

MAX TAOS 7.0.4 Cumulative Release Note

*Ascend Communications, Inc.
March 2, 1999*

MAX is a trademark of Ascend Communications, Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Copyright © 1999, Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.



Caution: You must use the software loading procedure explained in [“Upgrading system software” on page 11](#) to load this version of software onto your system. Read the instructions carefully before upgrading your system.

This cumulative release note describes corrections and enhancements introduced in software releases after 7.0.0 for the MAX.

How to use this release note

To use this release note:

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

Note: If you are already on a 7.0.x release, you only need to load the “f” binary, as described in [“Upgrading system software” on page 11](#).

- 3 Upgrade to the new software by following the instructions in “Upgrading 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

True Access Operating System 1

TAOS kernel components 1

TAOS extension components 1

Known issues 1

Corrections 2

TR 2660	Dial in V.110 client could connect to PPTP server behind a MAX.	2
TR 3163	A MAX 2000 did not process a finger request from FreeBSD with tcp option selected.	2
TR 3425	A MAX 1800 showed No Circuit Available; it did not send a set up message to switch.	2
TR 3556	Normal Link Down traps were sent from a MAX 4000.	2
TR 3659	A MAX 200Plus did not complete a Zmodem transfer.	2
TR 3685	In the 50-700 status menu, the Max showed the Enet I/F: AUI when it is plugged into a UTP connection.	2
TR 3693	A MAX 4000 was unable to complete call-by-call terminal server calls.	2
TR 3725	The Ascend Maximum Time attribute did not take affect for CBCP sessions. ...	2
TR 3766	During a CBCP session, Ascend-Xmit-Rate and Ascend-Data-Rate were reported as zero.	2
TR 3772	A MAX 6000 did not establish more than one nailed connection.	3
TR 3784	MAX-stacked Ascend unit failed with CLID authenticated MP calls.	3
TR 3838	Incoming calls were not properly routed through PBX-T1 conversion when pbx type=data and answer service=none.	3
TR 3845	MAX did not send a busy signal when a modem dialed a busy line.	3
TR 3848	A MAX 1800 did not drop the second channel when ALU dropped below Idle PCT threshold.	3
TR 3928	During a telnet session to a Max, the Edit window displayed the Ethernet profile.	3
TR 3935	MAX 4004 with two PRIs handling analog and IP calls reset with FE1.	3
TR 3966	A MAX 4000 using control port would reset without FE.	3
TR 3975	A MAX did not send cause code 17 to Net/BRI line.	3
TR 4034	A MAX configured to do Pool Summary marked MP/MPP calls as non-private.	3
TR 4040	A MAX reset with FE1 when an encrypted tunnel password was sent through RADUIS.	3

