software versions 4.6Ci18 or earlier and all 4.6Cp releases. You can load these versions of software through the serial port or by using TFTP. TFTP is the recommended upgrade method for standard loads.
Fat load	4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size greater than 960 KB (for MAX units) or 448K (for Pipeline units). Before upgrading to a fat load for the first time, you must upgrade to a thin load. You must use TFTP to upgrade to fat loads.
Thin load	4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size less than 960 KB (for MAX units) or 448 KB (for Pipeline units). TFTP is the recommended upgrade method for thin loads.

Restricted load	6.0.0 or later MAX release denoted by an "r" preceding the build name. For example, rti.m40 is the restricted load for the MAX 4000 T1 IP-only software build. Before upgrading to an extended load for the first time, you must upgrade to a restricted load. Note that after you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade. A restricted load only contains essential system software and is not meant to be run in a working environment. It does not have full functionality and is to be used only to upload to an extended load. Restricted loads *do* allow you to access the unit via Telnet. TFTP is the recommended upgrade method for restricted loads.
Extended load	6.0.0 or later MAX release denoted by an "f" preceding the build name. You must use TFTP to upgrade to extended loads. For example, `fti.m40` is the extended load for the MAX 4000 T1 IP-only software build. MAX 6000 and Pipeline releases do not have extended loads.

Guidelines for upgrading system software

Caution: Before upgrading, consider the following very important guidelines:

- Use TFTP to upgrade if possible. TFTP is more reliable and saves the Ascend unit configuration when you upgrade.
- You cannot load a fat load or an extended load through the serial port. You must use TFTP.
- If you are using TFTP to upgrade your software, use the `fsave` command immediately after executing the `tload` command. Failure to do so might cause your Ascend unit to lose its configuration.
- If possible, you should always stay with the same build of software when you upgrade. If you load a different version, your Ascend unit may lose its configuration. If this happens, you must restore your configuration from a backup.
- If you are upgrading to a software version 5.0A or 5.0Aix fat load for the first time, you must be on a load that supports the fat load format. All versions of software 5.0A or above support fat loads. You should perform the upgrade in two steps:
  - Upgrade to a thin load of the same build
  - Upgrade to the fat load
- If you are upgrading to a software version 6.0.0 or above, you must be on a load that supports the extended load format. All versions of software 6.0.0 or above support extended loads. You should perform the upgrade in two steps:
  - Upgrade to a restricted load of the same build
  - Upgrade to the extended load
- The MAX 6000 does not have extended or restricted loads.
- After you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade.
- You can upgrade to a thin load or a restricted load from any version of software.

- If you are upgrading from software version 4.6C or earlier to software version 5.0A or later, see "Upgrading system software from versions earlier than 4.6C to version 5.0A or above" on page 26 for important information before you start.

Table 3 explains where to find the information you need to upgrade your unit.

Table 3. Ascend system software versions

Version you are upgrading to	Use the instructions in...
Standard load (4.6Ci18 or earlier and all 4.6Cp releases)	"Upgrading system software with a standard load" on page 20.
Fat or thin load (4.6Ci19 to 5.0Aix and all 5.0Ap releases)	"Upgrading system software with a fat or thin load" on page 21.
Extended load (6.0.0 or later)	"Upgrading system software with an extended load" on page 24.

Guidelines for downgrading system software

The MAX expects a specific organization of the parameters in a configuration file. When you upgrade a MAX, you *can* restore a configuration that was saved on an older release. The MAX enters default values for parameters if the MAX supports a parameter that is not included in the configuration file.

When you downgrade to older versions of software, the configuration might not upload completely, because older software does not support the parameters that might be in configuration files from newer releases.

You must upload a configuration that was saved from the same version of software to make sure that the MAX receives a complete configuration. If you upload a configuration from a newer version of software, you should check all parameter values to verify they are configured accurately.

If you are downgrading system software, make sure that you have a configuration saved from a MAX running with the older software and that you have console access to the MAX. Then, proceed as follows:

1. Use TFTP to load the system software.
2. Enter **`FCLEAR`** to clear the MAX unit's flash memory.
3. Enter **`NVRAMCLEAR`** to clear the MAX unit's main configuration and reset the MAX.
   The MAX restarts and loads the older version of system software.
4. When the MAX is up, manually enter basic information, including IP address, subnet mask, and default gateway to the Ethernet interface.
   After entering you must be able to use Telnet to access the MAX.
5. From the MAX unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

6. At the > prompt, use the `TRestore` command to restore the configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

   ```
   > trestore tftp-server router1.cfg
   ```

7. At the > prompt, enter **`Exit`** to return to the VT100 interface.

Preparing to upgrade your software

Make sure you perform all the tasks explained in Table 4 before upgrading your software.

