Lucent Technologies
Bell Labs Innovations



MAX™ 6000 TAOS 10.1

Release Note

March, 2003

Copyright © 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

CE 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 and Broadband 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.

Lucent Technologies

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 iii

Section 1 Upgrading and Downgrading 1-1

External PCMCIA DRAM card 1-1
Enabling Field Service and Operations parameters 1-2
Keeping the same software binary name 1-2
Using TFTP to upgrade or downgrade 1-3
- Creating redundant backup images for a MAX 6000 unit 1-3
- Using TFTP to upgrade a MAX 6000 1-4
- Using TFTP to upgrade a MAX 6000 for MultiVoice® binaries 1-5
- Using TFTP to downgrade 1-7

Using the serial port to upgrade or downgrade 1-7
- Saving the current system configuration 1-8
- Upgrading system software 1-9
- Restoring the configuration 1-9
- Downgrading the software 1-10
- Restoring passwords 1-10

Section 2 About this release 2-1

Features in TAOS 10.1 2-1
Licensing for Premium Feature Set 2-2
Feature Identification Numbers 2-2
Firmware in TAOS 10.1 2-3
- Firmware versions for digital modem cards 2-3
- Firmware versions for MultiDSP slot cards 2-3

Overview of slot card support in this release 2-3

Section 3 Features in TAOS 10.1 3-1

Disabling end-point discriminator negotiation in establishing PPP sessions 3-1
IP-in-IP tunneling support 3-2
- IP-in-IP encapsulation 3-2
  - Settings in a connection profile 3-2
  - Settings in a RADIUS profile 3-2
  - Sample IP-in-IP connection 3-3

Session idle timer enhancements for layer 2 tunneling 3-4
Specifying whether to log L2TP `syslog` messages 3-4
Configurable L2TP hello packet policy 3-4
- New `Hello Policy` parameter 3-5
- Sample configuration 3-5

Physical channel ID (38) in incoming call request 3-5
Q.931 Cause Code (12) with Call-Disconnect-Notify 3-6
DSCP marking and remarking for L2TP 3-6
DSCP marking and remarking for tunneling protocols 3-6
Command-line interface settings for DSCP marking and remarking for L2TP .. 3-7
RADIUS interface changes: 3-7
ToS byte copying 3-8
ToS byte copying 3-8
New `TOS Copying` parameter 3-8
New RADIUS `Ascend-TOS-Copying (266)` attribute 3-8
Multicast support extended to all vrouters 3-9
New Multicast menu 3-9
Displaying information about VRouters 3-11
V.92 PCM upstream 3-12
Enabling V.92 PCMU 3-12
MultiVoice: CLI indicator enhancement 3-13
Configuring frames per packet for each codec 3-14
E1 R1/R2 group II and group b cause codes 3-16
R2 to ISDN 3-17
ISDN to R2 3-18
R2 to CAS 3-18
CAS to R2 3-19
MultiVoice: Enabling DTMF tone passing, QoS, and adaptive-jitter-buffer for G.723.1 and G.728 codecs 3-20
RFC2833 for DTMF-tone-passing 3-21
Quality of Service (QoS) statistics 3-21
Adaptive Jitter Buffer 3-21
MultiVoice: Special trunk group for hairpin call 3-21
Silence suppression and adaptive jitter buffer 3-22
MIB `hashcode.mib` now supported 3-22
Support for alarm MIBs 3-25
Supported alarm MIBs 3-25
MIB tables 3-26
Specifying the maximum number of alarms in `alarmClearTable` 3-26
Clearing alarms from the `alarmActiveTable` and `alarmClearedTable` ... 3-27
Deleting an alarm model table 3-27
MIB traps 3-27
TAOS modifications to the alarm MIBs 3-27
Supported alarms 3-28
Configuring Link Control and Network Control Protocol timeout values 3-30
Support for PPP Extensible Authentication Protocol (EAP) 3-31

Section 4 Change requests in TAOS 10.1 4-1

Section 5 Notices and Known Issues 5-1

Notice of end of sale for MAX 6000 units 5-1
Product Codes Impacted 5-1
Replacement products 5-3
Notice of TAOS license and upgrade changes 5-3
Price change for base TAOS software 5-3
Price change for upgrades and maintenance to TAOS 10.0 software 5-3

Distribution change for TAOS 10.0 software 5-4
TAOS software license agreement change 5-4
Support for voice DSP modules ends 5-4
Data and RAS known issues 5-4
MultiVoice® known issues 5-6

Appendix A Document Set A-1

Upgrading and Downgrading

1

External PCMCIA DRAM card 1-1

Enabling Field Service and Operations parameters 1-2

Keeping the same software binary name 1-2

Using TFTP to upgrade or downgrade 1-3

Using the serial port to upgrade or downgrade 1-7



Caution When you upgrade a MAX 6000 unit's version of the True Access™ Operating System (TAOS), the newer version might use a configuration file format that is incompatible with the version that preceded it. The upgrade process automatically converts the unit's configuration file to the newer format. You need a backup copy of the configuration file created using the older format in case it ever becomes necessary to revert back to a previous version of TAOS (for example, 8.0.3). If you fail to create and save a backup copy of the configuration before you change the unit's version of TAOS, you might lose all configuration information.



Caution The standard software binaries you use to upgrade to True Access™ Operating System (TAOS) 9.1 require additional flash memory available to the MAX 6000 unit only by means of an external PCMCIA flash card. The MAX 6000 unit requires a Lucent-approved external PCMCIA card.



Caution If possible, change a MAX 6000 unit's version of TAOS by using TFTP. Refer to "Using TFTP to upgrade or downgrade" on page 1-3 for further details.

As you prepare to change the system software on a MAX 6000 unit, you must verify that the Field Service and Operations parameters are enabled on the unit.

External PCMCIA DRAM card

The standard software binaries you use to upgrade to True Access™ Operating System (TAOS) 10.1 require additional Dynamic RAM (DRAM) memory available to the MAX 6000 unit only by means of an external PCMCIA DRAM card. The MAX 6000 unit requires the following Lucent external PCMCIA card: MX60-DRAM-32MB 300560083

Table 1-1 lists models of MAX 6000 units that are *pre-installed* with the DRAM necessary to upgrade to 10.1 (and do *not* need the installation of MA60-DRAM-32MB):

Table 1-1. MAX 6000 unit product codes impacted by this notice

Product code	Comcode	Description
MX60-4E1-32-AC	300271566	MAX 6000 E1 with (1) AC power supply and 32MB DRAM card
MX60-4E1-32-DC	300271574	MAX 6000 E1 with (1) DC power supply and 32MB DRAM card
MX60-4T1-32-AC	300271590	MAX 6000 T1 with (1) AC power supply and 32MB DRAM card
MX60-4T1-32-DC	300271582	MAX 6000 T1 with (1) DC power supply and 32MB DRAM card

Enabling Field Service and Operations parameters

The `Field Service` parameter in the `Security` profile enables or disables permission to perform Lucent-specific field service operations, such as changing the operating system software on a MAX 6000 unit. The `Field Service` parameter is not applicable if the Operations parameter, also in the Security profile, is set to `No`. Before you begin the process of changing the unit's version of TAOS, ensure that the security profile you use as an administrator is configured to support `Field Service` and `Operations`.

For example, the following `Full Access` security profile of a MAX 6000 unit is correctly configured to support a change of operating system software:

```
00-300 Security
 00-303 Full Access
 >Name=Full Access
  Passwd=*SECURE*
  Operations=Yes
  Edit Security=Yes
  Edit System=Yes
  Field Service=Yes
```

Keeping the same software binary name

If possible, you should always keep the same software binary name when you upgrade or downgrade. For example, the MultiVoice® binary for TAOS 9.0.2 is called `tbiv.bin`. To upgrade to release TAOS 10.1, continue to use `tbiv.bin` even though the contents have changed, unless you are upgrading with the MultiVoice® binary that supports VDSP cards. If you want to support voice DSP, the binary name before the prefix will end with the numeral 6 (for example, `tbiv6.m60`).

MAX 6000 units no longer supports AppleTalk and the binary file has changed.

If you install a different version, your unit might lose its configuration. If this happens, you might need to manually restore your configuration. There might 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.

Use TFTP to transfer a build intended for a different type of network interface. For example, your MAX 6000 unit might have a T1 interface. If you are attempting to transfer a build that is appropriate for an E1 interface, the MAX 6000 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 a 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 6000 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.

Using TFTP to upgrade or downgrade

TFTP is a more reliable way to obtain, store, and then change the version of TAOS than the alternative (that is, using the serial port to upgrade). If you use TFTP, you must use a MAX 6000 unit's external flash memory to upgrade the unit's version of TAOS.

Creating redundant backup images for a MAX 6000 unit

The PCMCIA flash memory card for a MAX 6000 unitnow supports two copies of TAOS code. If the first version of software code becomes corrupted, the MAX 6000 unit can boot up the second version.

To create the redundant backup image, proceed as follows:

The order of these two steps is not important, but the MAX 6000 unit will be unable to recover from a failure in the primary code image until they have both been executed. The migration to the backed up binary is transparent to the user and no action is required by you to effect the migration.

1 Create a backup copy of the currently running binary on the PCMCIA flash card by using the `fBackupImage` debug command, as follows:

```
> fBackupImage
Preparing for image copy...
This load contains an IOP part
Copying 1797281 bytes from PCMCIA flash to PCMCIA...
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Image copied to high PCMCIA flash successfully.
 >
```

2 Load the `lvs.m60` image into internal flash with the `tload -i` debug monitor command to support the backup image.

For example:

```
> tload -i <tftp-server> lvs.m60
saving config to flash
.........................................
.

loading code from 192.168.21.44
file lvs.m60...
.
.

tftp download complete. Verifying image...
Downloaded image is OK.
```

Using TFTP to upgrade a MAX 6000

Note The following upgrade steps assume you have not used the MultiVoice® binaries to upgrade to release TAOS 10.1. If you used the MultiVoice® binaries, you must downgrade to a previous TAOS release (see "Using TFTP to downgrade" on page 1-7) before proceeding with the upgrade steps in this section.

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 6000 unit's configuration.

To upgrade system software using TFTP:

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 want to upgrade.
- The builds of the system software version to which you want to upgrade.

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 current 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 previously-named configuration `config803.cfg` in the TFTP home directory of the server named `tftp-server`:

```
tsave -m tftp-server config803.cfg
```



Caution The MAX 6000 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 10.1. 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.

1 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 external flash from the machine named `tftp-server`.

2 Enter the following command immediately after executing the `tload` command to save your current configuration to internal flash memory so that it can be recovered after Step 6:

```
> fsave
```

Failure to perform this step might result in the loss of all previous configuration data (including the IP address) and you might not be able to access this MAX 6000 via telnet.

3 Enter the following command to clear NVRAM so that the configuration saved in internal flash in Step 5 is restored to NVRAM upon the next reset cycle:

```
> nvramclear
```

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

This completes the procedure for upgrading to TAOS 10.1.

Using TFTP to upgrade a MAX 6000 for MultiVoice® binaries



Note The MAX 6000 unit's software binary files that support MultiVoice® are too large to fit on the internal flash. To support the new features offered by this software binary file, you must have an external PCMCIA flash card installed in the unit to upgrade. The MAX 6000 requires a Lucent-approved external PCMCIA card.

To upgrade using TFTP, you must enter a few FAT flash filesystem commands in the correct sequence. If you do not enter them in the correct sequence, you could lose the MAX 6000 unit's configuration.

To upgrade system software by way of TFTP:

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 want to upgrade.

– The builds of the system software version to which you want to upgrade.

2 **From the unit's VT100 interface, press Ctrl-D to invoke the DO menu and select `D=Diagnostics`.**

3 **Ensure that a flash card is present in the PCMCIA slot and at the `>` prompt, format the external flash card:**

```
format -b
```



Caution Reformatting the external flash card deletes any voice announcements that are currently stored on the card. After completing the upgrade procedure, you will need to re-download your voice announcements. For more, see the documentation that came with your MAX 6000 unit.

4 **Use the `tsave -m` command to save your current 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 into the previously-named `config803.cfg` in the TFTP home directory of the server named `tftp-server`:**

```
tsave -m tftp-server config803.cfg
```



Caution The MAX 6000 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 10.1. 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.

5 **Load the standalone handler to the space reserved at the beginning of the external flash card. Enter the following command:**

```
tload -b tftp-server m60handler.bin
```

6 **Make a `/current` directory on the external flash card:**

```
mkdir /current
```

7 **With the `fload` command, load a binary into the `/current` directory:**

`fload tftp-server tbiv6.m60 /current/`*`tbiv`*`.bin`

where *`tbiv`* is an arbitrary name that must be followed by `.bin` and it must be placed in the `/current` directory. During reset, the first `*.bin` file the unit finds in the `/current` directory of the formatted external flash card will be run.

8 **Enter the following command immediately after executing the `fload` command to save your current configuration from NVRAM to internal flash memory so that it can be recovered after Step 9:**

`> fsave`

Failure to perform this step might result in the loss of all previous configuration data (including the IP address) and you might not be able to access this MAX 6000 via telnet.

9 **Enter the following command to clear NVRAM so that the configuration saved in internal flash in Step 8 is restored to NVRAM upon the next reset cycle:**

`> nvramclear`

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



Caution While the unit resets, it searches for the image on the external PCMCIA flash card. If available, the unit uses the image. Otherwise, if the image is not available (for example, the flash card is unplugged), then the image on the internal flash is used. If the image on the internal flash memory is an older version of TAOS (that is, previous to TAOS 10.1), your configuration might be corrupted.

This completes the procedure for upgrading to TAOS 10.1.

Using TFTP to downgrade

To downgrade system software using TFTP, you must follow the same basic steps as you did when you upgraded TAOS, with one exception.

