



TAOS 7.0.28

Cumulative Release Note for MAX™ 4000/2000/1800


Copyright © 2001, 2002 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 techcomm@lucent.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.

European Community (EC) RTTE compliance

 Hereby, Lucent Technologies, declares that the equipment documented in this publication is in compliance with the essential requirements and other relevant provisions of the Radio and Telecommunications Technical Equipment (RTTE) Directive 1999/5/EC.

To view the official *Declaration of Conformity* certificate for this equipment, according to EN 45014, access the Lucent INS online documentation library at <http://www.lucentdocs.com/ins>.

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

Lucent, the Lucent logo, and all Lucent brand and product names are trademarks or registered trademarks of Lucent Technologies Inc. Other brand and product names are trademarks of their respective holders.

Ordering information

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

Feedback

Lucent Technologies appreciates customer comments about this manual. Please send them to techcomm@lucent.com.

Customer Service

Product and service information, and software upgrades, are available 24 hours a day. Technical assistance options accommodate varying levels of urgency.

Finding information and software

To obtain software upgrades, release notes, and addenda for this product, log in to Lucent OnLine Customer Support at <http://www.lucent.com/support>.

Lucent OnLine Customer Support also provides technical information, product information, and descriptions of available services. The center is open 24 hours a day, seven days a week. Log in and select a service.

Obtaining technical assistance

Lucent OnLine Customer Support at <http://www.lucent.com/support> provides easy access to technical support. You can obtain technical assistance through email or the Internet, or by telephone. If you need assistance, make sure that you have the following information available:

- Active service or maintenance contract number, entitlement ID, or site ID
- Product name, model, and serial number
- Software version or release number
- 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 a Live Chat. Select one of these sites when you log in to <http://www.lucent.com/support>.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information of Lucent OnLine Customer Support or if you have a very urgent need, contact TAC. Access Lucent OnLine Customer Support at <http://www.lucent.com/support> and click **Contact Us** for a list of telephone numbers inside and outside the United States.

Alternatively, call 1-866-LUCENT8 (1-866-582-3688) from any location in North America for a menu of Lucent services. Or call +1 510-769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Contents

Customer Service 3

Introducing TAOS 7.0.28 1

 Changing TAOS System Software 1

 Enhancement in TAOS 7.0.28 11

 Firmware versions..... 11

 Known issues 11

Previous TAOS 7.0 releases..... 12

 Enhancements in previous TAOS 7.0 releases 12

 OSPF supports MD5 authentication 12

 New settings for CLID-Auth-Mode..... 14

 Alphabetical listing of additional parameters 14

 Problems Corrected in previous TAOS 7.0 releases..... 31

Introducing TAOS 7.0.28

The True Access™ Operating System (TAOS) runs on the advanced WAN access products of Lucent Technologies. These products provide modular chassis that integrate a range of technologies to enable service providers and enterprise managers to install customized network infrastructures. As new enhancements are added to TAOS, the amount of memory used by the operating system grows. Therefore, the products running later versions of TAOS report less available memory. When you install TAOS 7.0.28 you see a smaller amount of available memory on the MAX than was available to a unit that ran a previous TAOS release. This is because the software binaries have gotten bigger and the memory used to store those software binaries is greater.

This True Access™ Operating System (TAOS) maintenance release supports the following MAX WAN access units:

- MAX 4000
- MAX 2000
- MAX 1800

Note: The generally available version of the TAOS 7.0.28 software does not include software binaries for MAX 6000 or MAX 800 units. Refer to TAOS 7.0.22 software for these units. Or contact Lucent Customer Support to obtain compatible TAOS software to operate the MAX 800 unit. Log in to Lucent OnLine Customer Support at <http://www.lucent.com/support>. Alternatively, you can call 1-866-LUCENT8 (1-866-582-3688) from any location in North America for a menu of Lucent services. Or call +1510-769-6001 for an operator. However, if you do not have an active services agreement or contract, you will be charged for time and materials.

Following are the sections that describe what's new in the TAOS 7.0.28 maintenance release:

- [“Changing TAOS System Software” on page 1](#)
- [“Enhancement in TAOS 7.0.28” on page 11](#)
- [“Firmware versions” on page 11](#)
- [“Known issues” on page 11](#)

See [“Previous TAOS 7.0 releases” on page 12](#) for information about problems corrected and enhancements included with previous maintenance releases.

Changing TAOS System Software



Caution: Newer versions of TAOS, such as 8.0.x, 7.2.x, or 7.4.x, use a new configuration file format which is incompatible with the format used in previous system software releases, such as TAOS 7.0.x. The upgrade process automatically converts the MAX unit's configuration file to the new format. If it ever becomes necessary to revert back to TAOS 7.0.28, 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 newer versions of TAOS, such as 8.0.0, will result in a loss of all configuration information for the unit.

You must read and understand the following sections before you upgrade to TAOS 7.0.28 or downgrade from TAOS 7.0.28. They instruct you to stay with the same build, instruct you how to upgrade to TAOS 7.0.28 using TFTP or the serial port, and instruct you how to downgrade from TAOS 7.0.28 using TFTP or the serial port.

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 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 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 a 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 unit's VT100 interface, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
- 3 At the > prompt, use the `Tsave -m` 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 saves 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 7.0.28, 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 7.0.28.



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

This completes the upgrade to TAOS 7.0.28.

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 2.)

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 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 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 unit.

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 unit.
Your communications program normally takes anywhere from 5 to 15 minutes to send the file to the 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 file transfer, the unit resets. Upon completion of the self-test, the 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 Open the Sys Diag menu.
- 5 Select `Restore Cfg`, and press Enter.
The following message appears:
`Waiting for upload data...`
- 6 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 7.0.28.

