Lucent Technologies
Bell Labs Innovations



MAX™ TAOS 8.0.5

Cumulative Release Note

July 2001

Copyright© 2001 Lucent Technologies Inc. All rights reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Lucent Technologies. For permission to reproduce or distribute, please email your request to techpubs@ascend.com.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Edge Access Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

4ESS, 5ESS, A Network of Expertise, AnyMedia, APX 8000, AqueView, AUDIX, B-STDX 8000, B-STDX 9000, ...Beyond Compare, CaseView, Cajun, CajunDocs, CAJUNVIEW, Callmaster, CallVisor, CBX 500, CellPipe, ChoiceNet, ClearReach, ComOS, cvMAX, DACScan, Dacsmate, Datakit, DEFINITY, Definity One, DSLMAX, DSL Terminator, DSLPipe, DSLTNT, Elemedia, Elemedia Enhanced, EMMI, End to End Solutions, EPAC, eSight, ESS, EVEREST, Gigabit-scaled campus networking, Globalview, GRF, GX 250, GX 550, HyperPATH, Inferno, InfernoSpaces, Intragy, IntragyAccess, IntragyCentral, Intuity, IP Navigator, IPWorX, LineReach, LinkReach, MAX, MAXENT, MAX TNT, Multiband, Multiband PLUS, Multiband RPM, MultiDSL, MultiVoice, MultiVPN, Navis, NavisAccess, NavisConnect, NavisCore, NavisRadius, NavisXtend, NetCare, NetLight, NetPartner, OneVision, Open Systems Innovations, OpenTrunk, P550, PacketStar, PathStar, Pinnacle, Pipeline, PMVision, PortMaster, SecureConnect, Selectools, Series56, SmoothConnect, Stinger, SYSTIMAX, True Access, WaveLAN, WaveMANAGER, WaveMODEM, WebXtend, and Where Network Solutions Never End are trademarks of Lucent Technologies Inc. Advantage Pak, Advantage Services, AnyMedia, ...Beyond Compare, End to End Solutions, Inter.NetWorking, MAXENT, and NetWork Knowledge Solutions are service marks of Lucent Technologies Inc. Other trademarks, service marks, and trade names mentioned in this publication belong to their respective owners.

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

C++ Standard Template Library software copyright© 1994 Hewlett-Packard Company and copyright© 1997 Silicon Graphics. Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Neither Hewlett-Packard nor Silicon Graphics makes any representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Berkeley Software Distribution (BSD) UNIX software copyright© 1982, 1986, 1988, 1993 The Regents of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley, and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ordering Information

You can order the most up-to-date product information and computer-based training online at http://www.lucent.com/ins/bookstore.

Feedback

Lucent Technologies appreciates any comments about this release note. Please send them to techcomm@lucent.com.

Lucent Technologies

Contents

What's new in 8.0.5 1

Problems corrected ***1***

Also in this release ***2***

How to use this release note ***2***

Customer Service ***3***
Finding information and software 3
Obtaining technical assistance 3

Notices 4

Notice of TAOS 8.0.5 software upgrade and release note availability ***4***

Notice of modified RADIUS username and password lengths ***4***

Notice of canned and canless slot cards ***5***

Firmware versions 6

Upgrading to (and downgrading from) TAOS 8.0.5 7

MAX 3000 T1 users might need to upgrade memory and firmware before loading TAOS 8.0.5 ..... ***7***

Staying with the same build ***7***

Selecting the method ***8***

Using TFTP to upgrade ***8***

Using the serial port to upgrade ***9***
Preparing to upgrade 9
Saving your configuration 10

Upgrading the software 10
Restoring the configuration 11
Restoring passwords 12

Using TFTP to downgrade..... 12

Using the serial port to downgrade..... 13
Preparing to downgrade 14
Save the current configuration 14
Downgrading the software 15
Restoring the configuration 15
Restoring passwords 16

Problem corrections from previous releases 17

Known issues 22

This release note describes corrections introduced in True Access™ Operating System (TAOS) releases after 8.0.4 for the MAX 6000, MAX 3000 and MAX 800.

Lucent's TAOS runs on Lucent'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 to (and downgrading from) TAOS 8.0.5" on page 7 to load this version of software onto your system. Read the instructions carefully before upgrading your system. When downgrading software, the MAX unit's configuration could be lost. For complete information, refer to "Upgrading to (and downgrading from) TAOS 8.0.5" on page 7.

Note: The diagnostic command Avm is now called Lanport modem.