1 **Instead of using the `fsave` command, as described in the previous upgrade procedures, 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 Config803
```

restores `Config803`, a configuration compatible with TAOS 8.0.3, from the unit named `tftp-server`.

Note The `-f` argument is necessary in this step. Failure to use the `-f` argument will cause `trestore` to place the configuration in binary format into NVRAM, rendering the configuration unusable to the MAX 6000 unit.

2 **On the MAX 6000 only, reformat the external flash card:**

```
format -e
```



Caution Reformatting the external flash card deletes the voice announcements that are currently stored on the card. After completing the upgrade procedure, you need to re-download your voice announcements. For more, see the documentation that came with your MAX 6000 unit.

3 **Refer to the upgrade procedures in the release note for the software version you are downgrading to.**

Using the serial port to upgrade or downgrade



Caution You can upgrade system software using the serial console only on a MAX 6000 unit, and doing so deletes all existing profiles. Save your current profile settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. For security reasons, password information is not stored in backup files. If you have many passwords, you should

consider using TFTP to upgrade your software. (See "Using TFTP to upgrade or downgrade" on page 1-3.)



Note Using the serial port to upgrade is no longer supported for MultiVoice® because the internal flash is not large enough to support the downloading of TAOS 10.1 MultiVoice® binaries.

Before upgrading your MAX 6000 through the serial port, make sure you have the following equipment, software, and configuration settings:

- An IBM compatible PC or Macintosh system with a serial port capable of connecting to the MAX 6000 unit's Console port.
- A straight-through serial cable.
- Data communications software for your system with appropriate communications software (for example, Procomm Plus, HyperTerminal for the PC, or ZTerm for the Macintosh). Verify that the line-width settings of the communications software are set to at least 80 characters.
- Verify that the `Term Rate` parameter, located in the `Sys Config` menu, specifies `57600`.
- Verify that the baud rate of your data communications software is set to the default value of `57600`.



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 6000 unit unusable.

Verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture the ASCII characters it receives to disk 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 `System > Sys Config`.

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

Saving the current system configuration

To save the MAX 6000 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 profile and examine the saved configuration file.**

Upgrading system software

To upgrade the software using the MAX 6000 unit's serial port:

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.

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 (for example, a single filter stored in a special configuration file).

1 **From the MAX 6000 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 to clear the configuration from the internal flash:**

```
> fclear
```

3 **At the `>` prompt, enter the `nvramclear` command:**

```
> nvramclear
```

This causes the system to reset. When it comes back up, continue 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...
```

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 10.1.

If you have any questions about how to send an ASCII file, consult the documentation for your communications program.

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

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

Press any key to return to the configuration menus.

8 **Reset the unit by selecting `System > Sys Diag > Sys Reset` and confirming the reset.**

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 6000 unit.**

Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your MAX 6000 unit. The time displayed on the screen does not represent real time. Ignore *bad batch* messages from your communication program. These are normal messages.

After the file transfer, the MAX 6000 unitresets. Upon completion of the self-test, the MAX 6000 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 FTP server and downgrade the software again. If you continue to have problems, contact Lucent Technologies technical support for assistance.

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 might 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.

About this release

2

Features in TAOS 10.1 2-1

Licensing for Premium Feature Set 2-2

Feature Identification Numbers 2-2

Firmware in TAOS 10.1 2-3

Overview of slot card support in this release 2-3

The True Access™ Operating System (TAOS) contains a foundation of built-in software features for WAN access environments, as well as optional extensions that require separate licensing to support a wide variety of WAN access environments.

The *MAX™ 6000 TAOS 10.1 Release Note* describes all new features introduced in TAOS 10.1 for MAX 6000 units. The MAX 6000 unit continues as the platform in the MAX family that can operate as a MultiVoice® gateway. MAX 3000 units are not supported by this release, and are no longer supported as a MultiVoice® gateways.

Refer to "Notices and Known Issues" on page 5-1 to see if there are limitations that apply to features in this release.



Caution You must use the software procedures in "Upgrading and Downgrading" on page 1-1 to load this new version of software onto your system or to restore a previous version. Read the instructions carefully before upgrading or downgrading your system.

Features in TAOS 10.1

This release note organizes TAOS 10.1 features using the following feature categories:

- Encapsulation
- IP
- L2TP
- Multicast
- MultiDSP
- Multivoice®
- SNMP
- Other

Licensing for Premium Feature Set

Beginning with TAOS 10.1, the system requires an additional Premium Feature Set software license. To verify that the Premium Feature Set license for 10.1 has been enabled in the system, look in the `00-100 Sys Option` status window for the following display:

```
10.1 FSet Enabled
```

The Premium Feature Set 10.1 licence enables the following feautures:

- V.92 PCM upstream
- V.92 modem on hold signaling on L2TP
- PPP Extensible Authentication Protocol (EAP)

For information about obtaining and enabling Lucent Technologies software licenses, contact your Lucent sales representative.

Feature Identification Numbers

Some features are tracked through development by means of a feature identification (FID) number. Table 2-1 describes t features in TAOS 10.1 that include a FID number.

Table 2-1. Features in TAOS 10.1 organized by FID number (page 1 of 2)

Feature Identification Number	Description
261445	"IP-in-IP tunneling support"
261615	"MultiVoice: Special trunk group for hairpin call"
510175	"Multicast support extended to all vrouters"
510538	"MultiVoice: CLI indicator enhancement"
510274	"Disabling end-point discriminator negotiation in establishing PPP sessions"
510618	"DSCP marking and remarking for L2TP"
510653	"Configuring frames per packet for each codec"
510708	"Q.931 Cause Code (12) with Call-Disconnect-Notify"
510710	"Physical channel ID (38) in incoming call request"
510728	"Configuring Link Control and Network Control Protocol timeout values"
510816	"Configurable L2TP hello packet policy"

Table 2-1. Features in TAOS 10.1 organized by FID number (page 2 of 2)

Feature Identification Number	Description
510817 510818	"Support for PPP Extensible Authentication Protocol (EAP)"
510820	"Session idle timer enhancements for layer 2 tunneling"

Firmware in TAOS 10.1

This section displays the digital modem card and MultiDSP slot card firmware versions supported in TAOS 10.1.

Firmware versions for digital modem cards

The Mindspeed firmware versions for the MAX TNT Digital Modem slot cards include support for V.90, K56flex, K56plus, and all slower, standard modem speeds. This release includes the following Mindspeed firmware:

- Series56 Digital Modem—`V2.0982-K56_DLP_CSM`
- Series56 III Digital Modem—`V5.8175`

Firmware versions for MultiDSP slot cards

This release includes the following firmware versions for all the MultiDSP slot cards:

- Controller—`V0.2.12`
- Modem—`V0.2006.0`
- PHS—`V2.1.1`
- VoIP—`V4.0.30`
- V.110—`V0.0.3`
- WORM—`V0.0.3`

Overview of slot card support in this release

Following are slot cards supported in TAOS 10.1:

- 8-Port module. Series 56K Modem (MX-SL-8MOD-S56)
- 12-Port module. Series 56K Modem (MX-SL-12MOD-S56)
- 16-Port module. Series 56K Modem (MX-SL-16MOD-S56)
- 2-Port IMUX (MX-SL-2PMHP)
- 6-Port IMUX (MX-SL-6PMHP)
- 8 Port ISDN BRI N S/T (MX-SL-8BRIN)
- 8 Port ISDN BRI T S/T (MX-SL-8BRIT)
- 8 Port ISDN BRI U (MX-SL-8BRIU)
- 48 Port MultiDSP Card (MX-SL-48M-DSP)

- 60 Port MultiDSP Card (MX-SL-60M-DSP)
- 8 Port PHS DSP Card (MXHP-SL-DSP8)
- 12 Port PHS DSP Card (MXHP-SL-DSP12)
- 16 Port PHS DSP Card (MXHP-SL-DSP16)
- 16 Port PHS DSP Card, canless (MX-SL-DSP16-CO)
- 8 Port MultiVoice DSP Card (MX-SL-8DSP)
- 12 Port MultiVoice DSP Card (MX-SL-12DSP)
- 16 Port MultiVoice DSP Card (MX-SL-16DSP)
- 8 Port V110 Card (MX-SL-8V110)

Features in TAOS 10.1

3

Encapsulation 3-1
IP 3-2
Layer 2 tunneling 3-3
Multicast 3-9
MultiDSP 3-12
MultiVoice® 3-13
SNMP 3-22
Other 3-30
Reference Entries 3-31

This Release Note is grouped into seven TAOS categories: Encapsulation, IP, Layer 2 Tunneling, MultiDSP, MultiVoice®, SNMP, and Other. The last section in this chapter presents reference entries for the features introduced in 10.1.

Encapsulation

Following are Encapulation-related features introduced with this release.

Disabling end-point discriminator negotiation in establishing PPP sessions

When establishing Point-to-Point Protocol (PPP) connections, negotiating an endpoint discriminator is unnecessary and increases the connection times.

You can now set values for the following parameters that direct the unit not to negotiate a Link Control Protocol (LCP) endpoint discriminator:

```
Ethernet > Answer > Encaps > MPP = No and
Ethernet > Answer > Encaps > MP = No
```

or

```
Ethernet->Answer->Id Auth = Called Require and
Connection > any Connection Profile > Encaps = PPP
```



Note An end point discriminator is required for Multilink PPP (MP) or Multilink Protocol Plus™ (MP+) calls.

IP

Following are IP-related features introduced with this release.

IP-in-IP tunneling support

The MAX 6000 now supports IP-in-IP encapsulation (RFC 2003). IP-in-IP functionality modifies an IP packet's typical routing by encapsulating the packet within another IP header. The encapsulating header specifies the address of a node that would not typically be selected as a destination on the basis of the packet's actual destination address. The router that receives the packet decapsulates it, and then routes the packet to its original destination. For additional details, see RFC 2003, *IP Encapsulation Within IP.*

This method of rerouting packets is referred to as *tunneling* the packet, and the end points of the tunnel is the device that encapsulates the packets (called the *encapsulator*) and the device that decapsulates the packets (called the *decapsulator*).

If the Foreign Agent receives an incoming packet that is larger than the IP-in-IP maximum transmission unit (MTU) size, the MAX 6000 fragments the packet before encapsulation. The MAX 6000 then ecapsulates each fragment independently. The IP-in-IP MTU size is currently fixed at 1480 bytes.

IP-in-IP encapsulation

The source address in the outer IP header of the IP-in-IP packet is set to the encapsulator IP address and the destination IP address is set to the IP address of the decapsulator.

Settings in a connection profile

An additional value, `IPINIP` has been added to the `Tunnel protocol` parameter. Following are the `Tunnel options` profile (shown with sample settings) that are relevant to IP-in-IP encapsulation.

```
Ethernet
  Connections
    connection name
      Tunnel options
        Profile type=Mobile-client
        Tunnel protocol=IPINIP
        Pri. Tunnel Server=10.2.3.4
```

Settings in a RADIUS profile

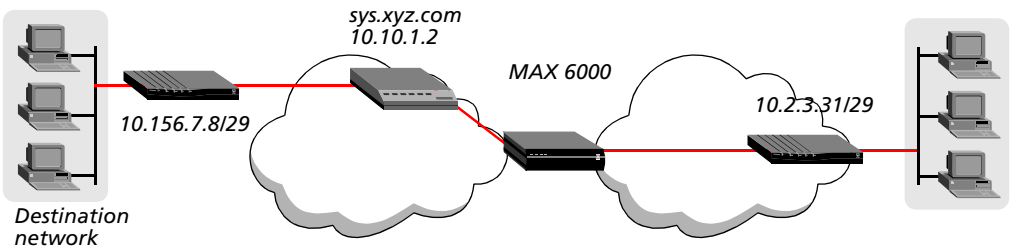
You can use the RADIUS attributes `Tunnel-Type (64)` and `Tunnel-Server-Endpoint (67)` to indicate IP-in-IP encapsulation. The value (7) for RADIUS attribute 64

(Tunnel-Type) is used to request IP-IN-IP encapsulation. Value (12) is also accepted for IP-IN-IP (see RFC 2868) but Lucent recommends that the correct value of (7) be used.

Sample IP-in-IP connection

Figure 3-1 shows a sample IP-in-IP tunnel. The Pipeline® unit with the address 10.2.3.31/29 logs into the destination network (10.156.7.8/29) by dialing in to the MAX 6000 unit unit. After the connection has been established, the MAX 6000 unit unit encapsulates the IP packets in this data stream and forwards them to the router at 10.10.1.2. That router decapsulates the packets and forwards them to their real destination.

Figure 3-1. IP-in-IP tunneling



Following are the values entered to configure a local profile:

```
Ethernet
  Connections
    p45
      Station=p45
      Active=Yes
      Encaps=PPP
        Encaps options
          Recv PW=localpw
        Ip options
          WAN Alias=10.2.3.31/29
        Tunnel options
          Profile type=Mobile-client
          Tunnel protocol=IPINIP
          Pri. Tunnel Server=sys.xyz.com
```

Following is a comparable RADIUS profile:

```
p50 Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 10.2.3.31,
   Framed-IP-Netmask = 255.255.255.248,
   Tunnel-Type = IPINIP,
   Tunnel-Server-Endpoint = "sys.xyz.com"
```

Layer 2 tunneling

Following are Layer 2 tunneling-related features introduced with this release.

Session idle timer enhancements for layer 2 tunneling

This release enhances the session idle timer for tunneling protocols by allowing you to configure generic filters that check against carried PPP frames that affect idle timer calculations. This feature is useful for preventing Link Control Protocol (LCP) Echo requests from keeping a session alive, even when no user data is being transferred.

In previous software release, generic call filters were ignored by the network access server (NAS) in L2F tunnels, Layer 2 Tunneling Protocols (L2TP) L2TP access concentrator (LAC), and PPTP access concentrator (PAC).

For information about configuring generic filters, see the *MAX Network Configuration Guide*.

Specifying whether to log L2TP `syslog` messages

In this release, you can specify whether `syslog` messages generated while the unit is processing a Layer 2 Tunneling Protocol (L2TP) call are sent to the `syslog` server.

The `Ethernet > Mod Config > Log` profile contains the new `Log Tunnel Progress` parameter, which enables and disables the transmission of the messages to `syslog`. If you specify `Yes` (the default), L2TP `syslog` messages are sent to the `syslog` server. When an L2TP tunnel is established, messages in the following format are sent:

`"TUNNEL-`*`session_ID`*`, L2TP Control Channel up with `*`peer_name`*`"`

`"TUNNEL-`*`session_ID`*`, L2TP Data Channel up with `*`peer_name`*
`[MBID `*`route_ID`*`]"`

When the tunnel is deactivated, messages in the following format are sent:

`"TUNNEL-`*`session_ID`*`, L2TP Tunnel Cleared: result code `*`result_code`*`,`
`error code `*`error_code`*`"`

If you specify `No`, L2TP `syslog` messages are not sent to the `syslog` server.