TR 4044	A MAX 4000 did not recognize break signals.	4
TR 4061	MAX 1800 did not adhere to MP+ thresholds when a call failed.	4
TR 4096	A MAX 6000 had a tload with checksum errors and it failed to restart.	4
TR 4169	A MAX 4000 would reset with FE29.	4
TR 4191	A MAX 6000 reset without FE during SCM and ftp.	4
TR 4197	MAX 2000 system software did not include support for OSPF.	4
TR 4325	A MAX 4000 exhibited a lag between modem call disconnect and No Carrier message at the calling modem.	4
TR 250228	A MAX 4000 had only one value for Call Back with v.110 attribute.	4
TR 250296	MAX sent SETUP for B-Channel before release was sent for that same B-Channel.	4
TR 258589	A MAX 4000 used incorrect Dialing Number and Dialed Number on PPTP.	4
TR 258656	A MAX 6000 did not respond to Appletalk ARP packets that were greater than 28 bytes.	4
TR 258672	A MAX 4000 backup PVC did not come up.	5
TR 258676	Bad clock source on a MAX 4000 caused the continuous modem to be retrained using DPNSS/DASS 2 lines.	5
TR 258680	FE 1 was sent every hour on a MAX 4000.	5
TR 258688	E1 channel 16 on a MAX 6000 could not be nailed when Signalling was set to None.	5
TR 258692	A MAX 4000 exhibited inconsistent x.75 behavior when v.42bis compression was used.	5
TR 258694	Data sent from a POS terminal was lost when the MAX did not buffer the 100 bytes.	5
TR 258701	ISDN overlap received numbers that were not in DNIS.	5
TR 258722	On a MAX 4000, avm command showed modems dropping off.	5
TR 258725	MP/MPP calls failed authentication in a MAX-stacked environment.	5
TR 258728	MAX would hang after several hours of running x.25 PAD calls.	5
TR 258730	A reset with FE1 was exhibited when two Immediate Telnet sessions used DNIS authentication.	5
TR 258748	Multipath external OSPF routes were not deleted from the MAX routing table.	6
TR 1000032	MAX set MRRU equal to MRU and then dropped ATMP packets.	6
TR 1000085	MAX modem code would be corrupted, causing calls to fail.	6
TR 1000094	A MAX 6000 as an ATMP HA running IPX did not work.	6
TR 1000096	R2 signaling did not support a B-5 tone.	6
TR 1000112	MAX 1800 MP connections failed.	6
TR 1000114	Attempt to disable either Net 5 and Australia PRA on a MAX disabled the other.	6
TR 1000115	In an MP Connection profile, Base Ch Count was incorrectly read as Max Ch Count for received MP calls.	6
TR 1000120	x.25 PVC and SVC could not be configured.	7
TR 1000126	A MAX generated an FE 106 when both SNMP and ATMP were active.	7
TR 1000137	E1 R2 enabled MAX 6000 did not time out if no seize ack.	7
TR 1000139	A MAX 4000 ifAdminStatus object was not recognized.	7
TR 1000140	Called Number and Calling Number were displayed as N/A though an active connection profile included X.25/PAD encapsulation.	7
TR 1000146	R2 outdial failed.	7
TR 1000165	A MAX 6000 generated FE1 during heavy modem outdial.	7

Enhancements	7
<i>OSPF supports MD5 authentication</i>	<i>7</i>
<i>New settings for CLID-Auth-Mode</i>	<i>9</i>
Rockwell (Conexant) code versions	9
<i>Notice of discontinuance:</i>	
<i>Software support for v.34 slot cards</i>	<i>9</i>
Upgrading system software	11

True Access Operating System

Ascend's True Access™ Operating System (TAOS) runs on Ascend's advanced WAN Access products, which provide modular chassis integrating a wide range of technologies that enable service providers and enterprise managers to install customized network infrastructures.

TAOS consists of two groups of components, TAOS kernel and TAOS extension. The TAOS kernel components included within Ascend's Access products provide a foundation of features for WAN access environments. The TAOS extension components provide software solutions that enable you to configure and support a wide variety of WAN access environments. Within each TAOS component, whether extension or kernel, you will find features that support that component.

TAOS kernel components

This is a cumulative list of the TAOS kernel components, feature identification (FID) numbers, and supporting enhancements introduced in software releases after 7.0.0 for the MAX:

Table 1. TAOS kernel components

Component	FID	Supporting enhancements
AAA Server	None	New settings for CLID-Auth-Mode

TAOS extension components

This is a cumulative list of the TAOS kernel components, feature identification (FID) numbers, and supporting enhancements introduced in software releases after 7.0.0 for the MAX:

Table 2. TAOS kernel components

Component	FID	Supporting enhancements
Virtual router	None	OSPF supports MD5 authentication

Known issues

The following known issues apply to release 7.0.4:

- Incoming calls are not properly routing through PBX-T1 conversion when pbx type=data and answer service=none.
- Some multimedia features are not supported in this release. Customers using the following features should not upgrade to 7.0.4:

- AIM/BONDING
- Time-of-day calling
- Backup and Overflow
- In a MAX, data flows between T1/E1 WAN ports and host devices over a limited number of internal data pathways. When BRI cards are installed, pathways normally allocated for built-in T1/E1 ports are effectively borrowed to support the BRI WAN ports, and are no longer available for T1/E1 usage. The host devices that can be affected by this limitation include modems and HDLC ports.