Note: The MegaMAX feature is not supported on any 8.0.x version of software. The MegaMAX feature is currently supported in software version 7.4.9, and information on the feature is available in the Release Notes supporting 7.4.9, available on `ftp.ascend.com`. Please contact your authorized dealer for information on ordering the MegaMAX feature.

Note: Release 8.0.5 does not support MultiVoice.

What's new in 8.0.5

Problems corrected

This cumulative release note describes corrections introduced in software releases after 8.0.1 for the MAX. Releases since 8.0.1 have been cumulative. This current release includes all changes since 8.0.4.

TR	Problem corrected
6001059	The MAX stopped taking incoming R2 signalling calls.
6001311	A MAX 6000 unit did not present the IP address of each frame relay connection to an SNMP manager.
6001312	The MAX occasionally rebooted itself issuing a warning 106 and a reset 385.
6001318	The Serial WAN interface indicated it was down when it was actually up and running Frame Relay.
6001422	MAX occasionally stopped routing when using NAT.
6001444	L2TP username was truncated in Syslog messages.

TR	Problem corrected
6001544	A MAX unit processed dial-in user sessions when the unit was configured to utilize MP, Callback, and RADIUS.
6001581	The MAX could not activate the second nailed BRI connection.
6001713	When a MAX unit would receive a RIP update, the console would freeze or a low throughput was observed.
6001742	MAX 6048 could not recognize V.90 S56 III Modem cards.
6001773	TAOS software loads for MAX 3000 BRI units (`m30abxkh` and `m30bixkh`) did not include proxy ARP support.
6001900	Incomplete MIF commands caused the MAX to send Warnings 330 and reset, generating an FE1.
6001901	On a MAX 6000, the MRU value in the Frame Relay profile could not be set beyond the default of 1524.
6001989	MIF Dial command did not work.
6002137	TCP CLEAR packets counts were inaccurate.
6002141	The immediate modem service on the MAX 3000 only worked with the default port value of 5000.
6002170	The MAX ignored the sub-address in BACP call back to add MP channels.
6000154	The MAX set the bearer capability in setup to *speech* rather than *3.1-kHz audio* for Modem & IP Fax outgoing calls.

Also in this release

"Problem corrections from previous releases" on page 17 lists the Trouble Report (TR) corrections in numerical order from previous releases.

"Known issues" on page 22 describes issues that you should be aware of before loading this release.

How to use this release note

To use this release note:

1 Read through the table of contents to determine which software releases apply to your environment.

2 Obtain the binary file from the Lucent Technologies eSight™ Service Center at `http://www.esight.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 to (and downgrading from) TAOS 8.0.5" on page 7.

3 Upgrade to the new software by following the instructions in "Upgrading to (and downgrading from) TAOS 8.0.5" on page 7. Then configure the features that apply to your site.

Note: See "Notice of TAOS 8.0.5 software upgrade and release note availability" on page 4.

Customer Service

To obtain product and service information, software upgrades, and technical assistance, visit the eSight™ Service Center at `http://www.esight.com.` The center is open 24 hours a day, seven days a week.

Finding information and software

The eSight Service Center at `http://www.esight.com` provides technical information, product information, and descriptions of available services. Log in and select a service. The eSight Service Center also provides software upgrades, release notes, and addenda.

Obtaining technical assistance

The eSight™ Service Center at `http://www.esight.com` provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone.

If you need to contact Lucent Technologies for assistance, make sure that you have the following information available:

- Active contract number, product name, model, and serial number
- Software version
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- 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 Lucent product
- Type of computer you are using
- Description of the problem

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or eSight Live chat. Select one of these sites when you log in to `http://www.esight.com`.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information on eSight or if you have a very urgent need, contact TAC. Access the eSight Service Center at `http://www.esight.com` and click `Contact Us` below the Lucent Technologies logo for a list of telephone numbers inside and outside the United States.

You can alternatively call (800) 272-3634 for a menu of Lucent services, or call (510) 769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Notices

Notice of TAOS 8.0.5 software upgrade and release note availability

TAOS 8.0.5 software upgrades and release notes might not be immediately available at the eSight™ Service Center at `http://www.esight.com`. To obtain TAOS 8.0.5 software upgrades and release notes for this product immediately after release, go to `ftp.ascend.com`.