Configurable L2TP hello packet policy

In this release, the system sends L2TP Hello messages to its peer only if the control channel or the control and data channels are inactive.

In previous software releases, you could disable the system's sending of Hello messages or configure the unit to always send them after the period specified by the `Hello Timer` parameter in the `Ethernet > Mod Config > L2 Tunneling Options > L2TP config` subprofile. However, because the receipt of an L2TP control or data packet from a remote peer indicates that the remote L2TP system is alive, the system need not send Hello messages if it is receiving control or data packets.

As in previous software releases, if the `Hello Timer` parameter is set to zero, the keepalive mechanism is disabled and the system does not send Hello messages to its peer. If, however, the `Hello Timer` parameter is set to a nonzero value, the system sends L2TP Hello messages only if has not received a control packet (as in previous releases) or control *and* data packets from a remote peer during the period defined by the `Hello Timer` parameter.

New `Hello Policy` parameter

A new parameter in the `Ethernet > Mod Config > L2 Tunneling Options > L2TP config` subprofile, `Hello Policy`, specifies whether a MAX 6000 unit's sending of L2TP Hello messages to its peer is based on an inactive control channel or inactive control *and* data channels. You can set this parameter to one of the following values:

- `No Ctrl Activ` (the default)—The MAX 6000 unit sends a periodic Hello Message only if the control channel is inactive. This setting matches TAOS implementation in previous software releases.
- `No Activity`—The MAX 6000 unit sends periodic Hello messages only if the control channel and all associated data channels are inactive.

Changes to the `Hello Policy` parameter take effect after the period specified by the `Hello Timer` parameter. The `Hello Policy` parameter is not applicable if L2TP is not active on the unit.

To disable the unit from sending Hello packets to its peer, set the `hello-timer` parameter to zero (`0`).

Sample configuration

The following sample settings configure a MAX 6000 unit to send Hello messages every 15 seconds if both control and data channels are inactive:

```
Ethernet
    90-E00 Mod Config
        L2 Tunneling Options
        ...
        L2TP Mode = LAC
        ...
            L2TP Config
                ...
                Hello Policy = No Activity
                Hello Timer = 15
                ...
```

Physical channel ID (38) in incoming call request

This new feature adds the Call Management Attribute Value Pair (AVP) `Physical Channel ID` to the L2TP control message `Incoming-Call-Request`.

The `Physical Channel ID` AVP is defined in RFC2661 (L2TP) as an optional AVP. It may be present in the control messages Incoming-Call-Request (ICRQ) and Outgoing-Call-Reply (OCRP) send by the L2TP Access Concentrator (LAC) to the L2TP Network Server (LNS).

The Physical Channel ID AVP, Attribute Type 25, encodes the vendor specific physical channel number used for a call.

The Attribute Value field for this AVP has the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|                       Physical Channel ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Physical Channel ID is a 4 octet value intended to be used for logging purposes only.

This AVP may be hidden by setting the H-bit. The M-bit for this AVP must be set to 0. The Length (before hiding) of this AVP is 10.

Q.931 Cause Code (12) with Call-Disconnect-Notify

This new feature adds the Call Management AVP "Q.931 Cause Code" to the L2TP control message Call-Disconnect-Notify.

The Q.931 Cause Code AVP is defined in RFC2661 (L2TP) as an optionnal AVP. It may be present in the control message Call-Disconnect-Notify (CDN) sent by either the LAC or LNS to notify the peer that a call disconnection has occured within the tunnel.

The Q.931 Cause Code AVP, Attribute Type 12, is used to give additional information in case of unsolicited call disconnection.

The Attribute Value field for this AVP has the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Cause Code           |   Cause Msg   | Advisory Msg...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Cause Code is the returned Q.931 Cause code, and Cause Msg is the returned Q.931 message code (e.g., DISCONNECT) associated with the Cause Code. Both values are returned in their native ITU encodings [DSS1]. An additional ASCII text Advisory Message may also be included (presence indicated by the AVP Length) to further explain the reason for disconnecting.

This AVP MUST NOT be hidden (i.e. the H-bit MUST be 0). The M-bit for this AVP MUST be set to 1. The Length of this AVP is 9, plus the size of the Advisory Message.

DSCP marking and remarking for L2TP

Differentiated Service Code Point (DSCP) marking and remarking enables application traffic to signal their QoS requirements into the Internet network.

The MAX 6000 now extends DSCP capabilities to Layer 2 Tunneling Protocol (L2TP) traffic, so that data packets *from* and *to* the client influence the DSCP value used in the outer IP header, which in turn control the QoS properties of these encapsulated packets as they traverse from LAC to LNS.

DSCP marking and remarking for tunneling protocols

Although DSCP marking and remarking are handled for most IP packets, layer 2 tunneling protocols (such as L2TP, PPTP) do not inherit these facilities for their encapsulated data.

DSCP capabilities for L2TP control packets are not yet supported in this release.

The outer IP header remains at the default value of zero if:

- The L2TP access concentrator (LAC) cannot access PPP information or might not be required to check the specific user identity, which means that the `connection` profile might not be available on the LAC. In such a situation, the DSCP value for outer IP header is always the default value, which is zero.
- If data packets are compressed or the call is an multilink protocol call, TAOS is unable to check against the whole packet. In this situation, where TAOS cannot locate the type of service (TOS) value, the DSCP value for outer IP header remains at the default value of zero.

Command-line interface settings for DSCP marking and remarking for L2TP

The `Ethernet > Connections > *any connection profile* > Tunnel options menu` now includes several new parameters, shown below with their default settings.

```
Ethernet
   Connections
      any connection profile
         Tunnel options
            TOS Filter = 0
            TOS Enabled = Yes
            TOS Mark Type = Precedence -T
            TOS DSCP = 00
            TOS Precedence = N/A
            TOS = Normal
```

Note To set these parameters, you must first set Ethernet > Connections > any connection profile > Active = Yes and Ethernet > Connections > Connections > any connection profile > Tunnel options > Tunnel protocol = L2TP

RADIUS interface changes:

This release includes the following new RADIUS attributes:

```
# Ascend IP TOS/DSCP Attributes for the tunnel traffic
ATTRIBUTE Ascend-Tunnel-TOS                282     integer
ATTRIBUTE Ascend-Tunnel-TOS-Precedence     283     integer
ATTRIBUTE Ascend-Tunnel-DSCP               284     integer
ATTRIBUTE Ascend-Tunnel-TOS-Filter         285     string
ATTRIBUTE Ascend-Tunnel-TOS-Copy           286     integer


VALUE Ascend-Tunnel-TOS IP-TOS-Normal           0
VALUE Ascend-Tunnel-TOS IP-TOS-Disabled         1
VALUE Ascend-Tunnel-TOS IP-TOS-Cost             2
VALUE Ascend-Tunnel-TOS IP-TOS-Reliability      4
VALUE Ascend-Tunnel-TOS IP-TOS-Throughput       8
VALUE Ascend-Tunnel-TOS IP-TOS-Latency          16
VALUE Ascend-Tunnel-TOS IP-TOS-Dscp             128
VALUE Ascend-Tunnel-TOS IP-TOS-Dscp-Remarking   129


VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Normal         0
```

```
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-One            32
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Two            64
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Three          96
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Four           128
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Five           160
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Six            192
VALUE Ascend-Tunnel-TOS-Precedence IP-TOS-Precedence-Pri-Seven          224
VALUE Ascend-Tunnel-TOS-Copy  Ascend-TOS-Copying-No          0
VALUE Ascend-Tunnel-TOS-Copy  Ascend-TOS-Copying-Yes         1
```

Values for `Ascend-Tunnel-TOS` attribute are created using the same rules as for `Ascend-IP-TOS` and Ascend-IP-OUTGOING-TOS.

The existing RADIUS attribute `Ascend-TOS-Copying` has now been replaced by `Ascend-Tunnel-TOS-Copy`.

ToS byte copying

With this release, you can specify that the MAX 6000 unit copies Type of Service (ToS) bits from the IP header into a Layer 2 Tunneling Protocol (L2TP) header.

ToS byte copying

When a PPP frame arrives at an L2TP access concentrator (LAC), the encapsulated IP frame might contain a ToS byte value defined by the client application. If so, the unit takes the ToS byte from the initial IP packet (within the PPP packet) received on the L2TP access concentrator (LAC). It then copies it to the UDP/IP ToS byte in the IP packet encapsulating the L2TP packet sent to the L2TP network server (LNS).

The ToS byte is copied, not created or changed. The fact that the UDP/IP frame contains the same ToS byte value that the client application set allows the unit to use Quality Of Service (QoS) during the transport of the frame within the customer network However, when you use the ToS byte copying feature, the MAX 6000 unit unit cannot perform compression or fragmentation of packets.

New `TOS Copying` parameter

The `Ethernet > Connections > *any connection profile* > Tunnel options` profile contains the new `TOS Copying` parameter, which controls whether or not the ToS byte is copied. If you set `TOS Copying` to `No`, the unit does not copy the ToS byte from the inner IP header, but sets the ToS byte in the outer IP header to `000`. If you set `TOS Copying` to `Yes`, the unit copies the ToS byte from the inner IP header.



Note ToS copying might not be possible if the connection uses compression, encryption, MP, or MP+.

New RADIUS `Ascend-TOS-Copying (266)` attribute

With this release, the new 16-bit VSA `Ascend-TOS-Copying (266)` has been added. This attribute controls whether the ToS byte is copied. If you set `Ascend-TOS-Copying` to `Ascend-TOS-Copying-No(0)`, the unit does not copy the ToS byte from the inner IP header, but sets the ToS byte in the outer IP header to `000`. If you set `Ascend-TOS-Copying` to `Ascend-TOS-Copying-Yes(1)`, the unit copies the ToS byte from the inner IP header.

ToS copying might not be possible if the connection uses compression, encryption, MP, or MP+.

Note The following user profile shows the use of the new attribute `Ascend-TOS-Copying`:

```
marcoshelflocal  User-Password="123"
  Tunnel-Type=L2TP,
  Tunnel-Server-Endpoint=10.5.6.10,
  Ascend-TOS-Copying = Ascend-TOS-Copying-Yes
If you use the Ascend-TOS-Copying attribute, you must set auth-radius-compat
to 16-bit-vendor-specific in the rad-auth-client subprofile of the
external-auth profile.
```

Multicast

Multicast support extended to all vrouters

With this release, the MAX 6000 extends multicast support from the main virtual router (VRouter) to all vrouters. Operation of multicast in each vrouter behaves identically to that in the main VRouter. Virtual routers need the ability to bridge multicast traffic. Support for Web TV and other multimedia applications.

Note For the MAX 6000, a multicast vrouter can only have a WAN connection profile as its MBONE because the MAX 6000 only has one ethernet port which is always in the main vrouter.

New Multicast menu

The `Ethernet > Mod Config > Multicast` menu now refers to the global vrouter. And the `Ethernet > Virtual Routers > any vRouter Name` profile has an additional submenu called `Multicast`, which has the following parameters (whose default values are the same as in the `Ethernet > Mod Config > Multicast`... profile):

```
Ethernet
  Virtual Routers
    any vRouter Name profile
   Multicast...
        Forwarding=Yes
        Membership Timeout=360
        Mbone Profile=
        HeartBeat Addr=0.0.0.0
        HeartBeat Udp Port=0
        HeartBeat Slot Time=0
        HeartBeat Slot Count=0
        Alarm threshold=0
```

```
Source Addr=0.0.0.0
Source Mask=0.0.0.0
```

Parameter	Setting
Fowarding	Enables multicast forwarding in the MAX 6000 unit. n Yes—Turns on multicast forwarding in the MAX 6000 unit. n No (the default)—Disables multicast forwarding.
Membership Timeout	Time-out (in seconds) for client responses to multicast polling messages. Specify an integer from 60 through 65535. The default is 360.
Mbone Profile	Name of a connection profile the TAOS unit uses to reach the MBONE router. Default value is null..
HeartBeat Addr	Multicast address for heartbeat monitoring. The MAX 6000 unit unit listens for packets to and from the associated group. Specify the address in dotted decimal notation. The default is 0.0.0.0.
HeartBeat Udp Port	User Datagram Protocol (UDP) port number. The default is 0 (zero). If specified, heartbeat monitoring listens only for multicast packets received on that port. (All the Heartbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.) .
HeartBeat Slot Time	Interval (in seconds) in which the MAX 6000 unit unit polls for multicast traffic. The default is 0 (zero).
HeartBeat Slot Count	How many times the MAX 6000 unit unit polls before comparing the number of multicast packets it received to the HeartBeat threshold value. The default is 0 (zero).
HeartBeat threshold	Minimum number of packets the MAX 6000 unit unit can receive without generating an alarm trap. The default is 0 (zero), which disables heartbeat monitoring.
Alarm threshold	Minimum number of packets the MAX 6000 unit unit can receive without generating an alarm trap. The default is 0 (zero), which disables heartbeat monitoring.
Source Addr	A multicast address. When it performs heartbeat monitoring, the MAX 6000 unit unit ignores packets from the IP address you specify. Specify the IP address in dotted decimal notation. The default is 0.0.0.0.
Source Mask	A subnet mask that the MAX 6000 unit unit applies to the Source Addr value. Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.

Note The `Client`, `Rate Limit`, and `Grp Leave Delay` parameters don't appear in this submenu as they do in the `Ethernet > Mod Config > Multicast` submenu because these parameters configure the IP interface. there is only one IP interface on the MAX, which cannot be placed into a Vrouter. Also note that each vrouter (excluding the main VRouter) supports a single WAN MBONE only.

Displaying information about VRouters

You can now use the `show igmp` command and the `show mrouting` command to display information about vrouters.

```
ascend% show igmp ?

show igmp ? Display help information

show igmp stats vRouterName Display IGMP Statistics

show igmp groups vRouterName Display IGMP groups Table

show igmp clients vRouterName Display IGMP clients


ascend% show mrouting ?

show mrouting stats vRouterName Display MROUTING Statistics
```

Note If vroutername is not specified it will default to the main VRouter.