(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`

- 7 Press any key to return to the configuration menus.
- 8 Reset the 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 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 unit's VT100 interface, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
 - 3 At the > prompt, use the `Tsave -m` command to save your configuration. For example, the following command saves the configuration named `config7026.cfg` from the TFTP home directory of the server named `tftp-server`:

```
tsave -m tftp-server config7026.cfg
```



Caution: If you need to upgrade once again to TAOS 7.0.28, 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.



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

This completes the downgrade from TAOS 7.0.28.

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 6.](#))

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 unit 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 unit.

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 unit.
Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your MAX 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 file transfer, the unit resets. Upon completion of the self-test, the 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 Open the Sys Diag menu.
- 5 Select Restore Cfg, and press Enter.
The following message appears:
Waiting for upload data...
- 6 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 7.0.28. 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

- 7 Press any key to return to the configuration menus.
- 8 Reset the 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.

Enhancement in TAOS 7.0.28

Note: TAOS 7.0.28 includes improved resistance to Denial of Service attempts.

Firmware versions

The following Conexant (formerly Rockwell) firmware versions are supported in this release:

- Series56 Digital Modem Modules support Conexant V2.098-K56_DLP_CSM firmware, which includes support for V.90, K56flex, K56plus, and all slower, standard modem speeds.
- V.34 Digital Modem Modules support Conexant V1.610G24-V34_DP (V.34 Modem-12) and V1.610G19-V34_DS (V.34 Modem).

The 2.098 Conexant firmware includes a workaround in V.8bis for Lucent Technologies interoperability, and improved Lucent Technologies client V.90 modem connectivity. Users still should upgrade their Lucent Technologies client modems with new Lucent Technologies firmware as available.

The 2.098 Conexant firmware also provides the following user features:

- Added S202/bit6 to control V90 high power after V8.
- Added S220 to control answer tone length on Server. By default, S220= 11, corresponding to 5 seconds of answer tone. Each unit in S220 corresponds to 450 ms, because each phase reversal is 450 ms long. For example, S220 = 19 will increase the answer tone time to 8.6 seconds. S220 = 03 will decrease the answer tone time to 1.4 seconds.
- Fixed semicolon (;) handling with +MS command.

Known issues

Issues you should be aware of before loading release 7.0.28 include the following:

- 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 is no longer be compatible with RADIUS, although Lucent Technologies' 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 Technologies' NavisAccess.
- Some multimedia features are not supported in this release. Customers using the following features should not upgrade to 7.0.28:

Previous TAOS 7.0 releases

Enhancements in previous TAOS 7.0 releases

- 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.
- In MAX units, data flows between T1 or 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 ISDN BRI cards are installed in the system, pathways normally allocated for built-in T1 or E1 ports are used to support the BRI WAN ports, and are not available for T1 or E1 usage.

Previous TAOS 7.0 releases

Previous TAOS 7.0 releases include enhancements and corrections, described in detail in the following sections:

- The [“Enhancements in previous TAOS 7.0 releases”](#) section describes the features introduced in this release and previous releases. They are organized by functional category.
- The [“Alphabetical listing of additional parameters” on page 14](#) describes parameters that have been introduced to the MAX unit’s VT100 interface since the release of TAOS 7.0.
- [“Problems Corrected in previous TAOS 7.0 releases” on page 31](#) lists the Trouble Report (TR) corrections in numerical order.
- [“Firmware versions” on page 11](#) lists the currently supported Conexant code versions.
- [“Known issues” on page 11](#) describes issues that you should be aware of before loading this release.

Enhancements in previous TAOS 7.0 releases

The following enhancements have been introduced since the release of TAOS 7.0.0 for the MAX family.

OSPF supports MD5 authentication

Units affected: MAX 6000, MAX 4000, MAX 2000, MAX 1800

Introduced in: 7.0.1

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

SeeAlso: 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

SeeAlso: KeyID

New settings for CLID-Auth-Mode

Units affected: MAX 6000, MAX 4000, MAX 2000, MAX 1800, MAX 800

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
```

Alphabetical listing of additional parameters

The following parameters have been introduced since release 7.0 of the TAOS system software for the MAX.

Acct Checkpoint

Description: Specifies the interval, in seconds, at which the MAX sends checkpoint packets to a daemon.

Usage: Enter a decimal number, from 0 to 60. The default is 0, which specifies that no checkpoint packets will be sent to a daemon.

Example:

```
Acct Checkpoint=60
```

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Max Retry, Acct Reset Timeout, Acct-ID Base, Allow Stop Only, Suppress Host Routes

Acct Compat Mode

Description: Enables or disables Vendor Specific Attribute (VSA) compatibility mode when the MAX is using RADIUS for accounting purposes.

When the user sets Acct Compat Mode to Old, the system uses a proprietary algorithm for encrypting and decrypting the User Password attribute. Unlike the RFC-defined algorithm, the proprietary algorithm does not null fill the password string to a multiple of 16 bytes before encryption. Also, when the password is longer than 16 bytes, the proprietary algorithm does not use the preceding segment's hash to calculate the next intermediate value.

Usage: Specify one of the following settings:

- **OLD** (the default)—Specifies that the MAX does not send the Vendor Specific attribute to the RADIUS server and does not recognize the Vendor Specific attribute if the server sends it.
- **Vendor Specific**—Specifies that the MAX both uses the Vendor Specific attribute to encapsulate Ascend vendor attributes and uses the RFC-defined User Password encryption algorithm.

Example:

```
Acct Compat Mode=Vendor Specific
```

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Checkpoint, Acct Max Retry, Acct Reset Timeout, Acct-ID Base, Allow Stop Only, Suppress Host Routes

Acct Max Retry

Description: Specifies the maximum number of retries for Accounting packets.

When the MAX is configured for RADIUS accounting, it sends Accounting Start and Stop packets to the RADIUS server to record connections. If the server does not acknowledge a packet within the number of seconds you specify for Acct Reset Timeout, the MAX tries again, resending the packet until the server responds, or dropping the packet if the queue of packets to be resent is full. You can limit the number of retries by setting a maximum.

Usage: To set the maximum number of retries for Accounting packets, set Acct Max Retry to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

Note: The MAX always makes at least one attempt. For example, if you set the number of retries to 10, the MAX makes 11 attempts: the original attempt plus 10 retries.

Example:

```
Acct Max Retry=10
```

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Checkpoint, Acct Reset Timeout, Acct-ID Base, Allow Stop Only, Suppress Host Routes

Acct Reset Timeout

Description: Specifies the number of seconds that must elapse before the MAX returns to using the primary RADIUS accounting server.

Usage: Specify the number of seconds. The default is 0 (zero), which specifies that the MAX does not return to using the primary RADIUS accounting server.

Example:

```
Acct Reset Timeout=60
```

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Checkpoint, Acct Max Retry, Acct-ID Base, Allow Stop Only, Suppress Host Routes

Acct-ID Base

Description: Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16. You can set Acct-ID Base globally or for each connection.

Usage: Specify one of the following values:

- 10 (the default)—Decimal
- 16—Hexadecimal

The value you specify controls how the MAX presents the Session ID attribute to the accounting server.

Example:

```
Acct-ID Base=10
```

Dependencies: Keep in mind the following additional information:

- If Acct does not specify RADIUS, Acct-ID Base does not apply.
- Changing the value of Acct-ID Base while accounting sessions are active results in inconsistent reporting between the Start and Stop records.

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Checkpoint, Acct Max Retry, Allow Stop Only, Suppress Host Routes

Allow Stop Only

Description: Specifies whether the MAX should send an Accounting Stop packet that does not contain a username. (At times, the MAX can send an Accounting Stop packet to the RADIUS server without having sent an Accounting Start packet. These Stop packets have no username.)

Usage: Specify Yes or No. Yes is the default.

Example:

Allow Stop Only=No

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Checkpoint, Acct Max Retry, Acct-ID Base, Suppress Host Routes

Apply To

Description: Specifies how the type of service applies to data flow for each connection.

Usage: Specify one of the following values:

- Incoming—The MAX applies the type of service filter to incoming traffic for this connection.
- Outgoing—The MAX applies the type of service filter to outgoing traffic for this connection.
- Both—The MAX applies the type of service filter to incoming and outgoing traffic for this connection.

Dependencies: If TOS Enabled=No, the Apply To setting is not applicable.

Location: Ethernet>Connections>*any connection profile*>IP Options

SeeAlso: Precedence, Source IP Check, TOS, TOS Enabled, TOS Filter

Ascend

Description: Specifies whether a trap is generated to indicate a change of state in a host interface. All port connections are monitored in a state machine and reported by this trap.

Usage: Specify Yes or No. The default is Yes.

Example:

Ascend=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable Traps

SeeAlso: SNMP authentication

AT Answer String

Description: User specifies AT commands to be added to the answer string of the MAX unit's default modem configuration.

Usage: Specify one or more valid AT commands, up to a limit of 36 characters. The default is null.

Do not begin the string with the characters AT. These two characters are automatically added to the beginning of the string, before the MAX sends the commands to the modem.

Do not include an A (answer) or a D (dial) command anywhere in the string. The MAX automatically adds an A command to the end of the string. A D command in the answer string causes the call to fail.

Dependencies: The answer string is the last of four strings sent to the modem when the MAX answers a call. Therefore, the commands you enter can overwrite settings specified elsewhere. For example, if the AT Answer String setting includes a +MS command with a baud rate different from the rate specified by the MAX Baud parameter, the AT Answer String value overwrites the Max Baud value.

Make sure the string that you enter is correct. The MAX does not check the validity of the string.

Location: System>Sys Config

Auth Compat Mode

Description: Enables or disables Vendor Specific Attribute (VSA) compatibility mode when the MAX is using RADIUS for authentication and authorization purposes.

Auth Compat Mode specifies whether or not the MAX refers to a proprietary algorithm for encrypting and decrypting the User Password attribute. Unlike the RFC-defined algorithm, the proprietary algorithm does not null fill the password string to a multiple of 16 bytes before encryption. Also, when the password is longer than 16 bytes, the proprietary algorithm does not use the preceding segment's hash to calculate the next intermediate value.

Usage: Specify one of the following settings:

- **OLD**—Specifies that the MAX does not send the Vendor Specific attribute to the RADIUS server and does not recognize the Vendor Specific attribute if the server sends it. In this mode, the system uses a proprietary algorithm of encrypting and decrypting the User Password attribute.
- **Vendor Specific**—Specifies that the MAX uses the Vendor Specific attribute to encapsulate Ascend vendor attributes, and uses the RFC-defined User Password encryption algorithm as well.

Example:

Auth Compat Mode=OLD

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Id Max Retry Time; Keep User Name; No Attr. 6, Use Termsrv; Realm Delimiters; Sess Timer

Auth Id Max Retry Time

Description: Specifies the maximum amount of time, in seconds, that the MAX will spend as it attempts to contact any RADIUS server when it authenticates ID.

Usage: Specify a numeric value from 0 to 60. The default is 0, which specifies that the MAX is set to use its internal default value.

Example:

Auth Id Max Retry Time=60

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Compat Mode; Keep User Name; No Attr. 6, Use Termsrv; Realm Delimiters; Sess Timer

Cold start

Description: Specifies whether the system generates a trap when the MAX reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

Usage: Specify Yes or No. The default is Yes.

Example:

Cold start=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SeeAlso: Warm start