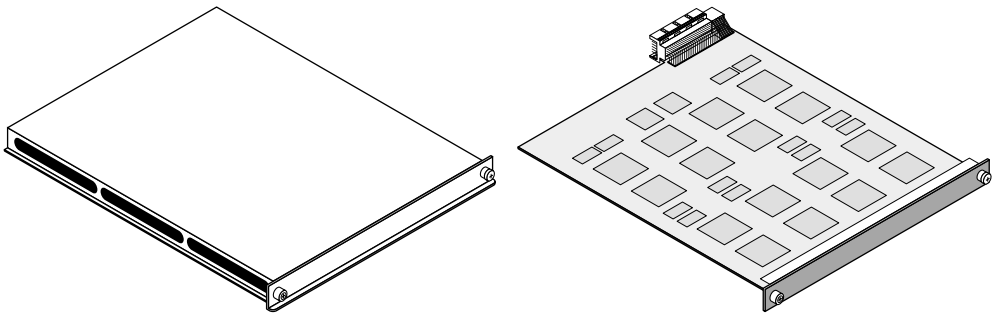
Notice of modified RADIUS username and password lengths

The following changes were made to bring MAX TAOS 8.0.5 into compliance with the IETF RADIUS draft version draft-ietf-radius-radius-v2-03.txt:

- MAX units now send username and password strings without any extraneous characters. This brings the unit into compliance with the IETF RADIUS draft. Further, the reported username and password lengths are now correct.
- MAX units no longer submit a RADIUS authentication request if the password exceeds 128 characters in length. Instead, the unit considers this an authentication failure and disconnects the call.

Notice of canned and canless slot cards

The following cards, whether in canned form (with the top sheetmetal cover) or canless form (without the sheetmetal cover), have the same functionality: A canopened slot card is a card whose sheetmetal cover has been removed. The MAX 6000 supports both canned and canless cards. The MAX 4000 supports only canned cards. And the MAX 3000 supports only canless slot cards.



Canless Wide Body Cards:		
0800-0196-051	MX-SL-8BRIN-C	8 port ISDN BRI N S/T Ntwk card, canless
0800-0196-053	MX-SL-8BRIT-C	8 port ISDN BRI T S/T Terminal, canless
0800-0097-051	MX-SL-8BRIU-C	8 port ISDN BRI U/T, canless
0800-0199-051	MX-SL-IDSL8-C	8 port IDSL, canless
Canless Kit Cards:		
0800-0179-103	MX-SL-DSP8-CO	8 port PHS card, canopened
0800-0179-102	MX-SL-DSP12-CO	12 port PHS card, canopened
0800-0179-101	MX-SL-DSP16-CO	16 port PHS card, canopened
0800-0179-109	MXV-SL-DSP8-CO	8 port MultiVoice card, canopened
0800-0179-108	MXV-SL-DSP12-CO	12 port MultiVoice card, canopened
0800-0179-107	MXV-SL-DSP16-CO	16 port MultiVoice card, canopened
0800-0192-101	MX-SL-2PMHP-CO	2 port IMUX card, canopened
0800-0195-101	MX-SL-6PMHP-CO	6 port IMUX card, canopened
0800-0670-101	MBX-SL-POTSFXS-CO	MAX POTS card, canopened
0800-0198-101	MX-SL-8V110-CO	8 port V110 card, canopened

Firmware versions

This release supports the following firmware versions:

Series56 digital modules—Mindspeed Technologies (a Conexant Systems company), V2.0982-K56_DLP_CSM firmware includes support for V.90, K56flex, K56plus, and all slower, standard modem speeds.

V.90 Series56 III modules—Mindspeed Technologies firmware version V5.8177 includes support for K56flex, K56plus, and all slower, standard modem speeds.

MultiDSP modules—Analog Devices, Inc. (ADI) firmware versions include:

- v0.1.46 (Controller)
- v0.1803.0 (RAS)

Upgrading to (and downgrading from) TAOS 8.0.5



Caution: TAOS 8.0.5 uses a new configuration file format which is incompatible with the format used in previous TAOS releases. The upgrade process automatically converts the MAX unit's configuration file to the new format. If it ever becomes necessary to revert back to a previous TAOS release, you will need a backup copy of the configuration file created using the older format. Failure to create and save a backup copy of the configuration prior to upgrading to TAOS 8.0.5 will result in a loss of all configuration information for the MAX unit.

You must read and understand the following sections before you upgrade to TAOS 8.0.5 or downgrade from TAOS 8.0.5. They instruct you to stay with the same build, instruct you how to upgrade to TAOS 8.0.5 using TFTP or the serial port, and instruct you how to downgrade from TAOS 8.0.5 using TFTP or the serial port.