You can now use the `iproute show vrouter` command to display the multicast address entries for the MAX routing table:

```
ascend % iproute show vrouter

Destination        Gateway         IF          Flg   Pref Met     Use     Age
127.0.0.0/8        -               bh0_cam     CP       0   0       0    7013
127.0.0.1/32       -               local       CP       0   0       0    7013
127.0.0.2/32       -               rj0_cam     CP       0   0       0    7013
224.0.0.0/4        -               mcast       CP       0   0       0    7013
224.0.0.1/32       -               local       CP       0   0       0    7013
224.0.0.2/32       -               local       CP       0   0       0    7013
224.0.0.9/32       -               local       CP       0   0       0    7013
Total Routes  = 7Hidden Routes = 0
```

Note As these parameters are not new but now appear in an additional location, the currently documented parameters apply to this feature with the modification that the parameters have an additional location of `Ethernet > Virtual Routers > any vRouter Name` profile > `Multicast`. Following are the parameters:

```
Forwarding=Yes
Membership Timeout=360
Mbone Profile=
HeartBeat Addr=0.0.0.0
HeartBeat Udp Port=0
HeartBeat Slot Time=0
```

```
HeartBeat Slot Count=0
Alarm threshold=0
Source Addr=0.0.0.0
Source Mask=0.0.0.0
```

MultiDSP

Following are MultiDSP-related features introduced with this release.

V.92 PCM upstream

The ITU V.92 Recommendation specifies the following enhancements:

- an increase in the maximum data rate towards the network
- significantly quicker start-up times on recognized connections
- the ability to put the modem on hold when the network indicates that an incoming call is waiting

V.92 modem-on-hold (MoH) and quick-connect features were introduced in earlier TAOS versions. This release introduces support for the V.92 PCM upstream (PCMU) feature, as well as SNMP and RADIUS configuration of all V.92 modem features.



Note Not all V.92 client modems fully support all V.92 capabilities. Lucent recommends that end users regularly check with their manufacturers for firmware updates. V.92 capabilities are only achieved when the client modems are V.92 compatible, otherwise the modems fall back to a V.90 or slower protocols. For V.92 PCM upstream connections, actual improvement over performance experienced with V.90 connections will vary on the basis of line conditions.

Enabling V.92 PCMU

With V.90 modulation, the upstream speed of a connection was limited to 33.6Kbps. V.92 PCMU enables MultiDSP modems to connect at a higher receive (upstream) data rate, to reduce upload times for large files and email attachments. Following are the related parameters, shown with default settings:

```
Ethernet
  Mod Config
    TServ Options
      MDM Modulation = V.90
      MDM V.92 Rx Baud = 48000
```

The `MDM Modulation` parameter sets the modulation protocol to be attempted by the modems during connection negotiation. When this is set to `V92`, the `MDM V.92 Rx Baud` parameter determines the maximum upstream (receive) baud rate to be negotiated by the modems. The default is 48000, which is the fastest rate supported by the PCMU feature.

The following parameter values enable V.92 with a maximum negotiable upstream speed of 48Kbps (the default):

```
Ethernet
  Mod Config
```

```
TServ Options
  ...
  MDM Modulation = V.92
  MDM V.92 Rx Baud = 44000
  ...
```

MultiVoice®

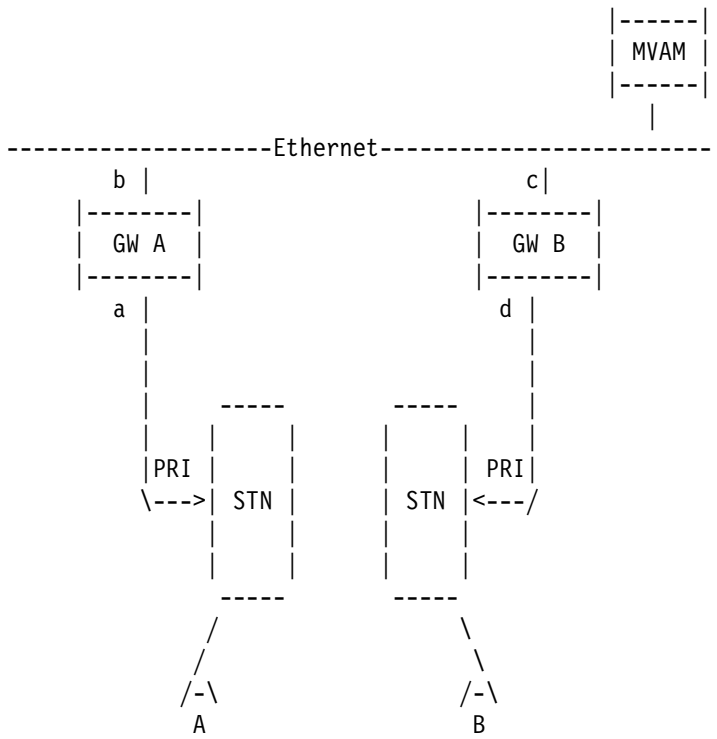
Following are MultiVoice-related features introduced with this release.

MultiVoice: CLI indicator enhancement

This feature provides transmission of the Calling Party Number information element from an incoming VoIP call on an E1/T1 interface over H.225/Q.931 to the receiving unit. Calling party number information, specifically, calling line identification presentation (CLIP) and calling like identification restriction (CLIR) indicators are passed from the incoming ISDN setup message over H.225/Q.931 to the destination gateway for inclusion in the outgoing ISDN setup message in voice over IP (VoIP) calls.

This feature improves calling line identifiaction (CLI) interconnectivity between networks by transparent end-to end transmission of the presentation indicator field of the calling party information element. Each individual E1/T1 port (ingress and egress ports) can be configured to override this field in both ends of the network.

Since there are gateways that will misinterpret the CLID as a result of encoding the Calling Party Number information element, the ability to control the sending of this element between gateways can be configured on a unit-wide basis. This is provided by the `extended-clid-support` parameter, which defaults to `No` to avoid compatability issues. This will not be necessary if third party equipment operates full accordance with specification H.225/Q.931.



Using the diagram above the following sequence demonstrates the path:

1 Phone A dials GW A, from the incoming Q.931 setup message the gateway extracts and stores the Calling Party Information element from the ingress call 'a'.

2 GW A contacts the MVAM over H.323 and is given the IP-Address of GW B.

3 If `extended-clid-support` is set to `Yes`, GW A sends the Calling Party Information Element over H.225/Q.931 to GW B 'b' to 'c'

Changing this parameter affects all modules on the unit as we do not know if the destination GW will be able to decode the calling party information element. In our own implementation this will result in misinterpreting the CLID. Therefore `extended-clid-support` defaults to `No` to avoid this problem. If other vendors have implemented decoding in full accordance with H.225/Q.931 then this will not be a problem.

4 If the E1/T1 interface at GW B on which the outgoing setup message is to be sent is configured to tx-clir-flag-in-voip then the ISDN setup message will be sent containing the same Calling Party Number information element 'd' as received at 'a' and phone B will ring.

The E1/T1 `tx-clir-flag-in-voip` defaults to 'No' as the existing implementation will not currently send this element.

Note The presentation and screening indicators will only be passed when present on the ingress line as part of Q.931. This excludes T1 CAS and E1/R2.

Configuring frames per packet for each codec

You can configure each of the available codecs and the number of frames per packet to negotiate using the new `codec-options` subprofile. By default, all codecs are

enabled and their frames per packet are set to 2. You can disable codecs selectively as required by your network. You cannot, however, disable the codec specified as preferred codec in the `packet-audio-mode` parameter.



Note TAOS 10.1 allows separate frames per packet settings for each codec, consequently, the generic `frames-per-packet` parameter is no longer supported. After upgrading to TAOS 10.1, the previous entry for the `frames-per-packet` is no longer maintained. If you attempt to load an old configuration file that had been saved earlier on a TFTP server or in flash memory, you receive an error message indicating that the "frames per packet" value is unknown and will be ignored.



Note The `frames-per-packet` value associated with a given codec might be ignored as as result of negotiation between gateways.

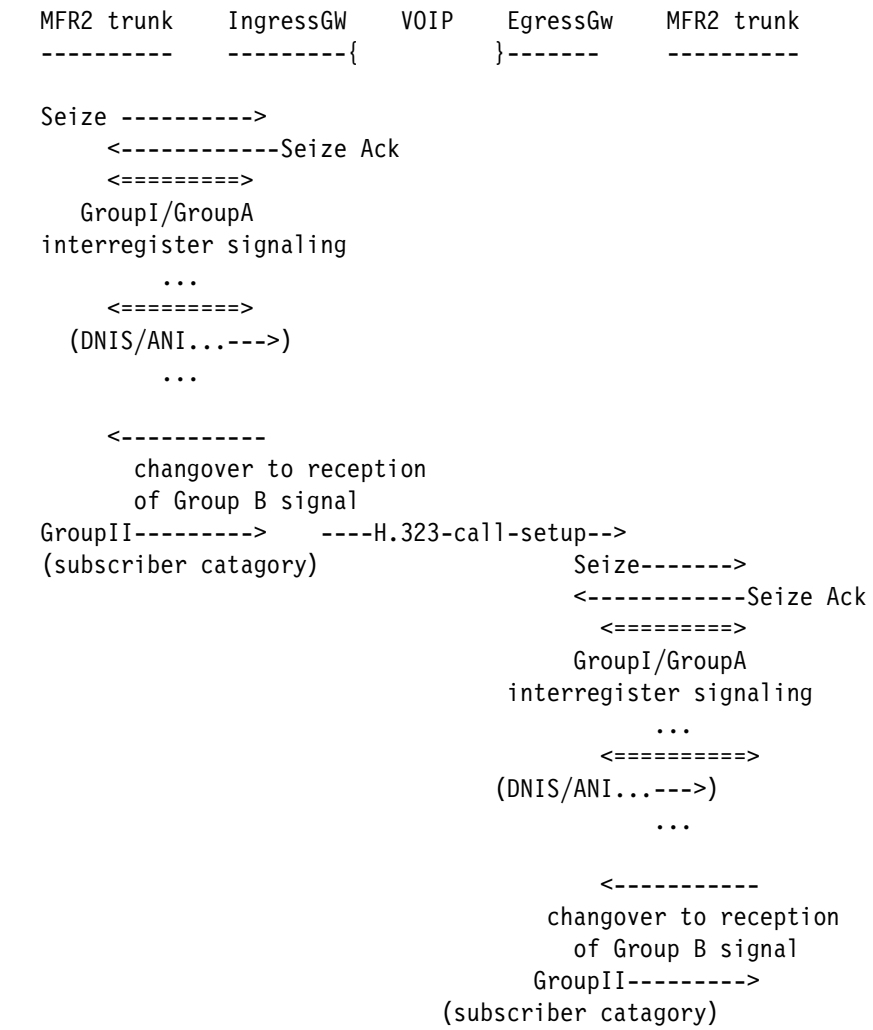
Parameter	Setting
`g711-ulaw-enabled`	Enables G.711 mu-law codec. Valid values are `yes` (default) or `no`.
`g711-ulaw-fpp`	Number of voice frames per RTP packet for G.711 mu-law codec. Valid values are whole numbers from 1-10. The default value is 2.
`g711-alaw-enabled`	Enables G.711 a-law codec. Valid values are `yes` (default) or `no`.
`g711-alaw-fpp`	Number of voice frames per RTP packet for G.711 a-law codec. Valid values are whole numbers from 1-10. The default value is 2.
`g723-enabled`	Enables G.723 codec. Valid values are `yes` (default) or `no`.
`g723-fpp`	Sets the number of voice frames per RTP packet for G.723 codec. Valid values are whole numbers from 1-10. The default value is 2.
`g723-6.4kps-enabled`	Enables G.723 6.4kps codec. Valid values are `yes` (default) or `no`.
`g723-6.4kps-fpp`	Number of voice frames per RTP packet for G.723 6.4kps codec. Valid values are whole numbers from 1-10. The default value is 2.
`g728-enabled`	Enables G.728 codec. Valid values are `yes` (default) or `no`.
`g728-fpp`	Number of voice frames per RTP packet for G.728 codec. Valid values are whole numbers from 1-10. The default value is 2.
`g729-enabled`	Enables G.729 codec. Valid values are `yes` (default) or `no`.
`g729-fpp`	Number of voice frames per RTP packet for G.729 codec. Valid values are whole numbers from 1-10. The default value is 2.

Parameter	Setting
`frgsm-enabled`	Enables FRGSM codec. Valid values are `yes` (default) or `no`.
`frgsm-fpp`	Number of voice frames per RTP packet for FRGSM codec. Valid values are whole numbers from 1-10. The default value is 2.

E1 R1/R2 group II and group b cause codes

This feature provides E1 R1/R2 cause codes. The generic operation of MF-R2 interregister signaling and some of the signal meanings are described in ITU Q.441.

The call flow below shows a typical virtual MF-R2 call setup sequence with true-connect enabled. This feature is meant for end-to-end operation between MF-R2 trunks. This can be best described as an extension to the "true-connect" feature which suspends connection of a subscriber until the call is actually answered by the far end. This feature allows for the correct trunk response to be relayed back to the outgoing MF-R2 trunk for the called subscriber's actual line condition.



```
                                                  <----------- GroupB
                                                       (subscriber line status)

                         <----Alerting----------
          <----------- GroupB
            (subscriber line status)

                                  <------------Answer
                   <----H.323-call-connect---
          <------------Answer
```

Although not shown, a GroupB response may be a negative response like `line busy` or `out-of-order`. In these cases, the GroupB signal is followed by a `release` or `disconnect` signal. Addition mappings for these signals are provided for interworking with CAS and Q.931 trunks.

The main objective of this feature is to relay the `subscriber line free` and `charge/no charge` signals for subscriber billing.

R2 to ISDN

The objective of this feature is to provide end-to-end transport of the R2 group B signal recieved at the Egress Gateway. Provisions must be made to handle other signaling schemes.