Console

Description: Specifies whether the system generates a trap when the console has changed state.

Usage: Specify Yes or No. The default is Yes.

Example:

Console=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Detect End of Packet

Description: Specifies whether the MAX buffers incoming data from TCP-Clear dial-in sessions that do not require V.120 processing.

Usage: Specify Yes or No. The default is No.

- Yes—After authenticating the session, the MAX unit begins buffering incoming WAN data. The MAX unit continues buffering data until it receives the specified End Of Packet Pattern, until it reaches the timeout specified by Flush Time, or until the data reaches the maximum packet length specified by Flush-Length, whichever occurs first.
- No—The MAX unit does not buffer incoming data from a TCP-Clear dial-in session.

Example:

Detect End of Packet=No

Location: Ethernet>Answer>TCP Clear options

Dirdo

Description: Specifies whether the system generates a trap when it receives a T-Online call without having received an answer or subaddress.

Usage: Specify Yes or No. Yes is the default.

Example:

Dirdo=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

EchoSuppressToneDisable

Description: Enables Echo suppressor tone. The MAX generates the tone at the beginning of a call.

Usage: Specify one of the following values:

Example:

EchoSuppressToneDisable=No

Location: System>Sys Config

Event overwrite

Description: Specifies whether the system generates a trap when a new event has overwritten an unread event. This trap is sent only for systems that support the Ascend accounting MIB. Once the trap has been sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events has occurred.

Usage: Specify Yes or No. The default is Yes.

Example:

Event overwrite=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SeeAlso: Radius change

FR link down

Description: Specifies whether a trap is sent whenever a DLCI ends.

Usage: Specify Yes or No. The default is Yes.

- Yes—Specifies that a trap is sent whenever a DLCI is brought down.
- No—Specifies that a trap is not sent whenever a DLCI is brought down.

Example:

FR link down=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SeeAlso: FR link up

FR link up

Description: Specifies whether a trap is sent whenever a DLCI is initiated.

Usage: You can specify Yes or No. The default is Yes.

Example:

FR link up=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SeeAlso: FR link down

Framed Only

Description: Specifies whether an incoming call must use a framed protocol.

Usage: Specify Yes or No. The default is No.

Example:

Framed Only=No

Location: Ethernet>Answer

Keep User Name

Description: Specifies User Name attribute handling.

Usage: Specify one of the following settings

- Change Name—The name provided by the server is used for the status display and for RADIUS accounting purposes.
- Keep Name—The MAX does not use the User Name value returned by the server. If a name has been specified (that is, if CLID or DNIS authentication is not used), the system uses that name. Otherwise, it uses the name sent to the server for authentication.
- Keep Realm Name—If the user name sent to the server for authentication is in a realm (for example, if it contains one of the characters @\%), the system behaves as if Keep User Name were set to Keep Name. Otherwise, the system behaves as if Change Name were specified.

Example:

Keep User Name=Change Name

Dependencies: A user authenticated by CLID or DNIS will appear to have the CLID or DNIS number as his or her username. If this condition is a problem, set Auth Keep User Name to Keep Realm Name.

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Compat Mode; Auth Id Max Retry Time; No Attr. 6, Use Termsrv; Realm Delimiters; Sess Timer

Lan Modem

Description: Specifies whether the system generates a trap when a digital modem is moved to the suspect list.

Usage: Specify Yes or No. The default is Yes.

Example:

Lan modem=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Link Down

Description: Specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.

Usage: Specify Yes or No. The default is Yes.

Example:

Link Down=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Link Up

Description: Specifies whether the system generates a trap when the communication link between the unit and the SNMP manager is reestablished.

Usage: Specify Yes or No. The default is Yes.

Example:

Link Up=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Max Dial Out Time

Description: Specifies the maximum number of seconds the MAX unit waits for a Call Setup Complete message from the remote side when dialing out.

Usage: Specify an integer from 0 to 255. The default is 20 seconds. If you set Max Dialout Time to 0 (zero), the unit uses its internal default of 20 seconds.

Example:

MAX Dialout Time=30

Dependencies: The Max Dialout Time setting does not influence the modem time out to detect carrier. Modems have an internal timer that counts down from dial out to establishing carrier with the remote modem (including training). For Conexant modems the internal timer has a default setting of 45 seconds.

Location: System>Sys Config

Modem:Call by Call

Description: Enables users that to select the call by call service options for outbound voice calls. These settings are required by NI-2 specifications.

Usage: Specify a number from 0 to 31, corresponding to the type of Call-By-Call service in use. The default is 0 (zero), which disables Call-By-Call service.

AT&T provides the following Call-By-Call services:

- 0—Disable Call-By-Call service
- 1—ISDN, including GSDN
- 2—Megacom 800
- 3—Megacom
- 6—ACCUNET Switched Digital Services
- 7—Long Distance Service, including AT&T World Connect
- 8—International 800-I800
- 16—AT&T MultiQuest

Sprint provides the following VPN and GVPN Call-By-Call services:

- 0—Reserved
- 1—Private
- 2—Inwatts
- 3—Outwatts
- 4—FX
- 5—Tie Trunk

MCI provides the following Call-By-Call services:

- 1—VNET/Vision
- 2—800
- 3—PRISM1, PRISM II, WATS