MAX 3000 T1 users might need to upgrade memory and firmware before loading TAOS 8.0.5

If you have a MAX 3000 T1 unit that is Rev A, Rev B, or a numeric revision, you need to order the 32MB SDRAM upgrade kit, part number MX30-HO-32MB, *before* you load TAOS 8.0.5 onto your unit. The unit's revision number (Rev) is noted on the large label on the bottom of the unit. Call 1-510-769-6001 (8am - 5pm PST) and ask for order administration to obtain the upgrade kit free of charge.

The upgrade kit includes a 32MB SDRAM DIMM and important instructions for obtaining and loading new boot firmware on the MAX 3000 T1 before installing the memory upgrade.

Staying with the same build

A *build* is the name of a software binary. For example, `ebixk.m60` is the MAX 6000 E1 IP-only software build compatible with BRI, X.25, and K-56 series modems. For the names of all the software builds and the features they provide see `/pub/Software-Releases/Max/Upgrade-Filenames.txt` on the Lucent Technologies, Inc. FTP server.

If possible, you should always stay with the same build of software when you upgrade or downgrade. If you install a different version, your unit may lose its configuration. If this happens, you may need to manually restore your configuration. There may be no automated way to restore configuration data from a backup when changing builds since, if the file formats between the builds are incompatible, no suitable backup exists.

If you use TFTP to transfer a build intended for a different type of network interface. For example, your MAX unit may have a T1 interface and you are attempting to transfer a build that is appropriate for an E1 interface. In such a case, the MAX unit can display the following message:

```
This load appears not to support your network interface.
Download aborted. Use tloadcode -f to force.
```

When the build is intended for different type of network interface, verify again that you have selected the correct build. If you use TFTP to transfer a build intended for another type of unit, the MAX unit displays the following message:

```
This load appears to be for another platform.
Download aborted. Use tloadcode -f to force.
```

When the build is intended for another type of unit, it is not recommended that you do this.

Selecting the method

If possible, change your MAX unit's system software using TFTP (Trivial File Transfer Protocol). TFTP provides you with a more reliable way to obtain, store, and then upgrade or downgrade the system software to your unit than the alternative, which is through the serial port of the unit.

Using TFTP to upgrade

To upgrade 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 MAX unit's configuration.

To upgrade system software by way of TFTP:

1. Locate the correct build of the software version you want to upgrade to and place it in the TFTP server home directory.
2. From the MAX unit's VT100 interface, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
3. At the > prompt, use the `Tsave` command to save your configuration in a way that allows you to match it with the version of system software with which it is compatible. For example, the following command restores the configuration named `config700.cfg` from the TFTP home directory of the server named `tftp-server`:

   ```
   tsave -m tftp-server config700.cfg
   ```



Caution: If it becomes necessary to downgrade from TAOS 8.0.1, you must be able to locate the configuration that is compatible with the system software. Otherwise, you may need to manually reconfigure the MAX unit.



Caution: The MAX unit's internal flash storage is limited. Use the `tsave -m` command to assure that the configuration you save is as small as possible. You must retain the saved configuration file permanently. You will need this file if it ever becomes necessary to revert back to the older version after you upgrade the unit to TAOS 8.0.5.



Caution: The file you save with the `Tsave` command contains all the passwords in clear text. 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 ebixk.m60
```

places `ebixk.m60` into flash from the machine named `tftp-server`.

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

```
> fsave
```

Use the `Fsave` command immediately after executing the `Tload` command.

6 Enter the following command:

```
> nvramclear
```

After the MAX unit clears NVRAM memory, the unit automatically resets itself two times.

This completes the upgrade to TAOS 8.0.5.

Using the serial port to upgrade



Caution: Upgrading system software by way of 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 MAX unit's user interface. To avoid having existing profiles overwritten, use TFTP to upgrade your unit. If you have many profiles and passwords, you should consider using TFTP to upgrade your software. (See "Using TFTP to upgrade" on page 8.)

Preparing to upgrade

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

- An IBM compatible PC or Macintosh system with a serial port capable of connecting to the MAX unit's Console port.
- A straight-through serial cable.
- Data communications software for your system with an appropriate communications software (for example, Procomm Plus, HyperTerminal for the PC or ZTerm for the Macintosh).



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 file transfer to halt, and can render the MAX 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 MAX unit's 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 transferred to your hard disk. When the file has been saved, your communications program displays a message indicating the transfer 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 save the file to the MAX.

Upgrading the software

To upgrade 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 MAX.

Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your MAX. 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 file transfer, the MAX resets. Upon completion of the self-test, the MAX unit’s initial menu appears in the Edit window with all parameters set to default values.

If the connection fails during the transfer, try obtaining another copy of the binary image from the Lucent Technologies, Inc. FTP server and upgrading the software again. If you still have problems, contact Lucent Technologies, Inc. technical support for assistance.

Restoring the configuration

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 gather more specific configuration information obtained from Lucent Technologies, Inc. (for example, a single filter stored in a special configuration file).

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

1 From the MAX unit’s VT100 interface, access the diagnostics monitor by pressing 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.



Caution: The compatible configuration file is not the one that you saved at the beginning of these steps. Use the saved configuration file in the event you downgrade from TAOS 8.0.5.

(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 MAX 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 transfer 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.

Using TFTP to downgrade

To downgrade system software 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 MAX unit's configuration.

1 Locate the following and place them in the TFTP server home directory:

- The configuration for the MAX unit that is compatible with the version of TAOS to which you will downgrade.
- The build of the system software version to which you will downgrade.

2 From the MAX unit's VT100 interface, 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 `config800.cfg` from the TFTP home directory of the server named `tftp-server`:

```
tsave -m tftp-server config800.cfg
```



Caution: If you need to upgrade once again to TAOS 8.0.1, you must be able to locate the configuration that is compatible with the system software. Otherwise, you may need to manually reconfigure the MAX unit.You must name the configuration file in a way that allows you to match it with the version of TAOS system software with which it is compatible. For example, save the configuration that is compatible with TAOS 8.0.1 as `Config800`.



Caution: The MAX unit's internal flash storage is limited. Use the `tsave -m` command to assure that the configuration you save is as small as possible. You must retain the saved configuration file permanently. You will need this file if it ever becomes necessary to upgrade the unit to TAOS 8.0.5 once again.



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

4 Enter the following command to downgrade the system software:

`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 ebixk.m60`

places `ebixk.m60` into flash from the machine named `tftp-server`.

5 Enter the following command to restore the compatible configuration to flash memory:

`trestore -f` *`hostname savedConfig`*

where ***`hostname`*** is the name or IP address of your TFTP server, and ***`savedConfig`*** is the compatible configuration on the server (relative to the TFTP home directory).

For example, the command:

`trestore -f tftp-server Config700`

places `Config700`, a configuration compatible with TAOS 7.0.0, from the unit named `tftp-server`.

Note: The `-f` is necessary in this step. Failure to use the `-f` will cause trestore to place the configuration in binary format into NVRAM, rendering the configuration unusable to the MAX unit.

6 Enter the following command:

`> nvramclear`

After the MAX unit clears NVRAM memory, the unit automatically resets itself two times.

This completes the downgrade from TAOS 8.0.5.

Using the serial port to downgrade



Caution: Downgrading system software by way of the serial console overwrites all existing profiles. Save your current configuration settings to your hard disk before you begin downgrading system software. After the downgrade, restore your configuration from the backup file you created. The backup file is readable text, so you can reenter the settings through the MAX unit's user interface. To avoid having existing configuration files overwritten, use TFTP to downgrade your unit. If you have many profiles and passwords, you should consider using TFTP to downgrade your software. (See "Using TFTP to downgrade" on page 12.)

Preparing to downgrade

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 MAX 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 transfer to halt, and can render the MAX unusable.

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.

Save the current configuration

To save the MAX unit's 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 transferred to your hard disk. When the file has been saved, your communications program displays a message indicating the transfer 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 transfer the file to the MAX.

Downgrading the software

To downgrade the system 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 MAX.

   Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your MAX. 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 file transfer, the MAX resets. Upon completion of the self-test, the MAX unit’s initial menu appears in the Edit window with all parameters set to default values.

If the file transfer fails during the transfer, try obtaining another copy of the binary image from the Lucent Technologies, Inc. FTP server and downgrading the software again. If you still have problems, contact Lucent Technologies, Inc. technical support for assistance.

Restoring the configuration

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 gather more specific configuration information obtained from Lucent Technologies, Inc. (for example, a single filter stored in a special configuration file).

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

1. From the MAX unit’s VT100 interface, access the diagnostics monitor by pressing 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 compatible configuration file to the unit.



Caution: You must install the compatible configuration that you saved before you upgraded to TAOS 8.0.5. If you did not save a compatible configuration, you must manually reconfigure the MAX 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 MAX 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 downgrading, 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 transfer 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.