The following is a description of the interworking of an ingress gateway with and R2 trunk in a VoIP session with an egress gateway using an ISDN interface.

```
MFR2 trunk    IngressGW    VOIP    EgressGw    ISDN trunk
----------    ---------{          }-------     ----------

Seize ---------->
     <------------Seize Ack
     <=========>
   GroupI/GroupA
interregister signaling
         ...
     <=========>
  (DNIS/ANI...--->)
         ...

     <-----------
       changover to reception
       of Group B signal
GroupII--------->    ----H.323-call-setup-->
(subscriber catagory)                   Q.931 Setup --->

                                        <------------Q.931 Proceeding

                                        <------------Q.931 Alerting
                     <----Alerting/Proceeding--
     <----------- GroupB
       (subscriber line status)
```

```
                                                <------------Q.931 Connect
                                        <------------Answer
                        <----H.323-call-connect---
                <------------Answer
```

Interworking with ISDN signaling is straightforward. The Group B signal used for a setup response is the E1 `Group B Answer Signal` on the ingress gateway. This is triggered upon receipt of the alerting signal and depends on the signaling-model.

Call failure group B signals are mapped from the disconnect cause code received at the egress gateway. `Cause Code Transparency` must be enabled. The mapping is borrowed from the Q.696 specification which describes interworking of ISUP/SS7 and R2 signaling. The group A signals are not mapped since switchover from Group A to Group B occurs before the setup request is created.

Table 3-1. Backward group signal mappings (from Q.696 6.2.2.4)

Disconnect cause code	R2 signal
34 (no circuit available)	Group A national congestion
34 (no circuit available)	Group A international exchange congestion
4	send special information tone
17 (user busy)	subscriber line busy
34 (no circuit available)	Group B congestion
1 (unassigned number)	unallocated number
27 (dest out of order)	subscriber's line out of order
34 (no circuit available)	default

ISDN to R2

The operation with R2 as the egress and ISDN as the ingress is similar to a ISDN-ISDN voip call except that cause code mapping follows those described in the section above and that Alerting and Proceeding is triggered by the GroupB signal. This also depends on the signaling-model. If `Fast Proceeding` is not set, the R2 signaling may exceed the T303 timeout time waiting on call proceeding.

The calling party class will be taken from the `Group Ii Signal` set in the E1 parameters of the egress gateway.

R2 to CAS

```
MFR2 trunk    IngressGW    VOIP    EgressGw    CAS
    ----------    ---------{          }--------    ---

    Seize ---------->
         <------------Seize Ack
```

```
        <==========>
      GroupI/GroupA
   interregister signaling
           ...
        <==========>
     (DNIS/ANI...--->)
           ...

        <------------
          changover to reception
          of Group B signal
   GroupII---------->    ----H.323-call-setup-->
   (subscriber catagory)                   Dial Out --->

                                           <------------Inband Alerting
                       <----Alerting/Proceeding--
        <----------- GroupB
          (subscriber line status)
                                           <------------Answer
                                <------------Answer
               <----H.323-call-connect---
        <------------Answer
```

Since CAS trunks provide very little information, all R2 signals are spoofed at the incoming trunk. All of the R2 signals are generated locally at the ingress gateway and derived from the hardcoded value or the E1 paremeters set at the ingress gateway. They in no way reflect the signaling of the far-end VoIP peer. The call does not proceed with a positive group B signal until the "alerting" is seen from the egress gateway. This, again, depends largely on the signaling-model, since the alerting is not a real CAS signal and is generated in various way depending on the VoIP signaling-model.

CAS to R2

```
CAS           IngressGW    VOIP    EgressGw    MFR2 trunk
    ----------    ---------{          }-------     ----------

    Incoming---------->
      (DNIS/ANI...--->)
             ...
                     ----H.323-call-setup-->
                                        Seize------->
                                           <------------Seize Ack
                                             <==========>
                                           GroupI/GroupA
                                      interregister signaling
                                                ...
                                             <==========>
                                     (DNIS/ANI...--->)
                                                ...

                                             <------------
```

```
                                                  changover to reception
                                                    of Group B signal
                                                 GroupII--------->
                                          (subscriber catagory)
                                                      <----------- GroupB
                                                           (subscriber line status)

                          <----Alerting/Proceeding-------
                <----------- Alerting
```

There is nothing special about CAS to R2 except that alerting may be delayed depending on the signaling-model used.

MultiVoice: Enabling DTMF tone passing, QoS, and adaptive-jitter-buffer for G.723.1 and G.728 codecs

Units affected: TNT/APX

Support for DTMF-tone-passing using RFC2833, quality of service (QoS) statistics and adaptive-jitter-buffer for G.723.1 and G.728 can now be enabled. QoS and adaptive-jitter-buffer are also supported by the full-rate GSM (FRGSM) codec. QoS statistics and adaptive-jitter-buffer can be enabled for all codecs.

The previous implementation of G728 and G723 did not support RFC2833 or QoS. All these new features are supported in TAOS releases 10.1 and later but are not backward compatible with old TAOS versions (9.0, 9.1 and 10.0).

Voice payload should travel properly through third-party gateways; however, QoS statistics will not be processed properly, if the third-pary gateways ignore the RTP extension.

The following table shows the supported features by codec:

Table 3-2. Features supported by codec

codec	QoS Polling	RFC2833*	Adaptive Jitter Buffer
G.711 mu-law	yes	yes	yes
G.711 a-law	yes	yes	yes
G.729	yes	yes	yes
G.728	yes	yes	yes
G.723	yes	yes	yes
G.723 6.4kps	yes	yes	yes
FRGSM	yes	no	yes

Note MultiDSP modem firmware must be upgraded from V0.2.4 to V0.2.8, DSP firmware from V4.0.14 to V4.0.26, and RAS firmware from V0.2002.0 to V0.2004.0.

RFC2833 for DTMF-tone-passing

The `dtmf-tone-passing` parameter permits the passing of DTMF tones using RTP packets, as defined in RFC2833. The payload type can either be fixed (94) or be configured through dynamic payload type (such as for SIP). `dtmf-tone-passing` is available when `packet-audio-mode` is set to `g728`, `g723`, or `g723-6.4kps` only.

Parameter	Setting
`dtmf-tone-passing`	Valid value is `rfc2833`.

Quality of Service (QoS) statistics

The `rtpqos-polling-enable` parameter enables the collection of statistics for both directions of calls are exchanged through RTP header extentions. The information is then available to a call logging (CL) server at the end of each call. The statisics exchange is available only for MultiVoice. `rtpqos-polling-enable` is available when `packet-audio-mode` is set to `g728`, `g723`, `g723-6.4kps`, or `FRGSM` only.

Parameter	Setting
`rtpqos-tone-passing`	Valid values are `yes` or `no`.

Adaptive Jitter Buffer

The `ena-adap-jitter-buffer` parameter enables the algorithm that allows the jitter buffer depth be determined at run-time so that the jitter buffer can be optimized for both delay and voice quality. `ena-adap-jitter-buffer` is available when `packet-audio-mode` is set to `g728`, `g723`, `g723-6.4kps`, or `FRGSM` only.

Parameter	Setting
`ena-adap-jitter-buffer`	Valid values are `yes` or `no`.

MultiVoice: Special trunk group for hairpin call

The new `HairpinTrnkGrp` parameter specifies a trunk-group that will be used with hairpin calls. If `Use Trunk Group` is enabled in the `Sys Config` profile, hairpin calls will seek out outgoing trunks that matches the `HairpinTrnkGrp`. The `Trunk Group` of the `T1` profile will be used for the match. The valid range is 4 through 9999, consistent with the value of the `T1` trunk groups. The default is set to 9.

The trunk group will be used only when the `Sys Config` profile has `Use Trunk Grps=Yes`. The `Num Trunk Digits` parameter in the `Sys Config` profile will determine the active digits. For example, setting

```
HairpinTrnkGrp = 789
Num Trunk Digits = 1
```

will effectively make `HairpinTrnkGrp = 7`. This is consistent with the `Trunk Group` in the T1 or E1 profile.

If `HairpinTrnkGrp` is `0`, then any trunk-group will be chosen.

Silence suppression and adaptive jitter buffer

TAOS 10.1 now permits both both adaptive jitter buffer and silence suppression to be enabled simultaneously for all codecs used in Voice over IP (VoIP) calls.

Previously, if you attempted to enable adaptive jitter buffer by setting `VOIP:ena-adap-jitter-buffer` to `yes` and in the same profile, attempted to enable silence suppression by setting `silence-det-cng` to `yes`, you received an error message that they could not be enabled simultaneously. You can now enable both.

SNMP

Following are SNMP-related features introduced with this release.

MIB `hashcode.mib` now supported

The management information base (MIB) `hashcode.mib` is now supported. This MIB contains entries for all possible software licenses supported on MAX units and specifies whether a license is enabled or disabled. Following are the MIB objects and definitions:

```
ASCEND-HASH-CODE-MIB DEFINITIONS ::= BEGIN

IMPORTS
        sysHashCodeGroup  FROM ASCEND-MIB
        OBJECT-TYPE       FROM RFC-1212
        DisplayString     FROM ASCEND-MIB;

hashCodeTable  OBJECT-TYPE
        SYNTAX  SEQUENCE OF HashCodeTableEntry
        ACCESS  not-accessible
        STATUS  mandatory
        DESCRIPTION "A list of card code entries index by
                     the slotIndex and cardCodeFeature"
        ::= { sysHashCodeGroup 1 }

hashCodeTableEntry OBJECT-TYPE
        SYNTAX  HashCodeTableEntry
        ACCESS  not-accessible
        STATUS  mandatory
         DESCRIPTION "Definition of the row entries in the hash code table"
        INDEX  { hashCodeSlotIndex, hashCodeFeature }
        ::= { hashCodeTable 1 }

HashCodeTableEntry ::= SEQUENCE {
        hashCodeSlotIndex    INTEGER,
        hashCodeFeature      INTEGER,
```

```
        hashCodeState        INTEGER,
        hashCodeDescription  DisplayString,
        hashCodeDirty        INTEGER
                            }

hashCodeSlotIndex OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
         DESCRIPTION     "A unique value for each slot card. Its value ranges
                         between 1 and the value slotNumber."
        ::= { hashCodeTableEntry 1 }

hashCodeFeature OBJECT-TYPE
        SYNTAX  INTEGER {
                rs366(12),
                d-channel(13),
                auto-DBAE(14),
                bonding(15),
                aim(16),
                v25bis(17),
                x21(18),
                switched(19),
                multi-rate(20),
                t1-pri-conversion(21),
                pcbus(22),
                bridging(23),
                pipe-hx(24),
                frame-relay(25),
                ip-routing(26),
                ipx-routing(27),
                domestic(31),
                phs-2-1-support(33),
                modem-dialout(34),
                pipe-px(35),
                firewalls(36),
                serial-port-T1CSU(37),
                pipe-pots(39),
                force-multiband-platform-simulation(41),
                k56-slot-card-only(43),
                network-management(44),
                advanced-agent(45),
                phs-support(46),
                selectools(47),
                routing-protocols-disabled(48),
                atmp(49),
                maxdax(50),
                tnt-adsl-restricted(51),
                tnt-sdsl-restricted(52),
                tnt-idsl-restricted(53),
                voip(54),
                xcom-ss7(56),
                ss7asg(57),
```

```
                        l2tp(58),
                        pptp(59),
                        aodi(60),
                        ipinip(61),
                        sdtn(62),
                        vrouter(63),
                        madd-modem(64),
                        madd-96-devices(65),
                        madd-hdlc(66),
                        v110(67),
                        restrictDslTerm(68),
                        rtfax(69),
                        megamax(70),
                        l2f(71),
                        maxtap(72),
                        atmsvc(73),
                        frvc(74),
                        network-mgmt-voip(75),
                        network-mgmt-plus(76),
                        network-mgmt-plus-voip(77),
                        voip-max-capacity-allowed(79),
                        voip-pots(80),
                        cvmax(81),
                        wormarq(82),
                        nm-copper-loop-test(83),
                        nm-reporting(84),
                        nm-vpn(85),
                        nm-navis-radius(86),
                        tnt-x25(87),
                        restrict-redundancy(88),
                        pnni(89),
                        fgd-signaling(90),
                        ima(91),
                        maxlink-client(100),
                        data-call(101),
                        dual-slot-t1(102),
                        r2-signaling(103)
                        }
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION     "The list of available card code features."
                ::= { hashCodeTableEntry 2 }

        hashCodeState OBJECT-TYPE
                SYNTAX  INTEGER  {
                     enabled(1),  -- the hash code is licensed
                     disabled(2)  -- the hash code is not licensed, or is unavailable
                          }
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION     "The current hash code status"
                ::= { hashCodeTableEntry 3 }
```

```
hashCodeDescription OBJECT-TYPE
        SYNTAX  DisplayString
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION     "A description of the hash code feature"
        ::= { hashCodeTableEntry 4 }

hashCodeDirty OBJECT-TYPE
        SYNTAX  INTEGER  {
             dirty(1),     -- the hash code is dirty and may not be
             what is contained in the BASE profile.
             not-dirty(2)  -- the hash code is current and matched
             the value in the BASE profile.
             }
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION     "The current hash code status"
        ::= { hashCodeTableEntry 5 }

END
```

Consider the following:

- The `hashCodeSlotIndex` value is always 0 (zero) for MAX units.
- The `hashCodeDescription` value is always an empty string.
- After an `update` command alters the security programmable read-only memory (SPROM) bits, a query of the `systemStatusGroup.sysSPROM.sysSPROMOptions1.0` object identifier (OID) now indicates the new SPROM settings. However, you must still restart the unit for the changes to take effect.

Support for alarm MIBs

This release supports the alarm management information bases (MIBs) described in `draft-ietf-disman-alarm-mib-04.txt`.

Supported alarm MIBs

Four alarm MIBs are specified in `draft-ietf-disman-alarm-mib-04.txt`:

- `alarm.mib`
- `itu_alarm_tc.mib`
- `itu_iana_alarm_tc.mib`
- `itu_alarm.mib`

The MIBs provides information about the following:

- All possible alarms in the system
- Currently active alarms in the system
- Cleared alarms in the system

Use of the alarm MIBs requires the network management software license.