Table 4. Before upgrading

Task	Description
If necessary, activate a Security Profile that allows for field upgrade.	If you are not sure how, see the section about Security Profiles in your documentation.
Record all of the passwords you want to retain, and save your Ascend unit's current configuration to your computer's hard disk.	For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the `Tsave` command, however, *does* contain the system passwords. You can restore the `Tsave` configuration file using the serial console. If you chose to save your configuration using the serial console, you have to restore your passwords manually. Restoring passwords is explained in "Using the serial port to upgrade to a standard or a thin load" on page 26.
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Ascend technical support.	To ensure that you load the correct software binary, you should check the load currently installed on your unit. To do so: **1** Tab over to the 00-100 Sys Options window. **2** Press Enter to open the Sys Options menu. **3** Using the Down-Arrow key (or Ctrl- N), scroll down until you see a line similar to the following: `Load: tb.m40` **4** When upgrading, obtain the file with same name from the Ascend FTP site. If your unit does not display the current load or you are unsure about which load to use, contact technical support.

Table 4. Before upgrading (continued)

Task	Description
If you are upgrading to a fat load or an extended load for the first time, you must also obtain a thin load or a restricted load of the same build, if possible.	For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as `tbim.m40`), obtain a thin load of the same build (such as 5.0A `tbim.m40`). If you are upgrading to a MAX 6.0.0 extended load, obtain a 6.0.0 restricted load. Restricted loads are designated with an “r” in the load name. (For example `rtbam.m40` is a restricted load). Note that after you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade. Newer Pipeline 50 or 75 units do not have fat loads and no Pipeline units have extended or restricted loads. Refer to `/pub/Software-Releases/Pipeline/Upgrade-Filenames.txt` to determine if you have a new Pipeline 50 or 75 unit.
If you are using TFTP, make sure you load the correct binaries into the TFTP home directory on the TFTP server.	You must use TFTP to upgrade to a fat load or an extended load.
If you are using the serial port, make sure you have a reliable terminal emulation program, such as Procomm Plus.	If you use the serial port, you can only upgrade to a standard or a thin load. Upgrading through the serial port is not recommended. If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.

Upgrading system software with a standard load

To upgrade system software with a standard load you can use either the serial port or TFTP. TFTP is the recommended method because it preserves your Ascend unit’s configuration. If you want to use the serial port to upgrade, see “Using the serial port to upgrade to a standard or a thin load” on page 26.

Using TFTP to upgrade to a standard load

To upgrade to a standard load using TFTP, you must enter a few commands in the correct sequence. If you do not enter them in the correct sequence, you could lose the Ascend unit’s configuration.

To upgrade to a standard load via TFTP:

1. Obtain the software version you want to upgrade to and place it in the TFTP server home directory.
2. From the Ascend unit’s VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

3 At the > prompt, use the `Tsave` command to save your configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

```
> tsave tftp-server router1.cfg
```

Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.

Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4 Enter the following command:

`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 (relative to the TFTP home directory).

For example, the command:

```
tloadcode tftp-server t.m40
```

loads `t.m40` into flash from the machine named `tftp-server`.

Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so can cause your Ascend unit to lose its configuration.