Problem corrections from previous releases

The TR number and problem corrected in previous releases are listed in numerical order in Table 1.

Table 1. Problems corrected for the MAX

TR	Problem corrected	Corrected in
NA	MultiVoice: VOIP was not sending meaningful progress codes and cause codes in syslog messages.	8.0.4
NA	MultiVoice: An incorrect ARQ handle in ARQ was being sent by the gateway to the gatekeeper, causing call failures.	8.0.4
NA	FoIP: Polling Time (between DCS and TCF) must be 80ms: This fix makes the delay between receipt of the digital command signal (DCS) and training check frame (TCF) for Real-time fax operations platform dependent for MultiVoice Gateways. Previously, the time interval between transmission of DCS and TCF from the originating fax could exceed 80 ms on the MAX, causing training of the destination fax to fail.	8.0.3
NA	Improved call setup rate for MultiVoice calls: This set of fixes enhanced call setup operations for MultiVoice VoIP calls, raising the call setup rate to somewhere between 5 and 6 calls/sec. Previously, the current sustainable call setup rate for MultiVoice was approximately 2 calls/sec (with 500-600 active calls, 2 calls are torn down and 2 new calls originate each second).	8.0.3
NA	A MAX 6000 returned FE1 under load if 24 fax calls: This fix eliminates a fatal error which could occur when active call volume for MultiVoice Real-time fax calls reached or exceeded 24 simultaneous calls.	8.0.3
NA	Improvements in call setup and performance for MultiVoice: This set of fixes is part of an continuing effort to improve call setup rates and call processing. These specific fixes include the following: • Changes in the method of port caching for VoIP calls on a MAX • Modifications of H.225/H.245 call setup and processing to maximize VoIP call throughput to support processing higher volumes of call.	8.0.3
NA	No information was written to flash memory at the time of a reset.	8.0.3
3844	Warning 175 occasionally occurred with AppleTalk routing.	8.0.3
4047	MAX was not reporting correct service type for V.120.	8.0.2
4427	MAX was not releasing IP route entry information to the Vrouter Connection profile.	8.0.2
4616	MAX 4000 and MAX 2000 were occasionally resetting with FE 29 when running X.25 PAD.	8.0.2
5094	On MAX 6000 and MAX 4000, PRI channels would become overloaded and outgoing ISDN calls were occasionally unavailable.	8.0.2

Table 1. Problems corrected for the MAX (continued)

TR	Problem corrected	Corrected in
5452	Warning 104 occasionally displayed in the Fatal Error log in Diagnostic mode on the MAX.	8.0.4
5467	With SNTP enabled, the MAX generated an incorrect value for Acct-Session-Time in the RADIUS accounting STOP record.	8.0.3
5603	PIAFS version 2.1 call was always reported at 32k speed.	8.0.3
5664	CSM/3 modem cards would generate warning 384s (displayed in the Fatal Error log in Diagnostic mode).	8.0.4
5671	Calls terminated with disconnect/progress code of 9/2, indicating no modems were available.	8.0.3
5677	MAX 6000 occasionally reset with FE 8.	8.0.2
5682	V.42 compression for PIAFS was always disabled.	8.0.2
5697	On an outgoing call, the MAX 6000 was sending garbage packets before starting Link Control Protocol (LCP).	8.0.2
258778	Channel signaling on DASS2/DPNSS E1 lines stopped after a few hours of operation.	8.0.2
258789	MS-CHAP failed on MAX 200 and MAX 800.	8.0.4
258875	MAX did not recognize the CLI (Calling Line Id). The result of this not being recognized is that any authentication based on CLI, using a DPNSS line would fail, because the MAX ignored the CLI info that the switch sent to it.	8.0.3
258930	When a MAX came up after a reboot, with a configured RADIUS server it sent a message to the server indicating that any addresses allocated from RADIPAD to that unit should be freed.	8.0.4
258937	Terminal server settings were not being activated.	8.0.2
258938	DASS2/DPNSS PRI failed when receiving Channel Seize message from Marconi switch.	8.0.3
6001049	Nailed BRI card on MAX 3000 did not work.	8.0.4
6001085	Firewall was not refreshed for callback users defined in RADIUS.	8.0.4
6001088	OSPF AreaType parameter wasn’t setting Options bits in the OSPF header correctly.	8.0.4
6001089	PPTP Control Connection was not disconnecting after all sessions had ended.	8.0.4
6001140	Open modem command with a zero modem value occasionally caused the unit to reboot.	8.0.4

Table 1. Problems corrected for the MAX (continued)