MIB tables

The alarm MIB consists of a generic alarm model and lists active and cleared alarms. An alarm model defines the possible states an alarm can assume as well as the object ID (OID) of the notification (trap) that is sent out when an alarm changes state. To access alarm information on a system, you can query the following tables:

Table	Indicates
`alarmModelTable`	Information applicable to all instances of all alarms for a given system. If a notification is not represented in the `alarmModelTable`, it is not an alarm state transition. The table is indexed by { `alarmListName, alarmModelIndex, alarmModelState` }.
`alarmActiveTable`	List of alarms currently occurring on a system. You can query this table upon device discovery and rediscovery to determine which alarms are currently active on the device. The table is indexed by { `alarmListName, alarmActiveDateAndTime, alarmActiveIndex` }.
`alarmActiveVariableTable`	Notification variable bindings associated with the alarms in the `alarmActiveTable`. The table is indexed by { `alarmListName, alarmActiveIndex, alarmActiveVariableIndex` }.
`alarmActiveStatsTable`	Current and total raised alarm counts as well as the last time an alarm was raised and cleared per named alarm list. The table is indexed by { `alarmListName` }.
`alarmClearTable`	List of alarms no longer active on the system. The table is indexed by { `alarmListName, alarmClearDateAndTime, alarmActiveIndex` }.
`ituAlarmTable`	International Telecommunication Union Telecommunication Standardization Sector (ITU-T) alarm information for possible alarms on the system, including alarm severity and event type. The table is indexed by { `alarmListName, alarmModelIndex, ituAlarmPerceivedSeverity` }.
`ituAlarmActiveTable`	ITU-T information for active alarms entries. The table is indexed by { `alarmListName, alarmActiveDateAndTime, alarmActiveIndex` }.
`ituAlarmActiveStatsTable`	ITU-T alarm statistics information. The table is indexed by { `alarmListName` }.

Specifying the maximum number of alarms in `alarmClearTable`

To set the maximum number of alarms in `alarmClearTable`, set the new `Alarm Clear Table Limit` parameter in the `Ethernet > Mod Config > SNMP Options` profile. Specify a value from 1 through 200. The default value is 100.

Clearing alarms from the alarmActiveTable and alarmClearedTable

To clear the alarms in alarmActiveTable and alarmClearTable, disable the associated SNMP Traps profile by setting Active to No. When the SNMP Traps profile is disabled, the alarm model table reports RowStatus as NOT_IN_SERVICE.

Deleting an alarm model table

To delete an alarm model table, delete the corresponding SNMP Traps profile.

MIB traps

Following are the traps supported by the alarm MIBs:

```
alarmRaise NOTIFICATION-TYPE
          OBJECTS     { alarmModelIndex,
                        alarmModelState,
                        alarmActiveResourceType,
                        alarmActiveResourceId }
          STATUS      current
          DESCRIPTION
             "An instance of the alarm indicated by alarmModelIndex
             has been raised against the entity indicated by
             alarmActiveResourceType and alarmACtiveResourceId."
          ::= { alarmNotifications 0 1 }

alarmCleared NOTIFICATION-TYPE
            OBJECTS     { alarmModelIndex,
                          alarmActiveResourceType,
                          alarmActiveResourceId }
            STATUS      current
            DESCRIPTION
              "An instance of the alarm indicated by alarmModelIndex
              has been cleared against the entity indicated by
              alarmActiveResourceType and alarmACtiveResourceId."
            ::= { alarmNotifications 0 2 }
```

TAOS modifications to the alarm MIBs

This release implements the following modifications of draft-ietf-disman-alarm-mib-04.txt:

- The draft-ietf-disman-alarm-mib-04.txt draft does not define an official number for alarm.mib. The number assigned in this release is { ascend 43 }.
- InetAddressType and InetAddress are defined in INET-ADDRESS-MIB. Currently, TAOS does not support that MIB. The defintions of InetAddressType and InetAddress have been copied to alarm.mib.

- Read-write access to `alarmModelTable` is not allowed. The access for this table has been changed to read-only.

Supported alarms

Following are the alarms supported by the alarm MIBs:

```
ALARM_ASCEND_LINKDOWN
---------------------
state: cleared, warning, raise
resource type: RESOURCE_IF
resource id: ifIndex

ALARM_FR_LINKDOWN
-----------------
state: cleared, raise
resource type: RESOURCE_IF
resource id: ifIndex

ALARM_SLOT_DOWN
---------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: slot id

ALARM_MODEM_SUSPECTED
---------------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: (16-bit slot id) | (16-bit port id)

ALARM_WAN_DISABLED
------------------
state: cleared, raise
resource type: RESOURCE_IF
resource id: ifIndex

ALARM_POWERSUP_ABSENT
---------------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: power supply's s/n

ALARM_POWERSUP_DOWN
-------------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: power supply's s/n

ALARM_REDUN_NOTAVAIL
--------------------
state: cleared, peerdown, nopeer
no resource associated
```

```
ALARM_MEGCO_LINKDOWN
--------------------
state: cleared, raise
no resource associated

ALARM_TRUNK_SPARING
-------------------
state: cleared, transit, failed
resource type: RESOURCE_IF
resource id: max (primaryIfIndex, sparingIfIndex)

ALARM_LIM_SPARING
-----------------
state: cleared, transit, failed
resource type: RESOURCE_OTHER
resource id: max (primarySlotIndex, sparingSlotIndex)

ALARM_WATCHDOG_FAILURE
----------------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: watchdog id

ALARM_WATCHDOG_OPEN
-------------------
state: cleared, raise
resource type: RESOURCE_OTHER
resource id: watchdog id

ALARM_IMA_LINK_LIF, ALARM_IMA_LINK_LODS, ALARM_IMA_LINK_RFI,
ALARM_IMA_LINK_TX_MIS, ALARM_IMA_LINK_RX_MIS, ALARM_IMA_LINK_TX_FAULT,
ALARM_IMA_LINK_RX_FAULT, ALARM_IMA_LINK_TX_UN, ALARM_IMA_LINK_RX_UN,
ALARM_IMA_GROUP_STARTUP, ALARM_IMA_GROUP_CFG, ALARM_IMA_GROUP_CFGFE,
ALARM_IMA_GROUP_LINKS, ALARM_IMA_GROUP_LINKSFE, ALARM_IMA_GROUP_BLOCK,
ALARM_IMA_GROUP_TIME,
-----------------------------------------------------------------------
state: cleared, raise
resource type: RESOURCE_IF
resource id: ifIndex

ALARM_DSX1_LINE_ERROR
---------------------
state: cleared, raise
no resource associated

ALARM_DSX3_LINE_ERROR
---------------------
state: cleared, raise
no resource associated
```

Other

Following are features introduced with this release that are not covered by the preceding sections.

Configuring Link Control and Network Control Protocol timeout values

510728 Three new parameters, `Max PPP conf req retry`, `PPP conf req timer`, and `Max PPP conf req timer` allow you to set retry and timer values for Link Control Link Protocol (LCP) and Network Control Protocol (NCP). When the MAX sends a request, it waits for the amount of time specified (in hundredths of a second) in the `PPP conf req timer` parameter to receive an acknowledgment. If the MAX receives no response, it sends another request and waits for twice the amount of time it waited after the first attempt, that is, twice what is specified in the `PPP conf req timer` parameter.

If the second attempt fails, the MAX sends a request and waits for four times the amount of time specified in the `PPP conf req timer` parameter. The MAX repeats the retries as specified in the `Max PPP conf req retry` parameter, up to the value specified in the `Max PPP conf req timer` parameter. The MAX does not wait any longer than the value you specify in the `Max PPP conf Req timer` parameter.

Parameter	Setting
`Max PPP conf req retry`	A number from 0 to 255. Specify the number of retries allowed, if LCP/NCP fails.
`PPP conf req time`	A number from 0 to 65535. Specify the initial LCP/NCP restart timer, in 1/100 of a second. This timer doubles each the LCP/NCP config request fails.
`Max PPP conf req timer`	A number from 0 to 65535. Specify a maximum LCP/NCP restart timer, in 1/100 of a second.

For example, the following parameters are set to these values:

```
Max PPP conf req retry=10

PPP conf req timer=100

Max PPP conf req timer=300
```

The MAX unit sends a request and waits for the time specified in the `PPP conf req timer` parameter—100 X .01 second, or 1 second. If there is no acknowledgement, the unit sends another request. The unit then waits for either 2 seconds (100 x 2 X .01, that is, doubling the amount of time in specified by the `PPP conf req timer` parameter) or for the value set in the `Max PPP conf req timer` parameter, whichever is less.

If there is no acknowlegment after the second attempt, the MAX unit sends another request. The unit continues to attempt to send the request for the number of times

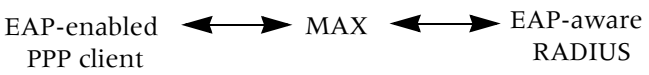
specified by the `Max PPP conf req retry` parameter. In the example, it continues to try to connect up to eight more times for a maximum of ten attempts.

Callback Control Protocol (CBCP) now only uses `PPP conf req timer` value as the initial time-out value for a CBCP connection request. If the request fails, it does not follow the doubling of the timer for regular PPP as described above. The time-out value set in the `PPP conf req timer` parameter remains the same for the entire set of retries.

Support for PPP Extensible Authentication Protocol (EAP)

With this release, the MAX 6000 implements Extensible Authentication Protocol (EAP) in the MAX for PPP sessions (RFC 2284, *PPP Extensible Authentication Protocol*). The TAOS implementation also requires RADIUS authentication to be enabled and configured on the MAX (RFC 2869, *RADIUS Extensions*).

When you use an EAP-aware RADIUS server for authentication, this new capability allows an EAP-enabled PPP client to successfully authenticate on a MAX.



When you want to use Extensible Authentication Protocol on the MAX, set the Recv Auth parameter to the new value: EAP. This parameter is located in `Ethernet` > `Answer` > `PPP options`.

Reference Entries

Following are the Reference entries supporting features in this release.

`Alarm Clear Table Limit`

Description Specifies the maximum number of alarms that the `alarmClearTable` can contain.

Usage Specify a number from 1 to 200. The default is 100.

Example `Alarm Clear Table Limit = 150`

Dependencies If the `SNMP Traps` profile is disabled (Active is set to `No`), the alarms in both the `alarmActiveTable` and `alarmClearTable` are removed. The `alarmModelTable` remains with `RowStatus` set as `NOT_IN_SERVICE`. The`alarmModelTable` is removed when the `SNMP Traps` profile is deleted.

Location `Ethernet > Mod Config > SNMP Options`

DTMF Tone Passing

Description Enables DTMF tone passing using RTP packets. The payload type can either be fixed (94) or be configured through dynamic payload type (such as for SIP).

Example `DTMF Tone Passing = rfc2833`

Dependencies This parameter is available when `Pkt Audio Mode` is set to `g728`, `g723`, or `g723-6.4kps` only.

Location `Ethernet > Mod Config > VOIP Options`

Enable Adaptive Jtr Buf

Description Enables the adaptive jitter buffer that optimizes the jitter buffer for both delay and voice quality.

Example `Enable Adaptive Jtr Buf = Yes`

Dependencies This parameter is available when `Pkt Packet Mode` is set as `g728`, `g723`, `g723-6.4kps`, or `FRGSM` only.

Location `Ethernet > Mod Config > VOIP Options`

Extended CLID

Description Enable sending of the presentation and screening indicators (Octet 0x3a) in the Q.931 Setup messages over H.225 as part of the Calling Party Number information element" Boolean field, `No` or `Yes`.

The default value is `No`.



Note Due to the way the CLID is decoded in the earlier implementation the extended CLID option defaults to 'no'. Where this option is enabled and the receiving GW does not support decode of the extended CLID the CLID will not be decoded correctly. Therefore this feature may only be switched on when the receiving gateway correctly decodes the setup message

Permission level

Usage `Extended CLID=[Yes|No]`

Example `Extended CLID=Yes`

Location `Ethernet > Mod Config > Voip Options`

See Also `Tx CLIR flag`

FRGSM Enabled

Description Enables FRGSM codec. Valid values are `Yes` (default) or `No`.

Example `FRGSM Enabled = Yes`

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

FRGSM Fpp

Description Sets the number of voice frames per RTP packet for FRGSM codec. Valid values are whole numbers from 1-10. The default value is 2.

Example `FRGSM Fpp = 10`

Dependencies FRGSM codec must be enabled.

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

G711 U Law Enabled

Description Enables G.711 u-law codec. Valid values are `Yes` (default) or `No`.

Example `G711 U Law Enabled = Yes`

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

G711 U Law Fpp

Description Sets the number of voice frames per RTP packet for G.711 u-law codec. Valid values are whole numbers from 1 through 10. The default value is 2.

Example `G711 U Law Fpp = 4`

Dependencies G.711 ulaw codec must be enabled.

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

G711 A Law Enabled

Description Enables G711 a-law codec. Valid values are `yes` (default) or `no`.

Example `G711 A Law Enabled = Yes`

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

G711 A Law Fpp

Description Sets the number of voice frames per RTP packet for G711 a-law codec. Valid values are whole numbers from 1-10. The default value is 2.

Example `G711 A Law Fpp = 9`

Dependencies G.711 alaw codec must be enabled.

Location `Ethernet > Mod Config > VOIP Options > Codec Options`

G723 Enabled

Description Enables G723 codec. Valid values are `yes` (default) or `no`.

Example G723 Enabled = Yes

Location Ethernet > Mod Config > VOIP Options > Codec Options

G723 Fpp

Description Sets the number of voice frames per RTP packet for G723 codec. Valid values are whole numbers from 1-10. The default value is 2.

Example G723 Fpp = 1

Dependencies G.723 coded must be enabled.

Location Ethernet > Mod Config > VOIP Options > Codec Options

G728 Enabled

Description Enables G.728 codec. Valid values are Yes (default) or No.

Example G728 Enabled = Yes

Location Ethernet > Mod Config > VOIP Options > Codec Options

G728 Fpp

Description Sets the number of voice frames per RTP packet for G.728 codec. Valid values are whole numbers from 1-10. The default value is 2.

Example G728 Fpp = 2

Dependencies G.728 codec must be enabled.