Corrections

<i>TR 2660</i>	Dial in V.110 client could connect to PPTP server behind a MAX. Corrected in: 7.0.3
<i>TR 3163</i>	A MAX 2000 did not process a finger request from FreeBSD with tcp option selected. Corrected in: 7.0.3
<i>TR 3425</i>	A MAX 1800 showed No Circuit Available; it did not send a set up message to switch. Corrected in: 7.0.3
<i>TR 3556</i>	Normal Link Down traps were sent from a MAX 4000. Corrected in: 7.0.3
<i>TR 3659</i>	A MAX 200Plus did not complete a Zmodem transfer. Corrected in: 7.0.3
<i>TR 3685</i>	In the 50-700 status menu, the Max showed the Enet I/F: AUI when it is plugged into a UTP connection. Corrected in: 7.0.3
<i>TR 3693</i>	A MAX 4000 was unable to complete call-by-call terminal server calls. Corrected in: 7.0.3
<i>TR 3725</i>	The Ascend Maximum Time attribute did not take affect for CBCP sessions. Corrected in: 7.0.3
<i>TR 3766</i>	During a CBCP session, Ascend-Xmit-Rate and Ascend-Data-Rate were reported as

zero.

Corrected in: 7.0.3

TR 3772 A MAX 6000 did not establish more than one nailed connection.

Corrected in: 7.0.3

TR 3784 MAX-stacked Ascend unit failed with CLID authenticated MP calls.

Corrected in: 7.0.3

TR 3838 Incoming calls were not properly routed through PBX-T1 conversion when pbx type=data and answer service=none.

Corrected in: 7.0.3

TR 3845 MAX did not send a busy signal when a modem dialed a busy line.

Corrected in: 7.0.3

TR 3848 A MAX 1800 did not drop the second channel when ALU dropped below Idle PCT threshold.

Corrected in: 7.0.3

TR 3928 During a telnet session to a Max, the Edit window displayed the Ethernet profile.

Corrected in: 7.0.3

TR 3935 MAX 4004 with two PRIs handling analog and IP calls reset with FE1.

Corrected in: 7.0.3

TR 3966 A MAX 4000 using control port would reset without FE.

Corrected in: 7.0.3

TR 3975 A MAX did not send cause code 17 to Net/BRI line.

Corrected in: 7.0.3

TR 4034 A MAX configured to do Pool Summary marked MP/MPP calls as non-private.

Corrected in: 7.0.3

TR 4040 A MAX reset with FE1 when an encrypted tunnel password was sent through

RADUIS.

Corrected in: 7.0.3

TR 4044

A MAX 4000 did not recognize break signals.

Corrected in: 7.0.3

TR 4061

MAX 1800 did not adhere to MP+ thresholds when a call failed.

Corrected in: 7.0.3

TR 4096

A MAX 6000 had a tload with checksum errors and it failed to restart.

Corrected in: 7.0.3

TR 4169

A MAX 4000 would reset with FE29.

Corrected in: 7.0.3

TR 4191

A MAX 6000 reset without FE during SCM and ftp.

Corrected in: 7.0.3

TR 4197

MAX 2000 system software did not include support for OSPF.

Corrected in: 7.0.3

TR 4325

A MAX 4000 exhibited a lag between modem call disconnect and No Carrier message at the calling modem.

Corrected in: 7.0.3

TR 250228

A MAX 4000 had only one value for Call Back with v.110 attribute.

Corrected in: 7.0.3

TR 250296

MAX sent SETUP for B-Channel before release was sent for that same B-Channel.

Corrected in: 7.0.3

TR 258589

A MAX 4000 used incorrect Dialing Number and Dialed Number on PPTP.