- 4—900
- 5—DAL

Dependencies: Modem:Call-by-Call applies only to calls placed by the digital modems in the MAX.

Example:

Modem:Call-by-Call

Location: System>Sys Config

Multicast monitor

Description: Specifies whether the system generates a trap when multicast heartbeat monitoring is configured and the system did not receive the specified number of heartbeat packets on a multicast interface.

Usage: Specify Yes or No. The default is Yes.

Example:

Multicast monitor=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

NoAttr. 6, Use Termsrv

Description: Specifies how the system behaves when it does not receive RADIUS Attribute 6 (User-Service).

Usage: Specify Yes or No. The default is Yes.

- Yes—The MAX initiates a terminal-server login if Attribute 6 is not received, regardless of whether Attribute 7 is received or not.
- No—If Attribute 6 is not received, but Attribute 7 is received, the unit initiates a framed-protocol login. It initiates a terminal-server login if neither Attribute 6 nor 7 is received.

Example:

NoAttr. 6, Use Termsrv=Yes

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Compat Mode, Auth Id Max Retry Time, Keep User Name, Realm Delimiters, Sess Timer

Overlap Receiving

Description: Enables or disables overlap receiving for incoming calls on the PRI line. Overlap receiving affects the procedure of establishing an incoming call received on a T1 or E1 PRI line on the unit. When using overlap receiving, the unit can use a series of information messages to gather the complete called-number from the network switch, enabling the use of features such as called-number authentication.

The Q.931 specification permits either en-bloc receiving or overlap receiving for an incoming call. With en-bloc receiving, the Setup message received from the network switch must contain all information required to process the call. With overlap receiving, the Setup message may contain incomplete called-number information, with the remainder (if any) sent in one or more additional Information messages after the network switch receives a Setup Acknowledge message from the called unit.

Usage: Specify Yes or No. The default is No.

Example:

Overlap Receiving=Yes

Dependencies: Overlap Receiving is N/A if Sig Mode is not configured as ISDN for T1, ISDN_NFRAS for T1, or ISDN for E1.

Location: Net/T1>Line Config>*any Net/T1 line*>Line 1

Perm Conn Update

Description: Specifies under what circumstances the MAX performs nonintrusive remote updates of the configurations of permanent connections.

Usage: Specify one of the following values:

- All (the default)—Specifies that the MAX will reestablish all existing permanent connections if they are fetched from the RADIUS server after the update. This setting causes service interruption every time the MAX updates or adds a nailed profile.
- Changed—Specifies that the MAX reestablishes only changed permanent connections.

Example:

Perm Conn Update=All

Location: System>Sys Config

Precedence

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. When TOS is enabled, you can set those bits (most significant bit first) to one of the following values:

- 000—Normal priority (the default).
- 001—Priority level 1.
- 010—Priority level 2.
- 011—Priority level 3.
- 100—Priority level 4.
- 101—Priority level 5.
- 110—Priority level 6.
- 111—Priority level 7 (the highest priority).

Example:

Precedence=001

Dependencies: If TOS Enabled=No, the Precedence setting is not applicable.

Location: Ethernet>Connections>*any Connection profile*>IP options

SeeAlso: Apply To, Precedence, TOS, TOS Enabled, TOS Filter

Radius change

Description: Specifies whether the system generates a trap when a new RADIUS server is being accessed. The trap returns the objectID and IP address of the new server.

Usage: Specify Yes or No. The default is Yes.

Example:

Radius change=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Realm Delimiters

Description: Specifies the characters that delimit a realm from the username.

Usage: Specify up to seven characters in any order. The default is N/A (not applicable). If you do not specify any characters, the system behaves as though Keep User Name is set to Change Name.

Example:

Realm Delimiters=1234567

Dependencies: The Realm Delimiters setting does not apply unless Keep User Name is set to Keep Realm Name.

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Compat Mode; Auth Id Max Retry Time; Keep User Name; No Attr. 6, Use Termsrv; Sess Timer

RIP Trigger

Description: Specifies whether the IP router or Virtual Router (VRouter) tags routes that have been updated in the routing table and sends updates that include only the changed routes.

Usage: Specify Yes or No. The default is Yes.

- Yes—The router tags changes to its routing table and includes only the tagged routes in its next update. Changes occur when a call arrives or disconnects, RIP or OSPF learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates 5 to 8 seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions. The result is reduced processing overhead for the router and its neighbors.
- No—The router sends full table updates every 20 to 40 seconds. To prevent RIP routers on a network from synchronizing and sending large updates in unison, the current software version does not broadcast the full table update at fixed 30-second intervals.

Example:

RIP trigger=No

Location: Ethernet>Mod Config>TServ options

Select CLID

Description: Specifies how the MAX applies CLID authentication to incoming calls.

Usage: Specify one of the following values:

- **First**—Select the first CLID received from the PSTN and attempt to match it to the Answer profile. The CLID can be either network provided or user provided.
- **Secure Prefer**—Select a secure CLID and attempt to match it to the Answer profile. If no secure CLID is found, an unsecure CLID, if present, will be chosen.
- **Secure Require**—Select a secure CLID, if present, and attempt to match it to the Answer profile. If no secure CLID is found, the MAX will behave as if no CLID is present.