Location Ethernet > Mod Config > VOIP Options > Codec Options

G729 Enabled

Description Enables G.729 codec. Valid values are yes (default) or no.

Example G729 Enabled = Yes

Location Ethernet > Mod Config > VOIP Options > Codec Options

G729 Fpp

Description Sets the number of voice frames per RTP packet for G.729 codec. Valid values are whole numbers from 1-10. The default value is 2.

Example G729 Fpp = 5

Dependencies G.729 codec must be enabled.

Location Ethernet > Mod Config > VOIP Options > Codec Options

Grp B No Charge Signal

Description This is the default subscriber line-free no-charge signal. Some national specific R2 specifications allow for a group B response of `subscriber line-free` and the subscriber line should not be charged a toll. If this signal is received from the far end switch at the egress gateway, this field detects the `no charge` signal at the egress gateway and generates the `no charge` response at the ingress gateway in the VoIP `true setup status` configuration. If `True Setup Status` is not enabled, all R2 calls will be acknowleged by the `Group B Answer Signal` regardless of the actual signal received at the egress gatweway. This parameter is checked dynamically during the R2 signaling stage of the call. Changes to this parameter occur instantaneously.

Usage Use this parameter to select he group B signal to send if subscriber line is `idle` or `no charge`. Choose from the values below:

- `B-1`
- `B-2`
- `B-3`
- `B-4`
- `B-5`
- `B-6`
- `B-7` (default)
- `B-8`
- `B-9`
- `B-10`
- `B-11`
- `B-12`
- `B-13`
- `B-14`
- `B-15`

Location `E1 > Line Interface`

HairpinTrnkGrp

Description The trunk group to route hairpin calls. Trunk groups must be enabled in the `System` profile and configured in `T1/E1` profile. The `HairpinTrnkGrp` can have a value from 0 through 9999. The default value is 0.

Example `HairpinTrnkGrp=9`

Dependencies The HairpinTrnkGrp is used only when the following is set in `System > Sys Config`

`Use Trunk Grps=Yes`

`Num Trunk Digits=1`

`Num Trunk Digits` indicates the number of valid digits in the `HairpinTrnkGrp`.

Location `Ethernet > Mod Config > VOIP Options`

Hello Policy

Description Specifies whether a TAOS unit sends L2TP Hello messages to its peer based on an inactive control channel or inactive control and data channels.

Usage Specify one of the following values:

- `No Ctrl Activ` (the default)—The TAOS unit sends a periodic Hello Message only if the control channel is inactive.
- `No Activity`—The TAOS unit sends periodic Hello messages only if the control channel and all associated data channels are inactive.

Example `Hello Policy = No Activity`

Dependencies Consider the following:

- The `Hello Policy` parameter is not applicable if L2TP is not active on the unit.
- Changes to the `Hello Policy` parameter take effect after the period specified by the `Hello Timer` parameter.
- To disable the unit from sending Hello packets to its peer, set the `Hello Timer` parameter to zero (`0`).

Location `Ethernet > Mod Config > L2 Tunneling Options > L2TP Config`

Log Tunnel Progress

Description Specifies whether `syslog` messages generated while the unit is processing a Layer 2 Tunneling Protocol (L2TP) call are sent to the `syslog` server.

Usage Specify one of the following settings:

- `Yes` (the default) specifies that L2TP `syslog` messages are sent to the `syslog` server.
- `No` specifies that L2TP syslog messages are not sent to the `syslog` server.

Example `Log Tunnel Progress = No`

Location `Ethernet > Mod Config > Log`

Max PPP conf req retry

Description Specifies the number of retries allowed if Link Control Link Protocol (LCP)/Network Control Protocol (NCP) fails.

Usage Specify a number from 0 to 255.

Example Max PPP conf req retry=5

Location `Ethernet > Answer > PPP Options`

See Also `Max PPP conf req timer, PPP conf req timer`

Max PPP conf req timer

Description Specifies the maximum Link Control Link Protocol (LCP)/Network Control Protocol (NCP) restart timer in 1/100th of a second.

Usage Specify a number from 0 to 65535.

Example Max PPP conf req timer=100

Location `Ethernet > Answer > PPP Options`

See Also `Max PPP conf req retry, PPP conf req timer`

PPP conf req timer

Description Specifies the initial Link Control Link Protocol (LCP)/Network Control Protocol (NCP) restart timer in 1/100th of a second. This timer doubles each time a LCP/NCP configuration request fails.

Usage Specify a number from 0 to 65535.

Example PPP conf req timer=100

Location `Ethernet > Answer > PPP Options`

See Also `Max PPP conf req timer, Max PPP conf req retry`

RTPQoS Polling Enable

Description Enables the collection of statistics for both directions of calls are exchanged through RTP header extentions. The information is then available to a call logging (CL) server at the end of each call.

Example `RTPQoS Polling Enable = yes`

Dependencies This parameter is available when `pkt Audio Mode` is set as `g728`, `g723`, `g723-6.4kps`, or `FRGSM` only.

Location `Ethernet > Mod Config > VOIP`

TOS

Description Specifies the Type of Service (TOS) for the data stream.

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

- `Normal` specifies normal service (the default).
- `Cost` minimizes monetary cost.
- `Reliability` maximizes reliability.
- `Throughput` maximizes throughput.

- `Latency` minimizes delay.

Example `TOS = cost`

Dependencies The MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP and TOS Copying to No. Also, you must set TOS Enabled to Yes and TOS Mark Type set to Precedence-TOS.

Location `Ethernet > Connections > *any connection profile* > Tunnel options`

See Also `Tunnel protocol, TOS Copying, TOS Filter, TOS Enabled, TOS Mark Type, TOS DSCP, TOS Precedence`

TOS Copying

Description Specifies whether the type of service (TOS) byte is copied.

Usage Specify one of the following settings:

- `Yes` specifies that the unit copies the TOS byte from the inner IP header.
- `No` (the default) specifies that the unit does not copy the TOS byte from the inner IP header, but sets the TOS byte in the outer IP header to 000.

Example `TOS Copying = Yes`

Dependencies TOS copying might not be possible if the connection uses compression, encryption, Multilink PPP (MP), or Multilink Protocol Plus (MP+). Also, the MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP.

Location `Ethernet > Connections > any connection profile > Tunnel options`

See Also `Tunnel protocol, TOS Filter, TOS Enabled, TOS Mark Type, TOS DSCP, TOS Precedence, TOS`

TOS DSCP

Description Specifies the Differentiated Services Code Point (DSCP) value.

Usage Specify a value from `00` through `3F` (hexadecimal). DSCP marking, as defined in RFC 2474, uses the first six bits in the second octet in the IP datagram to create values (from `00` through `3F`) specifying different classes of service:

Bit positions	TOS-precedence (RFC 791) indication	DSCP (RFC 2474) indication
0-2	Precedence (8 levels of priority)	DSCP value
3	Delay (normal or low)	DSCP value (continued)
4	Throughput (normal or high)	DSCP value (continued)
5	Reliability (normal or high)	DSCP value (continued)
6-7	Reserved	Reserved

Example DSCP = 3F

Dependencies Consider the following:

- For DSCP to apply, you must set TOS Mark Type to DSCP.
- The full byte (8 bits) of the DSCP field can be specified and will be set in the IP type of service (TOS) byte of the IP header. Even though only the most significant 6 bits are used and matched to select a per-hop behavior (PHB) by the differentiated services (DS) domains in the network, the system is flexible so that you can set the entire 8 bits in any desired way and experiment with the two unused bits.

Location Ethernet > Connections > *any connection profile* > Tunnel options

See Also Tunnel protocol, TOS Copying, TOS Filter, TOS Enabled, TOS Mark Type, TOS Precedence, TOS

TOS Enabled

Description Enables static, policy-based DSCP marking and remarking of the outer header, based on the DSCP value of the inner header.

Usage Specify one of the following settings:

- Yes specifies that the unit enables DSCP marking and remarking of the outer header.
- No (the default) specifies that the unit does not enable DSCP marking and remarking of the outer header.

Example TOS Enabled = yes

Dependencies The MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP and TOS Copying to No.

Location Ethernet > Connections > *any connection profile* > Tunnel options

See Also Tunnel protocol, TOS Copying, TOS Filter, TOS Mark Type, TOS DSCP, TOS Precedence, TOS

TOS Filter

Description Specifies the number of a filter profile that defines a type of service (TOS) filter.

Usage Specify the number of a defined profile. The default is 0.

Example TOS Filter = 3

Dependencies The MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP and TOS Copying to No.

Location Ethernet > Connections > *any connection profile* > Tunnel options

See Also Tunnel protocol, TOS Copying, TOS Enabled, TOS Mark Type, TOS DSCP, TOS Precedence, TOS

TOS Mark Type

Description Specifies how TAOS uses the first six bits in the second octet of the IP header to indicate the precedence and type of service (TOS) of the packet.

Usage Specify one of the following settings:

- Precedence-TOS (the default) specifies RFC 791 as the standard to differentiate class of service.
- DSCP specifies differentiated services code point (DSCP) marking, as defined in RFC 2474.
- DSCP-Remarking specifies differentiated services code point (DSCP) remarking

Example TOS Mark Type = DSCP

Dependencies The MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP and TOS Copying to No. Also, you must set TOS Enabled to Yes.

Location Ethernet > Connections > *any connection profile* > Tunnel options

See Also Tunnel protocol, TOS Copying, TOS Filter, TOS Enabled, TOS DSCP, TOS Precedence, TOS

TOS 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 to one of the following values (most significant bit first):

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

Example TOS Precedence = 001

Dependencies The MAX 6000 must support the L2TP software option, and you must set Ethernet > Connections > any connection profile > Tunnel option > Tunnel protocol to L2TP and TOS Copying to No. Also, you must set TOS Enabled to Yes and TOS Mark Type set to Precedence-TOS.

Location Ethernet > Connections > *any connection profile* > Tunnel Options

See Also Tunnel protocol, TOS Copying, TOS Filter, TOS Enabled, TOS Mark Type, TOS DSCP, TOS

True Setup Status

Description This parameter is checked dynamically during the R2 signaling stage of the call. Changes to this parameter are immediate. For E1 interregister signaling, this parameter is valid from the beginning of the R2 call session. For all other interaction, True Setup Status can be changed dynamically. This feature is expected to be used with Single Dial Enabled and vpnMode since the far-end setup status cannot be returned to the caller if input digits are requested.

Usage Select the following:
Yes to enable this feature
No to disable this feature

Example `True Setup Status = Yes`

Dependencies Parameters that affect True Setup Status in the VOIP profile:

Single Dial Enabled	Single Dial Enabled must be set to yes on the ingress gateway.
True Connect Enabled	true connect allows the call to call to be answered at the near end when the far-end outbound call has been answered. If disabled, the call will be answered at the near end when the 'alerting' is seen from the far-end terminal as opposed to immediately
Signaling Model	This parameter provides the line signaling call progress on a call setup depending on the H323 call state or the actual line signaling status. Signaling is send from the outbound gateway to the inbound gateway. The settings are as follows: n Fast Proceeding This is the recommended setting for a virtual R2 connection since the delay associated with interregister signaling in this model is not ideal for the H323 response timing. n Early Alerting Use this setting only for non-ISDN and non-R2 gateways. n Slow Proceeding Signals proceeding upon inband call progress and any subsequent alerting received by the egress gateway triggers alerting, which in turn causes the R2 to proceed and alert the near-end.

`Single Dial Enabled`	`Single Dial Enabled` must be set to `yes` on the ingress gateway.
`Cause Code Enabled`	This parameter is found in the `PSTN Options` subprofile. Set to `true` to translate correctly from Q.931 disconnect cause codes into the R2 group B connection failure codes. Failed calls default to the `congestion` cause code (equivalent to the CCITT B-4 signal) for cause codes not sent transparently from the ISDN through the H.323/H.225/Q.931. This is useful for ingress R2 and egress ISDN gateway setups.

Parameters that affect `True Setup Status` in the `E1 > Line Interface` profile:

`Grp B Answer Signal`	Use this for the default if the far-end is not an R2 trunk or the `line-idle charge/no charge indeterminate` signal is to be sent. This is used on the line-idle (national line idle usually expressed as B-1 (not CCITT)) or line idle charge (equivalent to CCITT B-6)).
`Grp B Busy Signal`	Use this for the default `setup failed` signal if the far-end is not an R2 trunk. This is usually either subscriber line busy (equivalent to CCITT B-3) or trunk congestion (equivalent to CCITT B-4).
`Grp B No Match Signal`	Use this signaling tone to reject a call to a vacant number. This should normally be the mapping for a disconnect with cause code 1 (`Unassigned Number`) or the mapping of the far-end group B signal `vacant number` (equivalent to CCITT B-5)
`Grp B Collect Signal`	Use this signal in response to a `reverse tolling` or `collect call` signal. The charge will taken at the near end gateway.
`Grp II Signal`	This is the default signaling tone used for the calling party class.

Location `Ethernet > Mod Config > Voip Options`

Tunnel protocol

Description Specifies the type of tunneling protocol the MAX unit uses to establish a tunnel.

Usage Specify one of the following values:

- `ATMP` (the default)—Ascend Tunnel Management Protocol
- `IPINIP`—IP-in-IP Tunneling Protocol
- `PPTP`—Point-to-Point Tunneling Protocol
- `L2F`—Layer 2 Forwarding
- `L2TP`—Layer 2 Tunnel Protocol

Example Tunnel protocol=L2TP

Location Ethernet>Mod Config>any Connection profile>Tunnel options

See Also ATMP HA RIP, Client ID, Home Network Name, Max Tunnels, Password, Pri. Tunnel Server, Profile Type, Sec. Tunnel Server, Tunnel VRouter, UDP Port

Tx CLIR flag

Description This option controls whether the CLIR flag from the original Q.931 setup message will be transmitted in egressing voip calls on this line. This optional field will NOT be passed in Q.931 unless this field is set to 'yes'. By default this field will be 'no'. Boolean field, 'no' or 'yes'

The default value will be 'no'.



Note Although there should be no side effects in enabling this option to transmit this flag over the outgoing setup message this value defaults to 'no' to ensure that only users who require this will see any change in operation.