Corrected in: 7.0.3

TR 258656

A MAX 6000 did not respond to Appletalk ARP packets that were greater than 28

bytes.

Corrected in: 7.0.3

TR 258672 A MAX 4000 backup PVC did not come up.

Corrected in: 7.0.3

TR 258676 Bad clock source on a MAX 4000 caused the continuous modem to be retrained using DPNSS/DASS 2 lines.

Corrected in: 7.0.3

TR 258680 FE 1 was sent every hour on a MAX 4000.

Corrected in: 7.0.3

TR 258688 E1 channel 16 on a MAX 6000 could not be nailed when Signalling was set to None.

Corrected in: 7.0.3

TR 258692 A MAX 4000 exhibited inconsistent x.75 behavior when v.42bis compression was used.

Corrected in: 7.0.3

TR 258694 Data sent from a POS terminal was lost when the MAX did not buffer the 100 bytes.

Corrected in: 7.0.3

TR 258701 ISDN overlap received numbers that were not in DNIS.

Corrected in: 7.0.3

TR 258722 On a MAX 4000, avm command showed modems dropping off.

Corrected in: 7.0.3

TR 258725 MP/MPP calls failed authentication in a MAX-stacked environment.

Corrected in: 7.0.3

TR 258728 MAX would hang after several hours of running x.25 PAD calls.

Corrected in: 7.0.3

TR 258730 A reset with FE1 was exhibited when two Immediate Telnet sessions used DNIS

Corrections

TAOS extension components

	authentication. Corrected in: 7.0.3
TR 258748	Multipath external OSPF routes were not deleted from the MAX routing table. Corrected in: 7.0.3
TR 1000032	MAX set MRRU equal to MRU and then dropped ATMP packets. Corrected in: 7.0.3
TR 1000085	MAX modem code would be corrupted, causing calls to fail. Corrected in: 7.0.3
TR 1000094	A MAX 6000 as an ATMP HA running IPX did not work. Corrected in: 7.0.3
TR 1000096	R2 signaling did not support a B-5 tone. Corrected in: 7.0.3
TR 1000112	MAX 1800 MP connections failed. 7.0.3
TR 1000114	Attempt to disable either Net 5 and Australia PRA on a MAX disabled the other. Corrected in: 7.0.3
TR 1000115	In an MP Connection profile, Base Ch Count was incorrectly read as Max Ch Count

	for received MP calls. Corrected in: 7.0.1
<i>TR 1000120</i>	x.25 PVC and SVC could not be configured. Corrected in: 7.0.3
<i>TR 1000126</i>	A MAX generated an FE 106 when both SNMP and ATMP were active. Corrected in: 7.0.1
<i>TR 1000137</i>	E1 R2 enabled MAX 6000 did not time out if no seize ack. Corrected in: 7.0.3
<i>TR 1000139</i>	A MAX 4000 ifAdminStatus object was not recognized. Corrected in: 7.0.3
<i>TR 1000140</i>	Called Number and Calling Number were displayed as N/A though an active connection profile included X.25/PAD encapsulation. Corrected in: 7.0.3
<i>TR 1000146</i>	R2 outdial failed. Corrected in: 7.0.3
<i>TR 1000165</i>	A MAX 6000 generated FE1 during heavy modem outdial. Corrected in: 7.0.3

Enhancements

OSPF supports MD5 authentication

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

Introduced in: 7.0.0

OSPF on the MAX supports the MD5 cryptographic authentication method. With this release, you can select the MD5 authentication type to direct the MAX to validate OSPF packet exchanges using MD5 encryption and an authentication Key ID or an authentication key that you specify.

AuthKey

Description: Specifies an authentication key that appears in OSPF and external authentication configurations. For OSPF configurations, the value of Auth-Key is a 64-bit clear password inserted into the OSPF packet header. It is used by OSPF routers to allow packets into or exclude packets from an area.

Usage: Specify a string of up to eight characters. The default for OSPF is `ascend0`.