TR	Problem corrected	Corrected in
6001141	When the image on the MAX 6000 external PCMCIA flash card became corrupted, the unit was not retrieving the good backup image from the internal flash.	8.0.4
6001154	On a MAX 6000, IPX routing table was not properly updating the local connection profile.	8.0.3
6001202	MAX 6000 reset occasionally with W106 and I385.	8.0.4
6001236	SNMP managers with write permission were not able to also read values.	8.0.4
6001253	Max 6000 telnet packets' fragment bit were set to 1 which prevented packet fragmentation.	8.0.4
6001326	Unable to configure Vrouter when the Disable Route software option was installed.	8.0.4
6001443	Username was not being reported in syslog when a tunnel failed to be established.	8.0.4
6001467	The customer was not receiving cause code 11 when CSM3 modems were used.	8.0.4
6001901	On a MAX 6000, the MRU value in the Frame Relay profile cannot be set beyond the default of 1524.	8.0.4
6002017	The MAX 4000 and MAX 6000 were dedicated to outgoing fax calls and telnetting to these units would occasionally create excessive ethernet traffic.	8.0.4
1000207	On a MAX 4000, the Fatal Error History Log displayed the incorrect security profile for the user.	8.0.3
1000260	Using a 128k ATMP connection the user only got 64k during FTP downloads.	8.0.3
1000281	On a MAX 6000, the Show users command would display a nonactive stacking channel as being used.	8.0.2
6000125	The RADIUS accounting record Acct-Session-Id had a trailing 0x00, when it should have been suppressed if the external auth profile had a vendor-specific value.	8.0.2
6000134	X.25 B-channel startup in AO/DI was not less than 5 seconds.	8.0.3
6000158	RADIUS accounting packets were not sent when user accounting was configured.	8.0.2
6000160	The MAX rejected calls for an AO/DI connection.	8.0.3
6000169	Upon reset, the subnet routes were not being propagated properly.	8.0.2

Table 1. Problems corrected for the MAX (continued)

TR	Problem corrected	Corrected in
6000236	MAX 800 occasionally rebooted, generating a Fatal Error 15 message in Diagnostic mode.	8.0.4
6000238	An analog PPP session was not established with a MAX when the call was terminated on a CSM/3 modem card.	8.0.3
6000248	AO/DI MPP Bundle was not being released properly.	8.0.4
6000256	The debug screen failed to respond properly.	8.0.2
6000273	A MAX exhibited Warning 104 and stopped routing calls when the unit was placed on a D4 AMI circuit.	8.0.3
6000297	Core Interop testing showed many `missing OK` messages in the syslog.	8.0.3
6000298	The CSM/3 card was failing POST.	8.0.2
6000316	Ipxping did not work for the MAX.	8.0.3
6000360	Occasionally, warning 179 occurred on the MAX 6000 with AppleTalk dialup.	8.0.3
6000366	PPP IP address negotiation was not working properly.	8.0.2
6000373	AO/DI - MAX occasionally sent RADIUS accounting records with unusually large data volumes.	8.0.3
6000422	MAX incorrectly required only a numeric value for Filter ID.	8.0.3
6000446	Channel information was not appearing in the end-of-call syslog message.	8.0.3
6000448	The primary RADIUS server could not be specified using SNMP.	8.0.3
6000458	Frame Relay backup connection intermittently drops and never recovers.	8.0.3
6000462	Edit All Calls=No and the Name/Password profiles was still editable.	8.0.3
6000501	Modem calls were forwarded to HDLC even though some of the modems were moved to the "Modems on pending 195 list."	8.0.4
6000541	Outgoing modem calls would fail because the first available modem was found in a slot other than the value found in the T1 configuration.	8.0.4
6000557	When quiescing line 1, line 2 would go offline. When quiescing line 3, line 4 would go offline. Also, you could not quiesce line 2 or line 4.	8.0.4
6000559	When a MAX received a V.110 call (but did not support V.110), it disconnected the call and reported a disconnect/progress code of 2/2.	8.0.4
6000570	Modem failed CLID authentication and was removed from currently active modems.	8.0.3

Table 1. Problems corrected for the MAX (continued)

TR	Problem corrected	Corrected in
6000580	MAX 3000 did not accept incoming IDSL calls.	8.0.4
6000585	On a MAX 6000 the Thailand E1/R2 register signaling had a failing digit.	8.0.4
6000609	Radius Accounting did not include the TCP-Clear Destination and the Session Length for local Connection profiles.	8.0.3
6000626	Using the Finger command, the MAX 6000 did not list users after reboot.	8.0.3
6000627	The behavior for the callStatusTable's index was not assigned the same way as ssnStatusTable's index.	8.0.2