- **User Prefer**—Select a user-provided CLID, if present, and attempt to match it to the Answer profile. If not found, the MAX chooses an available network CLID.
- **User Require**—Selects a user-provided CLID, if present, and attempt to match it to the Answer profile. If not found, the system will behave as if no CLID is present.

Example:

Select CLID=First

Location: Ethernet>Answer

Sess Timer

Description: Specifies the interval, in seconds, at which the MAX unit sends the number of sessions per Class attribute to the accounting server.

Usage: Specify a numeric value from 0 to 65535. The default is 0, which specifies that the unit does not send the number of sessions per Class attribute to the accounting server.

Example:

Session Timer=60

Location: Ethernet>Mod Config>Auth

SeeAlso: Auth Compat Mode; Auth Id Max Retry Time; Keep User Name; No Attr. 6, Use Termsrv; Realm Delimiters

SNMP authentication

Description: Specifies whether the system generates a trap when an authentication failure occurs.

Usage: Specify Yes or No. The default is Yes.

Example:

Authentication=Yes

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SourceIP Check

Description: Enables or disables antispoofing for the session. The source IP address in each packet must match the far-end remote address or the address agreed upon in IPCP negotiation. The far-end remote address can be that of a single host or that of a network. If the addresses do not match, the system discards the packet.

Description:

Usage: Specify Yes or No. The default is No.

Example:

SourceIP Check = Yes

Location: Ethernet>Connections>*any Connection profile*>IP options

SeeAlso: Apply To, Precedence, TOS, TOS Enabled, TOS Filter

Suppress Host Routes

Description: Specifies whether the MAX unit suppresses advertising of host routes in each update. Advertising the routes can cause excessive routing overhead.

Usage: Specify Yes or No. The default is No.

- Yes—Specifies that host routes are suppressed.
- No—Specifies that host routes are advertised.

Dependencies: If you set Suppress Host Routes to Yes, routes are suppressed according to the following rules:

- If a Connection profile specifies a Remote Address setting with a subnet mask of less than 32 bits, host routes for the interface are suppressed while the MAX negotiates a session. After the MAX establishes a session, it advertises only network routes for the interface.
- If a Connection profile specifies a Remote Address setting with a subnet mask of /32, the MAX does not suppress host routes for the interface.

Location: Ethernet>Mod Config>Accounting

SeeAlso: Acct Compat Mode, Acct Checkpoint, Acct Max Retry, Acct-ID Base, Allow Stop Only

Telnet password

Description: Specifies whether all failed Telnet login attempts generate a trap.

Usage: Specify Yes or No. The default is Yes.

Example:

Telnet password=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

TOS

Description: Specifies the type of service for the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits indicating precedence for priority queuing. The next four bits of the TOS byte are used to choose a link on the basis of the type of service. When TOS is enabled, you can set one of the following values in the packet:

- Normal (the default)—Specifies that the MAX unit applies normal TOS service. Normal is the default.
- Cost—The unit minimizes monetary cost.
- Reliability—The unit maximizes reliability.
- Throughput—The unit maximizes throughput.
- Latency—The unit minimizes delay.

Example:

TOS=Normal

Dependencies: If TOS Enabled=No, the TOS setting is not applicable.

Location: Ethernet>Connections>*any Connection profile*>IP options

SeeAlso: Apply To, Precedence, Source IP Check, TOS Enabled, TOS Filter

TOS Enabled

Description: Specifies whether type of service filters are enabled for each connection.

Usage: Specify Yes or No. The default is No.

- Yes—Type of service is active for this connection.
- No—Disables type of service for this connection.

Example:

TOS Enabled=Yes

Location: Ethernet>Connections>*any Connection profile*>IP options

SeeAlso: Apply To, Precedence, Source IP Check, TOS, TOS Filter

TOS Filter

Description: Specifies Type of Service (TOS) policy. In a Connection profile that has both its own local policy and an enabled TOS filter, the policy defined in the TOS filter takes precedence. Applying a TOS filter to a TOS connection enables administrators to define one priority setting for incoming packets on the connection and another for incoming packets addressed to a particular destination (the destination in a TOS filter).

Usage: Specify a number from 0 to 99999. The default is 0.

Example:

TOS Filter=12345

Dependencies: Keep in mind the following additional information:

- If TOS Enabled=No, the TOS setting is not applicable.
- The TOS Filter setting applies the data stream(s) specified by the Apply To parameter. For example, if Apply To=Incoming, the TOS filter setting applies only to the incoming data stream.

Location: Ethernet>Connections>*any Connection profile*>IP options

SeeAlso: Apply To, Precedence, Source IP Check, TOS, TOS Enabled

Use exceeded

Description: Specifies whether the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it or when the system DS0 usage has been exceeded.

Usage: Specify Yes or No. The default is Yes.

Example:

Use exceeded=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

Use TACACS+

Description: Specifies how the MAX unit interacts as a client of TACACS+ authentication servers.

Usage: Specify one of the following values:

- Yes—The MAX unit contacts the TACACS+ server to complete authentication.
- No—The unit does not contact the TACACS+ server to complete authentication.

Example:

Use TACACS+=Yes

Dependencies: Keep in mind the following additional information:

- If TACACS+ is not the specified authentication method for the MAX, then Use TACACS+=N/A.
- Do not name a Security profile with a name already assigned to a Connection profile.

Location: System>Security>*any Security profile*

Warm start