Location: Ethernet > Connections > Any connection profile > OSPF Options, Ethernet > Mod Config > OSPF Options

KeyID

Description: Specifies an authentication key (a password) used to allow OSPF routing. KeyID is a number from 0 to 255 inserted into the OSPF packet header. OSPF routers use

Usage: KeyID to allow or exclude packets from an area. The default value is 0.

Specify a number from 0 to 255.

Example: KeyID=125

Location: Ethernet > Connections > Any connection profile > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: AuthType

AuthType

Description: Specifies the type of authentication in use for validating OSPF packet exchanges: Simple (the default) or None. Simple authentication is designed to prevent configuration errors from affecting the OSPF routing database. It is not designed for firewall protection.

Usage: Specify one of the following values:

- None
Routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header may contain data, but it is not examined on packet reception. When you use this setting, the MAX performs a checksum on the entire contents of each OSPF packet (other than the 64-bit authentication field) to ensure against data corruption.
- Simple
This setting requires that you specify a 64-bit field in the auth-key parameter. Each packet sent on a particular network must have the configured value in its OSPF header 64-bit authentication field. Simple is the default.
- MD5
This setting requires that you specify a key identifier in the KeyID parameter. Each packet sent on a particular network must have the configured value in its OSPF header Key ID field.

Example: AuthType=Simple

Location: Ethernet > Connections > Any connection profile > OSPF Options, Ethernet > Mod

Config > OSPF Options

See Also: KeyID

New settings for CLID-Auth-Mode

Ascend units affected: All MAX

Introduced in: 7.0.1

In this release, if the CLID-Auth-Mode parameter supports new CLID-First and DNIS-First settings in addition to the CLID-Prefer and DNIS-Prefer settings.

If CLID-Auth-Mode is set to CLID-First or DNIS-First and the calling-line ID or called number is sent by the telco switch, the MAX TNT uses it to authenticate the call. If that level of authentication fails for any reason, or if the telco switch does not provide the calling-line ID or called number, the MAX TNT does not drop the call, but allows negotiations to proceed to password authentication.

The following commands set CLID-Auth-Mode to DNIS-First:

```
admin>read answer
```

```
ANSWER-DEFAULTS read
```

```
admin>set clid-auth-mode = dnis-first
```

```
admin>write
```

```
ANSWER-DEFAULTS written
```

Rockwell (Conexant) code versions

Here are the digital modem modules and Rockwell (Conexant) code versions supported by 7.0.1:

Digital modem modules	Rockwell (Conexant) code versions
K56-8, -12, and -16	2.098
V.34 Modem-12	1.610G24
V.34 Modem-8	1.610G19

Note: Rockwell (Conexant) 2.098 supports v.90, K56flex, K56plus, and all slower, standard modem speeds.

Notice of discontinuance:

Software support for 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.x

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.

If you wish to continue using TAOS 7.0.x with software support for these V.34 slot cards, you can expect technical support, including bug fixes, for one year from the release of TAOS 7.0.0.



Caution: If you need the continued, one year support for the slot cards listed above then do not download future TAOS code releases numbered 7.1 or later as those releases will not have software support for V.34 slot cards.

High-speed modem technology

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

Upgrading 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.

This section explains how to upgrade your system software. It contains the following sections:

- Definitions and terms
- Guidelines for upgrading system software
- Guidelines for downgrading system software.
- Before you begin
- Upgrading system software with a standard load
- Upgrading system software with a fat or thin load
- Upgrading system software with an extended load
- Upgrading system software from versions earlier than 4.6C to version 5.0A or above
- Using the serial port to upgrade to a standard or a thin load
- Changing to system software that does not support V.90
- System messages

Definitions and terms

This document uses the following terms:

Build	<p>The name of the software binary.</p> <p>For example, <code>t1.m40</code> is the MAX 4000 T1 IP-only software build. For the names of all the software builds and the features they provide see <code>/pub/Software-Releases/Max/Upgrade-Filenames.txt</code> on the Ascend FTP server.</p> <p>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.</p>
Standard load	<p>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.</p> <p>TFTP is the recommended upgrade method for standard loads.</p>
Fat load	<p>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.</p> <p>You must use TFTP to upgrade to fat loads.</p>

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 <i>do</i> allow you to access the unit via Telnet. TFTP is the recommended upgrade method for restricted loads. Pipeline releases do not have 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 20 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 15.
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 16.
Extended load (6.0.0 or later)	“Upgrading system software with an extended load” on page 19.