5 Enter the following command to save your configuration to flash memory:

```
> fsave
```

6 Enter the following command:

```
> nvramclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

This completes the upgrade.

Upgrading system software with a fat or thin load

Upgrading to a fat or thin load is not difficult, but you must be careful to follow the correct sequence of tasks.

Caution: If you are upgrading from software version 4.6C or earlier, see "Upgrading system software from versions earlier than 4.6C to version 5.0A or above" on page 26 for important information before upgrading.

To upgrade your system:

1 Obtain the software version binary you want to upgrade to and place it in the TFTP server home directory. If you are upgrading to a fat load for the first time, also obtain a thin load of the same build and place it in the same directory. (See page "Introduction to upgrade and downgrade procedures" on page 16 for an explanation of fat and thin loads.)

Caution: If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose all or part of its configuration. If this happens, you must restore your configuration from a backup.

For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as `tbim.m40`), obtain a thin load of the same build (such as 5.0A `tbim.m40`).

Note: Newer Pipeline 50 or 75 units do not have fat or thin loads, you only need to load a single software binary. Refer to `/pub/Software-Releases/Pipeline/Upgrade-Filenames.txt` on the Ascend FTP site to determine if you have a new Pipeline 50 or 75 unit.

2. From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

3. At the > prompt, use the `Tsave` command to save your configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

   `> tsave tftp-server router1.cfg`

   Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.

Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4. At the > prompt, enter:

   `> 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 (relative to the TFTP home directory).

Caution: If you are upgrading from a standard load to a fat load, make sure you load a thin load first.

For example, the command:

`> tloadcode tftp-server t.m40`

loads `t.m40` into flash from the machine named `tftp-server`.

Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so may cause your Ascend unit to lose its configuration.

5. Enter the following command to save your configuration to flash memory:

   `>` **`fsave`**

6. Enter the following command:

   `>` **`nvramclear`**

   After the Ascend unit clears NVRAM memory, it automatically resets.

7 If you are upgrading to a thin load, you are done. If you are upgrading to a fat load, repeat the procedure, this time uploading the fat load binary.

After a successful upgrade, one of the following messages appears.

- If the load is thin:

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

- If the load is fat:

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

This completes the upgrade if you have no errors. If the upgrade is not successful, refer to “Recovering from a failed fat load upgrade”next.

Recovering from a failed fat load upgrade

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 the Ascend unit initiates an Xmodem serial download. To recover from this error and load the fat system, you must first load a thin system that is fat-load aware. Proceed as follows:

1 Activate your Xmodem software.

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

3 Use the `Tload` command to download the fat load.

When you download a fat load, messages similar to the following appear on the diagnostics monitor screen:

```
> tload 192.168.1.82 tbam.m40
saving config to flash
........................................
loading code from 192.168.1.82:69
file tbam.m40..
fat load part 1:
..................................................................
......
fat load part 2:
..................................................
```

The “fat load part *n*:” messages notify you when the first and second halves of the download begin.

Upgrading system software with an extended load

Your first upgrade to an extended load requires a preliminary procedure. You must first upgrade to a restricted load. A restricted load only contains essential system software and is not meant to be run in a working environment. It does not have full functionality and is to be used only to upload to an extended load.

After you have upgraded your system to version 6.0.0 or above, you do not need to use a restricted load to upgrade. Note that the MAX 6000 and Pipeline units do not have extended loads.

Warning: You cannot upgrade to extended loads using an IP over X.25 connection because restricted loads do not have X.25 support.

Caution: If you are upgrading from software version 4.6C or earlier, see "Upgrading system software from versions earlier than 4.6C to version 5.0A or above" on page 26 for important information before upgrading.

To upgrade your system:

1 Obtain the software-version binary you want to upgrade to and place it in the TFTP server home directory.

Extended loads are denoted by an "f" preceding the build filename.

2 If this is the first time you have upgraded to an extended load, obtain a restricted load of the same build and place it in the directory.

For example, if you are upgrading a MAX 4000 to an extended load (such as `ftbam.m40`), obtain a MAX 4000 restricted load (such as `rtbam.m40`).

3 From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

`Esc [ Esc =`

Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

4 At the > prompt, use the `Tsave` command to save your configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

```
> tsave tftp-server router1.cfg
```

Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.

Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

5 At the > prompt, enter:

`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 (relative to the TFTP home directory).

Caution: If you want to upgrade your system for the first time to a software version 6.0.0 or later, you must first upgrade your system to a restricted load. Failure to do so can cause your Ascend unit to lose its configuration.

For example, the command:

`> ` **`tloadcode tftp-server rtbam.m40`**

loads the restricted load `rtbam.m40` into flash from the machine named `tftp-server`.

Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so can cause your Ascend unit to lose its configuration.

6 Enter the following command to save your configuration to flash memory:

`> ` **`fsave`**

7 Enter the following command:

`> ` **`nvramclear`**

After the Ascend unit clears NVRAM memory, it automatically resets.

If you have downloaded the extended load, the upgrade is complete.

If you have loaded a restricted load, your system boots up in restricted mode. Restricted mode only allows you to load software. You cannot change or save profiles. While in restricted mode, the Edit menu displays the following banner:

```
* * RESTRICTED MODE * * *
```

If your system boots up in restricted mode, perform the following steps:

1 At the > prompt, enter:

`> ` **`tloadcode`** ***`hostname filename`***

where ***`hostname`*** is the name or IP address of your TFTP server, and ***`filename`*** is the name of the extended load of system software on the server (relative to the TFTP home directory).

For example, the command:

`> ` **`tloadcode tftp-server ftbam.m40`**

loads the extended load `ftbam.m40` into flash from the machine named `tftp-server`.

2 Enter the following command:

`> ` **`nvramclear`**

After the Ascend unit clears NVRAM memory, it automatically resets.

Your system will then boot up with the new version of software running.

Upgrading system software from versions earlier than 4.6C to version 5.0A or above

If you are upgrading from software version 4.6C or earlier to version 5.0A or later, perform the upgrade in the following order:

1. Load version 4.6Ci18, following the procedure in "Upgrading system software with a standard load" on page 20.
2. Load version 5.0A, following the procedure in "Upgrading system software with a fat or thin load" on page 21.
3. Load version 5.0Aix or 6.0.0, following the procedure in "Upgrading system software with a fat or thin load" on page 21 (for software versions 5.0Aix) or "Upgrading system software with an extended load" on page 24 (for software version 6.0.0).

Caution: Failure to follow this procedure might cause your Ascend unit to lose or corrupt its configuration, and could render the unit unusable.

Using the serial port to upgrade to a standard or a thin load

Caution: Uploading system software via the serial console overwrites all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. The backup file is readable text, so you can reenter the settings through the Ascend unit's user interface. To avoid having existing profiles overwritten, use TFTP to upgrade your unit.

Caution: You cannot upload a fat load or an extended load using the serial port; it must be done using TFTP.

Upgrading through the serial port consists of the following general steps:

- Saving your configuration
- Uploading the software
- Restoring the configuration

Before you begin

Before upgrading your system through the serial port, make sure you have the following equipment and software:

- An IBM compatible PC or Macintosh with a serial port capable of connecting to the Ascend unit's Console port.
- A straight-through serial cable.
- Data communications software for your PC or Mac with XModem CRC/1K support (for example, Procomm Plus, HyperTerminal for PCs or ZTerm for the Mac).

Caution: If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.

Saving your configuration

Before you start, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to the same rate as the Term Rate parameter in the System Profile (Sys Config menu).

You can cancel the backup process at any time by pressing Ctrl-C.

To save the Pipeline configuration (except passwords) to disk:

1 Open the Sys Diag menu.

2 Select Save Config, and press Enter.

The following message appears:

```
Ready to download - type any key to start....
```

3 Turn on the Capture feature of your communications program, and supply a filename for the saved profiles. (Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.)

4 Press any key to start saving your configured profiles.

Rows of configuration information appear on the screen as the configuration file is downloaded to your hard disk. When the file has been saved, your communications program displays a message indicating the download is complete.

5 Turn off the Capture feature of your communications program.

6 Print a copy of your configured profiles for later reference.

You should examine the saved configuration file. Notice that some of the lines begin with `START=` and other lines begin with `END=`. A pair of these START/STOP lines and the block of data between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear. In fact, you can have profiles with all parameters at their defaults, in which case the corresponding START/STOP blocks are empty. Make sure that there are no extra lines of text or characters either before `START=` or after `END=`. If there are, delete them. They could cause problems when you try to upload the file to the Ascend unit.

Uploading the software

To upload the software:

1 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.) The following string of Xmodem control characters appears:

```
CKCKCKCK
```

If you do not see these characters, you probably did not press the four-key sequence quickly enough. Try again. Most people use both hands and keep one finger on the escape key.

2 Use the Xmodem file-transfer protocol to send the system file to the Ascend unit.

Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your Ascend unit. The time displayed on the screen does not represent real time. Do not worry if your communication program displays several "bad batch" messages. This is normal.

After the upload, the Ascend unit resets. Upon completion of the self-test, the Ascend unit's initial menu appears in the Edit window with all parameters set to default values. This completes the upgrade.

If the upload fails during the transfer, try downloading another copy of the binary image from the Ascend FTP server and re-loading the code to the Ascend unit. If you still have problems, contact Ascend technical support for assistance.

Restoring the configuration

Under certain circumstances, the serial-port method might not completely restore your configuration. You should therefore verify that your configuration was properly restored every time you use this method. If you have many profiles and passwords, you should consider using TFTP to upgrade your software. (See "Using TFTP to upgrade to a standard load" on page 20.)

To restore the configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example). You use the `Restore Cfg` command to restore a full configuration that you saved by using the `Save Cfg` command, or to upload more specific configuration information obtained from Ascend (for example, a single filter stored in a special configuration file).

To load configuration information through the serial port, perform the following steps.

1 From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

`Esc [ Esc =`

Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

2 At the > prompt, enter the `Fclear` command:

```
> fclear
```

3 At the > prompt, enter the `NVRAMClear` command:

```
> nvramclear
```

This causes the system to reset. When it comes back up, proceed with restoring your configuration.

4 Enter **`quit`** to exit the Diagnostic interface.

5 Open the Sys Diag menu.

6 Select `Restore Cfg`, and press Enter.

The following message appears:

```
Waiting for upload data...
```

7. Use the Send ASCII File feature of the communications software to send the configuration file to the unit. (If you have any questions about how to send an ASCII file, consult the documentation for your communications program.)

   When the restore has been completed, the following message appears:

   `Restore complete - type any key to return to menu`

8. Press any key to return to the configuration menus.
9. Reset the Ascend unit, by selecting System > Sys Diag > Sys Reset and confirming the reset.

Restoring passwords

For security, passwords are not written to configuration files created through the serial console. A configuration file created using the `Tsave` command, however, *does* contain the system passwords. You can restore the `Tsave` configuration file using the serial console.

After upgrading you may have to re-enter all the passwords on your system. If you edit your saved configuration file, however, and enter passwords in the appropriate fields (by replacing the word *SECURE* in each instance), these passwords will be restored. But note that if you do choose to edit your configuration file, you must save it as text only or you will not be able to load it into your unit.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1. Press Ctrl-D to invoke the DO menu, select `Password`, and choose the Full Access profile.
2. When you are prompted to enter the password, press Enter (the null password).

   After you have restored your privileges by entering the null password, you should immediately open the Connection profiles, Security profiles, and Ethernet profile (Mod Config menu), and reset the passwords to their previous values.

System messages

Table 5 explains the messages that can appear during your upgrade.

Table 5. System software messages

Message	Explanation

`UART initialized`
`fat load: bad CRC!!`
`forcing serial download at 57600 bps`
`please download a "thin" system...`
	The fat load has a CRC (cyclic redundancy check) error. Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Ascend unit initiates an Xmodem serial download. Load a thin load that understand the fat load format, as explained in "Upgrading system software with a fat or thin load" on page 21.

`File tbam.m40`
`incompatible fat load format--`
`discarding downloaded data`
	You attempted to upgrade to a fat load from a version of system software that does not understand the fat load format. You must first load a thin load that is fat load aware, as explained in "Upgrading system software with a fat or thin load" on page 21.

`This load has no platform identifier.` `Proceed with caution.`	This message can occur if you are running software version 5.0Ai11 or later and you load an earlier incremental or patch release onto your system. The message indicates that Tloadcode cannot determine which platform the code is intended for. If you are using the correct software version, you can ignore this message.
`This load appears not to support your network interface.` `Download aborted.  Use 'tloadcode -f' to force.`	Indicates you are attempting to load a version of code intended for a different network interface (for example, loading MAX 4000 T1 software onto a MAX 4000 E1 unit).
`This load appears to be for another platform.` `Download aborted.  Use 'tloadcode -f' to force.`	Indicates you are attempting to load a version of code onto a platform for which it is not intended (for example, loading MAX 4000 software onto a MAX 2000). This is not recommended

`UART initialized`
`fat load: inflate`
`......................................`
`......................`
`starting system...`
	Indicates you have successfully loaded a fat load.

`UART initialized`
`extended load:`
`inflate essential`
`.+.+..............................`
`invalid CRC!!`
`entering restricted mode`
`starting system...`
	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in "Upgrading system software with an extended load" on page 24.

Table 5. System software messages (continued)

Message	**Explanation**

`UART initialized`
`extended load:`
`inflate essential`
`.+.+..................................`
`.`
`invalid length!!`
`entering restricted mode`
`starting system...`
	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in "Upgrading system software with an extended load" on page 24.

`UART initialized`
`extended load:`
`inflate essential .+.+...............`
`inflate expendable..............|....`
`starting system...`
	Indicates you have successfully loaded an extended load.

`UART initialized`
`thin load: inflate`
`......................................`
`.....................`
`starting system...`
	Indicates you have successfully loaded a thin load.