Description: Specifies whether the system generates a trap when the MAX reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.

Usage: Specify Yes or No. The default is Yes.

Example:

Warm start=No

Location: Ethernet>SNMP Traps>*any SNMP trap profile*>Enable traps

SeeAlso: Cold start

Problems Corrected in previous TAOS 7.0 releases

A variety of corrections have been included since the TAOS 7.0 release. Table 0-1 summarizes the TR number, the TAOS 7.0 release in which the problem was corrected, and a summary of the problem corrected:

Table 0-1. Summary of Problems corrected:

TR	Problem corrected	Release
TR 2660	Dial in V.110 client could connect to PPTP server behind a MAX unit.	7.0.3
TR 2879	In a MAX unit's terminal-server menu mode, unavailable selections could be chosen.	7.0.22
TR 2987	A MAX unit showed V.110 modems available to process V.110 calls when it did not have V.110 modems available.	7.0.26
TR 3163	A MAX unit did not process a finger request from FreeBSD when the tcp option was selected.	7.0.3
TR 3425	Some of a MAX unit's BRI channels froze during outdial.	7.0.3
TR 3556	A MAX unit sent Normal Link Down traps.	7.0.3
TR 3659	A MAX 200Plus unit did not complete a Zmodem transfer.	7.0.3
TR 3685	In the 50-700 Status Menu, a Max unit showed the Enet I/F: AUI when it is plugged into a UTP connection.	7.0.3
TR 3693	A MAX 4000 was unable to complete call-by-call terminal server calls.	7.0.3
TR 3725	The Ascend Maximum Time attribute did not take affect for CBCP sessions.	7.0.3
TR 3766	During a CBCP session, Ascend-Xmit-Rate and Ascend-Data-Rate were reported as zero.	7.0.3
TR 3772	A MAX unit did not establish more than one nailed connection.	7.0.3
TR 3784	A MAX-stacked unit failed with CLID authenticated MP calls.	7.0.3

Previous TAOS 7.0 releases*Problems Corrected in previous TAOS 7.0 releases*

TR	Problem corrected	Release
TR 3828	A MAX unit managed by SNMP did not disable a specified modem.	7.0.26
TR 3838	A MAX unit did not properly route incoming calls through PBX-T1 conversion when <code>pbx_type=data</code> and <code>answer_service=none</code> .	7.0.3
TR 3844	An Appletalk-enabled MAX unit issued Warning 175.	7.0.22
TR 3845	A MAX unit did not send a busy signal when a modem dialed a busy line.	7.0.3
TR 3848	A MAX unit did not drop the second channel when ALU dropped below Idle PCT threshold.	7.0.3
TR 3928	During a telnet session to a Max unit, the Edit window displayed the Ethernet profile.	7.0.3
TR 3935	A MAX unit with two PRIs handling analog and IP calls reset with Fatal Error 1.	7.0.3
TR 3940	Telnet users could not connect to a MAX unit when telnetting to a broadcast IP address by way of a WAN line.	7.0.26
TR 3966	A MAX unit using the control port would reset without generating a Fatal Error.	7.0.3
TR 3975	A MAX unit did not send Cause Code 17 to Net/BRI line.	7.0.3
TR 4034	A MAX unit configured to do Pool Summary marked MP/MPP calls as non-private.	7.0.3
TR 4040	A MAX unit reset with Fatal Error1 when an encrypted tunnel password was sent through RADUIS.	7.0.3
TR 4044	A MAX unit did not recognize break signals.	7.0.3
TR 4061	MAX unit did not adhere to MP+ thresholds when a call failed.	7.0.3
TR 4096	A MAX unit had a tload with checksum errors and the unit failed to restart.	7.0.3
TR 4150	A MAX 6000 eliminated a UDP listening port for Radius Server when the user disabled CallLogging parameter.	7.0.22
TR 4169	A MAX 4000 unit reset with Fatal Error 29.	7.0.3
TR 4191	A MAX unit reset without Fatal Error during SCM and ftp.	7.0.3

TR	Problem corrected	Release
TR 4197	MAX 2000 system software did not include support for OSPF.	7.0.3
TR 4210	MAX unit sent ATMP RIP when ATMP RIP=Off for Home Agent (HA).	7.0.28
TR 4214	A MAX unit did not use free modems.	7.0.26
TR 4303	Direct SecureID authentication was not supported, and dial-in users to a MAX unit received a Remote Authentication Timeout message.	7.0.28
TR 4323	A MAX unit did not complete a CLID-authenticated, RADIUS connection to a PIAFS terminal.	7.0.26
TR 4325	A MAX unit exhibited a lag between modem call disconnect and No Carrier message at the calling modem.	7.0.3
TR 4390	After several hours, a MAX unit supporting permanent ISDN connectivity stopped working.	7.0.28
TR 4417	When a Windows user entered an incorrect ID or Password during CHAP authentication, they did not receive an authentication failure message.	7.0.26
TR 4508	A voice call failed when a MAX unit placed two simultaneous outgoing voice calls on a T1 or T1-PBX line.	7.0.26
TR 4514	A MAX 800 unit installed with PCMCIA modems could not support multiple channel MP or MP+ calls.	7.0.26
TR 4556	IPX header compression caused dialup Windows clients to crash or reset.	7.0.26
TR 4569	A MAX unit with RADIUS accounting enabled occasionally reported records with an incorrect session ID.	7.0.28
TR 4615	A MAX unit configured to support PRI ISDN reset with Fatal Error 1.	7.0.22
TR 4616	A MAX unit configured to support X.25 reset with an Fatal Error 29.	7.0.28
TR 4679	A MAX unit reset occasionally with Fatal Error 8 when PPTP was used from PIAFS terminal.	7.0.28
TR 4694	A MAX 6000 unit occasionally reset, generating a Warning 179.	7.0.26
TR 4757	A Max unit sent Navis Access logging transmissions to radius accounting.	7.0.22

Previous TAOS 7.0 releases*Problems Corrected in previous TAOS 7.0 releases*

TR	Problem corrected	Release
TR 4764	A MAX unit that used its permanent ISDN connection to continuously place outgoing calls exhibited memory leaks.	7.0.22
TR 4867	In diagnostic mode, a MAX unit generated IPX protection violation errors.	7.0.26
TR 4868	MAX unit supporting OSPF reset issuing a Warnings 175, 200, and 201.	7.0.22
TR 4888	A system software upgrade corrupted a MAX unit's L2TP configuration.	7.0.26
TR 4905	A MAX unit reset with Fatal Error 1 after issuing a Warning 179.	7.0.22
TR 4926	A MAX unit incorrectly reported Ascend-Num-In-Multilink as zero (0) whenever a session timed out.	7.0.26
TR 5055	A user could not ping a MAX unit when their connection was authenticated through a RADIUS server configured to include the Ascend-PPP-Address attribute.	7.0.26