6000632	MAX 4000 occasionally rebooted, generating a Fatal Error 1 message in Diagnostic mode.	8.0.4
6000638	Fatal history showed incorrect code revision on the MAX 6000.	8.0.3
6000657	Acct-Authentic information was not saved across callbacks.	8.0.4
6000694	MultiVoice: In NT mode, T1/E1 lines were unable to take VOIP calls when trunk groups were enabled.	8.0.4
6000704	Disconnect code 1 and 2s were occurring on the MAX 6000.	8.0.2
6000709	CLID/DNIS authenticated L2TP V120 sessions didn't come up.	8.0.4
6000712	When MAX had Client DNS server configured, MAX returned Configure-Reject with DNS options, and PC could not negotiate DNS address.	8.0.4
6000753	Show users command produced incorrect Slot:Port information on the terminal server.	8.0.4
6000781	The LCD menu incorrectly set some fields as N/A.	8.0.4
6000877	The connection failed when the MAX 800 BRI outgoing call was configured on channel 00.	8.0.4
6000910	MAX 6000 CSM3 card provided wrong ambient temperature information.	8.0.4
6000928	When a PIAFS call could not be connected because all ports on the PIAFS card were in use, the incoming call should have been disconnected with a USER_BUSY disconnect code rather than a NORMAL_CLEARING code.	8.0.4
6000995	MAX 6000 with 8.0.3 rebooted, generating a Fatal Error 29 message in the Diagnostic mode.	8.0.4
6001016	The MAX unit could not find the proper connection profile for IPX nodes allocated from the IPX pool network.	8.0.4
6001029	DS1 interface data displayed only for 3 of the 4 available DS1 interfaces.	8.0.4

Table 1. Problems corrected for the MAX (continued)

TR	Problem corrected	Corrected in
6001030	Compression Control Protocol (CCP) request with null options list was not being accepted.	8.0.4
6001033	The first PPP frame received from a dialup modem client was being ignored by the MAX.	8.0.4
6001048	MAX was not disconnecting a call when authentication failed.	8.0.4
6000043	Occasionally, warning 179s would occur when booting the MAX 6000 with a PIAFS card.	8.0.3
6000082	Occasionally, MAX 6000 reset with FE 38.	8.0.3
6000088	Fatal errors were occasionally occurring on incoming calls.	8.0.3

Known issues

Issues you should be aware of before loading release 8.0.5 include the following:

- Performing hash-code upgrades following a TAOS Release downgrade:

  If you downgrade from TAOS 8.0.x to TAOS 7.x.x on a unit with an 8-digit serial number, do not use the revision command to perform hash-code upgrades. Use the update command only.

- Change in Call-logging packet format

  In releases prior to 7.2.0, the format of Call-logging packets are identical to RADIUS Accounting packets. With the introduction of 7.2.0, Call-logging will no longer be compatible with RADIUS, although Lucent's NavisAccess product fully supports Call-logging. The MAX continues to support RADIUS accounting, SNMP and SYSLOG functionality.

  Because of the proprietary nature of and potential modification to call-logging packets, you should not use call-logging packets with any application other than Lucent's NavisAccess.

- Some multimedia features are not supported in this release. Customers using the following features should not upgrade to 8.0.1:

  – AIM/BONDING

  – Time-of-day calling

  – Backup and overflow

- The default value for the parameter CBCP Trunk group was out of the valid range. The default value has been changed from 0 to 4. This correction might cause a previously saved profile to yield a different value when this release is loaded.

- To support OSPF and dual shelf controllers on a single network, you must make sure that no more than one shelf is an OSPF Designated Router. Proceed as follows:

- In MAX units, data flows between T1/E1 WAN ports and host devices such as modems and HDLC ports using a limited group of internal data pathways. The capacity of these pathways is sufficient to accommodate the built-in WAN ports of the MAX. When BRI cards are installed in the system, pathways normally allocated for built-in T1/E1 ports are used to support the BRI WAN ports, and are not available for T1/E1 usage.

  Note: More than 64 digital (HDLC) calls requires an optional HDLC module and no more than 96 digital calls are supported under any circumstances.

  Table 2 summarizes how the addition of BRI cards affects the availability of built-in WAN ports in various MAX units. These limits apply regardless of the type of BRI card used (Net, Host, IDSL, etc.).

  Table 2. WAN ports available when BRI cards are in use

MAX unit	Number of BRI cards	WAN ports available
MAX 6000	0	1, 2, 3, 4
	1	1, 2, 3
	2, 3	1, 2
	4	1
	5, 6	None
MAX 3000	0	1, 2
	1	2