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 which clears the MAX unit’s flash memory.
- 3 Enter NVRAMCLEAR which clears the MAX unit’s main configuration and resets the MAX.

The MAX restarts and loads the older version of system software.

- 4 When the MAX is up, manually enter basic information being sure to include at least IP address, subnet mask, and default gateway to the Ethernet interface.
After entering you must be able to telnet to 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 as in the following example:

> trestore tftp-server router1.cfg
This restores the configuration named router1.cfg from the TFTP home directory of the server named tftp-server. This file must exist and be readable.
- 7 At the > prompt, enter Exit to return to the VT100 interface.

Before you begin

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, <i>does</i> 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 will 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 21.
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Ascend technical support.	<p>To ensure that you load the correct software binary, you should check the load currently installed on your unit. To do so:</p> <ol style="list-style-type: none"> 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. <p>If your unit does not display the current load or you are unsure about which load to use, contact technical support.</p>

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.	<p>For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as <code>tbim.m40</code>), obtain a thin load of the same build (such as <code>5.0A tbim.m40</code>).</p> <p>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 <code>rtbam.m40</code> 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.</p> <p>Newer Pipeline 50 or 75 units do not have fat loads and no Pipeline units have extended or restricted loads. Refer to <code>/pub/Software-Releases/Pipeline/Upgrade-FileNames.txt</code> to determine if you have a new Pipeline 50 or 75 unit.</p>
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.	<p>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.</p> <p>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.</p>

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 21.

Using TFTP to upgrade to a standard load

To upgrade to a standard load using TFTP, you only have to enter a few commands. But you must enter them in the correct sequence, or 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.

Upgrading system software

Upgrading system software with a fat or thin load

- 3 At the > prompt, use the Tsave command to save your configuration as in the following example:

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

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. 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 20 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 “Definitions and terms” on page 11 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, as in the following example:

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

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. 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:

```
nvrnclear
```

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 20 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 “P” 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, as in the following example:

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

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. 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).

Upgrading system software

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



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:

```
nvrnclear
```

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:

```
nvrnclear
```

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 15.
- 2 Load version 5.0A, following the procedure in “[Upgrading system software with a fat or thin load](#)” on page 16.
- 3 Load version 5.0Aix or 6.0.0, following the procedure in “[Upgrading system software with a fat or thin load](#)” on page 16 (for software versions 5.0Aix) or “[Upgrading system software with an extended load](#)” on page 19 (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. Since the backup file is readable text, 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 15.)

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

- 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 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.

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.

Changing to system software that does not support V.90

If the software version on the MAX supports Rockwell (Conexant) V.90 code, the default value for the Ethernet > Mod Config > TServ Options > MDM Modulation parameter is V.90. If you downgrade to a software version on the MAX that does not support Rockwell (Conexant) V.90 code, you must set the MDM Modulation parameter to either K56 or V.34. In general, if you downgrade to older software versions and need to restore a configuration, you must originally have saved the configuration from a MAX running the older version of code.

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 16.

Table 5. System software messages (continued)

Message	Explanation
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 16.
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 19.
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 19.

Upgrading system software

System messages

Table 5. System software messages (continued)

Message	Explanation
UART initialized extended load: <code>inflate essential .+.+.+</code> <code>inflate expendable.....</code> starting system...	Indicates you have successfully loaded an extended load.
UART initialized thin load: <code>inflate</code> <code>.....</code> starting system...	Indicates you have successfully loaded a thin load.