Permission level

Usage Tx CLIR flag=[Yes|No]

Example Tx CLIR flag=Yes

Location Net/T1 > Line Config > Line *N*; Net/E1 > Line Config > Line *N*

See Also Extended CLID

Change requests in TAOS 10.1 4

Table 4-1describes the change requests that are included in TAOS 10.1.

Table 4-1. Customer requests fulfilled in TAOS 10.1 (page 1 of 2)

Change request number	Description
6002142	Max 6000 displayed problems with Brazil R2 implementation
6002378	Max 6000 supporting AODI did not supply attribute 5 (NAS-Port) in Accounting start and stop request packets.
6002416	MAX TNT running 8.0.4: packets cause accounting server timeout
6006867	Max 6000 running 9.1.2 failed to support Ascend-Private-Route.
7006440	MAX6000 loaded with software version 8.0.4 occasionally reset displaying a Fatal Error 8
7006648	MAXTNT-Framed-IPX-Network value is reversed when sending the accounting start packet
7006666	Wanopen debug does not end on L2 tunnel calls
7006894	Max supporting Telnet to incoming X.75 and V.120 users occasionally resets, generating a Fatal Error 2 message.
7006913	Occasionally, Max6000 exhibited negative packet counters after several months of uptime.
7006934	MIF command `set 000.DIAG.0.UPD REM CFG=Yes` always results in `+ERROR`.
7007027	V.90 S56 III Modem-24 slot card failed to accept calls successfully, generating a Warning 195 message.
7007223	Max unit fails to refresh some Frame Relay parameters after a reset.
7007323	When a MAX 6000 unit started and registered, the unit sent a Service Change Request on all DS0 physical terminations with their current service state rather than to only those that were not in service.
7007333	MAX unit incorrectly sends RADIUS Accounting Log "Acct-Link-Count =0" for MP sessions

Table 4-1. Customer requests fulfilled in TAOS 10.1 (page 2 of 2)

Change request number	Description
7007351	TNT rejected an incoming v.120 call at the ISDN level, when the incoming Q.931 Setup message contained v.120 Bearer Capatibility and Low-Layer Compatibility (LLC) information.
7007513	A MAX 6000 unit's SWAN interface was unavailable.
7007572	MultiDSP cards fail to synchronize with lower V.34 symbol rates.
7007637	Max6000 failed to connect when dialing a 3rd party router and using RADIUS and Bidirectional CHAP authentication. The user profile (followed 8.0.1 release notes) was configured for single lookup, but was failing due to the Max 6000 performning a second lookup.
7007897	Max6000 with Telnet mode set to ASCII did not suppress bit-8 to 0 {zero}.
7008397	PPP IPNCP Negotation is failing between a third-party CPE router and unit installed with 10.0.x
7008442	The Watchdog MIB is not supported with some 10.0.x software loads.
7008500	The Max 6000 does not indicate a down T1/PRI correctly in the VT100 interface

Notices and Known Issues

5

Notice of end of sale for MAX 6000 units 5-1

Notice of TAOS license and upgrade changes 5-3

Support for voice DSP modules ends 5-4

Data and RAS known issues. 5-4

MultiVoice® known issues. 5-6

Following are notices and known issues for MAX 6000 units, voice DSP modules, MultiVoice® data and remote access server (RAS) services.

Notice of end of sale for MAX 6000 units

On July 26 of 2002, Lucent Technologies served a twelve (12) month notice of the End of Sale on the MAX 6000 product line. Orders for this product line will be accepted only until July 31, 2003 and will not be accepted thereafter.

The last TAOS software release to support the MAX 6000 platform will be 10.1.x. TAOS software loads released after 10.1.x will not be supported on the MAX 6000 platform. Software support will end one year after the posted end of sale (EOS) date. Due to the size of TAOS 10.1.x software release, an external DRAM memory card will be required for MAX 6000 units, which do not have an existing 32MB memory daughter card on the internal motherboard.

It is recommended that all future purchases of MAX 6000 units be the models with the 32MB memory daughter card.

Product Codes Impacted

Table 5-1 decribes product codes impacted by this notice.

Table 5-1. MAX 6000 unit product codes impacted by this notice

Product code	Comcode	Description
MX60-4E1-32-AC	300271566	MAX 6000 E1 with (1) AC power supply and 32MB DRAM card

Table 5-1. MAX 6000 unit product codes impacted by this notice

Product code	Comcode	Description
MX60-4E1-32-DC	300271574	MAX 6000 E1 with (1) DC power supply and 32MB DRAM card
MX60-4T1-32-AC	300271590	MAX 6000 T1 with (1) AC power supply and 32MB DRAM card
MX60-4T1-32-DC	300271582	MAX 6000 T1 with (1) DC power supply and 32MB DRAM card
MX60-4E1-AC	300075876	MAX 6000 E1 with (1) AC power supply
MX60-4E1- DC	300075884	MAX 6000 E1 with (1) DC power supply
MX60-4T1-AC	407929298	MAX 6000 T1 with (1) AC power supply
MX60-4T1-DC	407929306	MAX 6000 T1 with (1) DC power supply
MX60-4E1-2AC	300075850	MAX 6000 with (4) E1s and (2) AC power supplies
MX60-4E1-2DC	300075868	MAX 6000 with (4) T1s and (2) DC power supplies
MX60-4T1-2AC	407929280	MAX 6000 with (4) T1s and (2) AC power supplies
MX60-4T1-2DC	407929751	MAX 6000 with (4) T1s and (2) DC power supplies
N46R2-461	no comcode	IP28X/460 Center Router
MX60-T1AC-D48NA	300352911	48-Port T1 MAX 6000 Bundle with ISDN and FR software enabled
MX60-T1AC-D96NA	300352903	96-Port T1 MAX 6000 Bundle with ISDN and FR software enabled
MX60- E1AC-D60IX	300352937	60-Port E1 MAX 6000 Bundle with ISDN, FR and R2 software
MX60- E1AC-D120IX	300352929	120-Port E1 MAX 6000 Bundle with ISDN, FR and R2 software
MXV6-GWT-48-AC	300351566	48-Port T1 MAX 6000 Bundle with AC power
MXV6-GWT-48-2AC	300351574	48-Port T1 MAX 6000 Bundle Dual AC power
MXV6-GWT-48-DC	300351582	48-Port T1 MAX 6000 Bundle with DC power
MXV6-GWT-48-2DC	300351590	48-Port T1 MAX 6000 Bundle Dual DC power
MXV6-GWE-60-AC	300351608	60-Port E1 MAX 6000 Bundle with AC power
MXV6-GWE-60-2AC	300351616	60-Port E1 MAX 6000 Bundle Dual AC power
MXV6-GWE-60-DC	300351624	60-Port E1 MAX 6000 Bundle with DC power

Table 5-1. MAX 6000 unit product codes impacted by this notice

Product code	Comcode	Description
MXV6-GWE-60-2DC	300351632	60-Port E1 MAX 6000 Bundle Dual DC power
MX60-SPU-2T1	300076114	Software hash-code to remove (2) T1 restriction enabling 3 rd &4 th T1
MX60-SPU-2E1	300076106	Software hash-code to remove (2) E1 restriction enabling 3 rd & 4 th T1
MX-SL-48M-DSP	300331550	MAX MultiDSP 48 Port Card
MX-SL-60M-DSP	300331543	MAX MultiDSP 60 Port Card.
MX60-OSLIC	300350998	Base TAOS RTU software license for the MAX 6000

Replacement products

Replacement products might be priced higher than the products they replace. If so, existing contracts should be adjusted to reflect new prices. APX 1000 units are the replacement for MAX 6000 units.

Notice of TAOS license and upgrade changes

Starting with the release of TAOS 9.1, the following changes are now in effect for TAOS base software and TAOS software upgrades, service, and maintenance.

Price change for base TAOS software

With the release of TAOS 9.1, MAX 3000, MAX 6000, MAX TNT®, and APX 8000 hardware and TAOS software are priced separately. The TAOS software license is now a mandatory item for any new order. The license grants licensees the right to use the base TAOS 9.1 software on the specific platform purchased.

Note The right to upgrade to a subsequent TAOS minor or major software release that includes new operating system software enhancements is no longer included as part of the base TAOS software license.

Price change for upgrades and maintenance to TAOS 10.0 software

Upgrades to TAOS 10.0 software and subsequent releases for the MAX 3000, MAX 6000, MAX TNT®, and APX 8000 platforms are available through Lucent Worldwide Services as part of an annual software maintenance contract. These contracts are priced separately for each platform and include the following software and services:

- TAOS software updates, upgrades, and support
- TAOS software licenses (or *hash codes*), updates, upgrades, and support
- Remote technical support
- Hardware maintenance and return

Note Only customers with an established software maintenance contract are authorized to upgrade designated TAOS-enabled units to TAOS 10.0 and to download the required TAOS 10.0 software files.

Distribution change for TAOS 10.0 software

TAOS 10.0 and subsequent general-availability TAOS software releases are no longer available from `ftp.ascend.com`. Upgrades to TAOS 10.0 and all subsequent releases and updates (maintenance releases) are available instead from the Lucent OnLine Customer Support at `http://www.lucent.com/support`.

TAOS software license agreement change

Lucent Technologies is introducing a new software license agreement that grants you a personal, nontransferable, nonexclusive right to use TAOS 10.0 in object code form only, and its accompanying documentation. The agreement prohibits you from loading or using TAOS software on any unit of Lucent equipment other than the unit for which you purchased the software, unless otherwise agreed upon in writing by Lucent.

Use of TAOS software on any equipment other than that for which it was obtained, or any material breach of these conditions, immediately and automatically terminates the license. Lucent reserves the right to pursue all available legal remedies to enforce the terms and conditions of the software license.

Support for voice DSP modules ends

TAOS support for voice DSP modules ends on May 17, 2002. Until that time, only maintenance releases for TAOS 9.0 and TAOS 9.1 will include support for the voice-only modules. For example, TAOS 9.0.x and 9.1.x includes enhancements and problem corrections for voice DSP modules.

TAOS releases after the 9.1.x will not support voice DSP modules and no enhancements or problem corrections will be developed for them. However, later TAOS releases continue to provide MultiDSP modules with support for MultiVoice® Gateways, voice over IP, and fax over IP when the modules are installed in MAX 6000 or MAX 3000 units.

A voice DSP module's product warranty, repair, and technical support programs continue for the duration of existing contracts.

Data and RAS known issues

Data and remote access server (RAS) known issues you should be aware of before loading TAOS release 10.0.2 include the following:

- Always check a MAX 6000 unit's real-time clock settings, located in the `System > Sys Config` menu, immediately after the unit completes a power-on self test (POST).
- TAOS 10.0.2 for MAX 6000 unit does not support AppleTalk. Do not upgrade to TAOS 10.0.2 if your network requirements include support for AppleTalk.
- After you upgrade a MAX unit from the TAOS 8.0-118 Limited Availability Release to TAOS 10.0.2, you must reenter the settings you want to specify for the `Modem Ans N#` parameter (located in the `Call Numbers` profile). The unit

does not automatically transfer the values you previously specified for the parameter.

- The Call Logging packet format is changed.

  In releases prior to 7.2.0, the format of Call Logging packets is identical to RADIUS Accounting packets. With the introduction of 7.2.0, Call Logging is no longer compatible with RADIUS, although Lucent Technologies' NavisAccess™ product fully supports Call Logging. The MAX 6000 unit 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™ software.

- Some multimedia enhancements are not supported in TAOS 10.0.2. Customers using the following enhancements should not upgrade to TAOS 10.0.2:
  - 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 TAOS 10.0.2 is loaded.
- In an E1 environment, the MultiDSP module can exhibit a lower-than-expected call connection rate as it terminates modem calls placed to the MAX unit. Lucent Technologies recommends that you specify `S202=66+A8E=,,,0;` for the AT Answer String parameter, located in the unit's Sys Config profile.
- In MAX 6000 unit 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 6000 unit. 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 A traffic load of more than 64 digital (HDLC) calls requires an optional HDLC module, and no more than 96 digital calls are supported under any circumstances.

  The following table summarizes how the addition of BRI cards affects the availability of built-in WAN ports in various MAX 6000 unit units. These limits apply regardless of the type of BRI card used (Net, Host, IDSL, etc.).

Table 6.

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

Table 6.

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

MultiVoice® known issues

Known issues you should be aware of before upgrading a MAX 6000 unit include the following:

- A small percentage of calls might experience broken one-way voice path when using break-in announcements stored in G.729 format.
- Voice DSP and MultiDSP modules cannot coexist on the same MAX unit.
- When a MultiDSP module is used with the G.711 audio codec, you must set the `Frames-Per-Packet` parameter in the `VOIP Options` profile to a value of 4 or more.
- If one or more voice DSP modules (MXV-SL-DSP8, MXV-SL-DSP12, or MXV-SL-DSP16) are configured in a MAX 6000 unit, the Navis™ QOS and RFC 2833 features introduced with TAOS 10.0.2 are not supported.
- A MAX 6000 unit supports voice announcements that are stored on the external PCMCIA flash card. Break-in announcements, multiple languages, and the branding of voice announcements are supported on the unit.
- The maximum supported configuration for a MAX 6000 unit is two T1 PRI or two E1 PRI interfaces, 48 or 60 calls respectively.
- If you have a MultiDSP module in a MAX 6000 unit, and at least one card is configured to support MultiVoice® using simple audio codecs (for example, G.711), then all VoIP calls will be restricted to use simple audio codecs as well.
- The MAX 6000 unit no longer supports RT24 coding for packetization of voice.

Document Set

A

The MAX 6000 unit documentation set is available on the Documentation Library CD-ROM included with your MAX 6000 unit. You can order additional copies of the documentation on CD-ROM or paper from the online bookstore or you can view the documentation online. Go to `http://www.lucentdocs.com/ins` for more information about these options.

The MAX 6000 unit documentation set consists of the following manuals:

- *Edge Access and Broadband Access Safety and Compliance Guide*
- *MAX Administration Guide*
- *Hardware Installation and Basic Configuration Guide*
- *Network Configuration Guide*
- *MAX Reference*
- *TAOS Glossary*
- *TAOS RADIUS Guide and Reference*