TR 5075	A stacked-Max unit displayed incorrect Show User's information.	7.0.26
TR 5181	RADIUS accounting was not working when Auth-Type was set to RADIUS/LOGOUT.	7.0.28
TR 250228	A MAX unit had only one value for Call Back with v.110 attribute.	7.0.3
TR 250296	A MAX unit sent SETUP for B-Channel before release was sent for that same B-Channel.	7.0.3
TR 250298	TCP host and dial-in MAX units reported inauthentic values for accounting attributes Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets.	7.0.26
TR 258589	A MAX unit used incorrect Dialing Number and Dialed Number on PPTP.	7.0.3
TR 258608	Data call from a Multiband VSX to a MAX Host/Dual call was cleared with ISDN code 16.	7.0.28
TR 258639	A MAX unit generated an Error 101 when it initiated a CLID authenticated connection to a Pipeline unit.	7.0.26
TR 258640	A MAX unit did not complete a transfer between a modem client and an X.25 host.	7.0.26

TR	Problem corrected	Release
TR 258646	L2TP and AAC authentication failed when a MAX unit used single RADIUS server.	7.0.22
TR 258648	A MAX unit's Overlap Receiving, PRI Prefix, Trailing Digits, and T302 Timer parameters were not included in the unit's system software load.	7.0.26
TR 258656	A MAX unit did not respond to Appletalk ARP packets that were greater than 28 bytes.	7.0.3
TR 258672	A MAX unit's backup PVC did not come up.	7.0.3
TR 258676	Clock slips on a MAX unit connected to DPNSS/DASS 2 lines caused dialin users to experience poor performance and continuous modem retrainings.	7.0.3
TR 258680	Fatal Error 1 was sent every hour on a MAX unit.	7.0.3
TR 258688	E1 channel 16 on a MAX 6000 could not be nailed when Signalling was set to None.	7.0.3
TR 258692	A MAX unit exhibited inconsistent x.75 behavior when v.42bis compression was used.	7.0.3
TR 258694	Data sent from a POS terminal was lost when a MAX unit did not buffer the 100 bytes.	7.0.3
TR 258701	ISDN overlap received numbers that were not in DNIS.	7.0.3
TR 258722	On a MAX unit, avm command showed modems dropping off.	7.0.3
TR 258725	MP/MPP calls failed authentication in a MAX-stacked environment.	7.0.3
TR 258728	A MAX unit would hang after several hours of running x.25 PAD calls.	7.0.3
TR 258730	A reset with Fatal Error 1 was exhibited when two Immediate Telnet sessions used DNIS authentication.	7.0.3
TR 258738	During call setup, a MAX unit did not allow for network-provided CLID authentication.	7.0.28
TR 258748	Multipath external OSPF routes were not deleted from a MAX unit's routing table.	7.0.3
TR 258756	A MAX unit failed to maintain a FTP connection when it used Firewall and NAT on the same dialout profile.	7.0.26
TR 258766	After sustained usage, a MAX unit stopped creating PPTP tunnels.	7.0.26

Previous TAOS 7.0 releases*Problems Corrected in previous TAOS 7.0 releases*

TR	Problem corrected	Release
TR 258770	RADIUS filtering was not applied to a MAX unit after a CLID-authenticated callback.	7.0.28
TR 258772	SourceIP Check did not work on some spoofed packets.	7.0.26
TR 258776	A MAX unit reset as it created a point-to-point tunnel, generating a Fatal Error 29.	7.0.26
TR 258787	On a Max 200Plus unit, the Filter-ID setting did not function.	7.0.26
TR 258791	Without referring to a secondary home agent, a MAX unit terminated a tunnel registration process when a primary home agent was unavailable.	7.0.26
TR 258813	A MAX 4000 unit listed unused, available modems as busy.	7.0.26
TR 258821	While functioning as a Home Agent, a MAX unit generated, and did not clear, unused ATMP tunnels.	7.0.22
TR 258836	A MAX unit issued Warning 104, FE 29 and then reset.	7.0.26
TR 258878	When a user selected X.32 Encapsulation in the Encaps Options subprofile, a MAX unit did not provide a Password parameter.	7.0.26
TR 1000032	A MAX unit set MRRU equal to MRU and then dropped ATMP packets.	7.0.3
TR 1000085	A MAX unit's modem code would be corrupted, causing calls to fail.	7.0.3
TR 1000094	A MAX unit configured as an ATMP HA running IPX did not work.	7.0.3
TR 1000096	R2 signaling on a MAX unit did not support a B-5 tone.	7.0.3
TR 1000105	IPX network traffic was incorrectly received and stored in the Max unit's routing table from permanent virtual circuits when Route IPX = No.	7.0.26
TR 1000112	A MAX unit's MP connections failed.	7.0.3
TR 1000114	An attempt to disable either Net 5 and Australia PRA on a MAX unit disabled the other.	7.0.3
TR 1000115	In an MP Connection profile, Base Ch Count was incorrectly read as Max Ch Count for received MP calls.	7.0.1
TR 1000120	x.25 PVC and SVC could not be configured on a MAX unit.	7.0.3

Previous TAOS 7.0 releases
Problems Corrected in previous TAOS 7.0 releases

TR	Problem corrected	Release
TR 1000126	A MAX generated an Fatal Error 106 when both SNMP and ATMP were active.	7.0.1
TR 1000137	A MAX E1 unit did not conform to ITU-T R2 protocol standards for timeout.	7.0.3
TR 1000139	A MAX unit's ifAdminStatus object was not recognized.	7.0.3
TR 1000140	Called Number and Calling Number were displayed as N/A though an active connection profile included X.25/PAD encapsulation.	7.0.3
TR 1000145	A MAX unit in a high data-traffic, ISDN and R2 outdial environment issued Fatal Error 17 and Warning 179.	7.0.22
TR 1000146	R2 outdial failed on a MAX unit.	7.0.3
TR 1000150	A MAX unit issued Warning 561 and Fatal Error 18 then reset.	7.0.22
TR 1000165	A MAX unit generated Fatal Error 1 during heavy modem outdial.	7.0.3
TR 1000186	A MAX E1 unit displayed a Red Alarm LED.	7.0.22
TR 1000192	A MAX E1/R2 unit's CLID response was incorrectly handled.	7.0.22
TR 1000211	A MAX accepted and processed calls on E1 ports that the user had set to be disabled.	7.0.26
TR 1000223	A MAX unit configured to support E1/PRICalls failed to process Interface ID information in SETUP message sent from a switch.	7.0.28
TR 1000243	A MAX unit in a stacked environment reset with an Fatal Error 8.	7.0.28
TR 1000256	A MAX unit reset when configured as an ATMP Foreign Agent, generating a Fatal Error 38.	7.0.28
TR 6000082	Truncated TCP packets lead a MAX unit to infrequently reset with an Fatal Error 38.	7.0.28

Previous TAOS 7.0 releases

Problems Corrected in previous TAOS 7.0 releases
