Lucent Technologies
Bell Labs Innovations



# MAX™ 6000/3000 TAOS 10.0

Release Note

March 15, 2002
For software version: 10.0.0

**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 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

**Introducing TAOS 10.0 ..... 1**

What is in TAOS 10.0 ..... 1
Features organized by type ..... 1

**Changing operating system software ..... 4**

Enabling Field Service and Operations parameters ..... 4
Keeping the same software binary name ..... 5
Using TFTP to upgrade or downgrade ..... 5
- Creating redundant backup images for a MAX 6000 unit ..... 5
- Using TFTP to upgrade a MAX 3000 unit ..... 6
- Using TFTP to upgrade a MAX 6000 ..... 8
- Using TFTP to upgrade a MAX 6000 for MultiVoice® binaries ..... 9
- Using TFTP to downgrade ..... 10

Using the serial port to upgrade or downgrade ..... 11
- Saving the current system configuration ..... 12
- Upgrading system software ..... 12
- Restoring the configuration ..... 12
- Downgrading the software ..... 13
- Restoring passwords ..... 14

**Firmware versions ..... 14**

**New WAN access features ..... 15**

Two new disconnect cause codes introduced ..... 15
Enhanced support for the V.92 protocol in the MAX VT100 interface added ..... 15
- New `modem-on-hold` parameter added to `Connections` profiles ..... 16
- New and modified V.92 parameters in the `TServ options` menu ..... 17
- Using SNMP to specify values for V.92 and V.44 parameters ..... 19
- Using RADIUS to specify a modem-on-hold value ..... 20

MultiDSP MAX slot card support for V.110 added ..... 20
MultiDSP MAX slot card support for PHS added ..... 20
X.28 PAD login modified ..... 20
- New terminal server security mode ..... 20
- New POS Auth parameter for terminal server security mode ..... 21
- Configuring the X.121 source address for X.25 PAD calls ..... 21

Number of characters in of Recv Name parameter value field increased ..... 22
Support for Vietnamese R2 signaling added ..... 22
Support for multiple compression protocols added ..... 22
Manual control of Ethernet modes added ..... 23

New Parameters ..... 23

**New Tunneling features ..... 24**

New traps added to indicate L2TP tunnel failure and deactivation ..... 24
New trap definitions ..... 24
Enabling L2TP traps ..... 25
Limitation on the number of calls processed by an L2TP tunnel added ..... 25
New `Max Calls per Tunnel` parameter specifies a maximum number of calls per tunnel ..... 26
New SNMP commands can specify a maximum number of calls per tunnel ..... 27
MAX unit support for IP fax removed ..... 27
New Suppress Endpoint Disc parameter to disable end-point discriminators added ..... 27
New `Data PKT UDP` parameter to disable L2TP packet checksum added ..... 28

**New RADIUS features ..... 28**

Two new parameters that report NAS port type to RADIUS accounting added ..... 28
Support for the `Port Type List (44)` vendor-specific attribute-value pair added ..... 30
Nonzero IP address reporting for all channels added to accounting records ..... 31
NAS-identifier support added to request packets ..... 31
Outgoing attributes support added to `diag radif` command ..... 31
Using the `level` option ..... 32
Support for disabling RADIUS accounting and call logging for VoIP calls added ..... 33
New Voip Accounting and Voip Call Logging parameters added ..... 33
`Event-Timestamp (55)` attribute added to RADIUS accounting requests ..... 33
Session timeouts and new `syslog` message added for L2TP, PPTP, and L2F calls ..... 34
Specifying the amount of time before an idle call is disconnected ..... 34
Specifying the maximum amount of time for a call ..... 34
New `syslog` message ..... 35
New RADIUS `NAS-Port` attribute value ..... 35
New NASPort Format parameter added ..... 35
RADIUS changes ..... 35

**New SNMP features ..... 35**

New traps indicating L2TP tunnel failure and deactivation added ..... 35
New trap definitions ..... 36
Enabling L2TP traps ..... 37

**New IP routing features ..... 37**

New command that temporarily disables IP addresses listed in address pools added ..... 37

**Problems corrected in TAOS 10.0 ..... 38**

**Notices and known issues ..... 40**

Notice of end of sale for MAX Slot card ..... 40
Product codes impacted ..... 41
Replacement products ..... 41
Notice of end of sale for MAX 3000 ..... 42
Product codes impacted ..... 42
Replacement products ..... 43

Notice of TAOS license and upgrade changes ..... 43
Price change for base TAOS software ..... 43
Price change for upgrades and maintenance to TAOS 10.0 software ..... 43
Distribution change for TAOS 10.0 software ..... 44
TAOS software license agreement change ..... 44
Support for voice DSP modules ends ..... 44
Data and RAS known issues ..... 44
MultiVoice® known issues ..... 46

# Introducing TAOS 10.0

**Note:** The MAX™ 3000 unit is no longer supported as a MultiVoice® Gateway. The MAX 6000 unit continues be the platform in the MAX family that can operate as a MultiVoice® Gateway.

The True Access™ Operating System (TAOS) runs on the advanced WAN access products of Lucent Technologies. These products provide modular chassis that integrate a range of technologies to enable service providers and enterprise managers to install customized network infrastructures. As new enhancements are added to TAOS, the amount of memory used by the operating system grows. Therefore, the products running later versions of TAOS report less available memory. When you install TAOS 10.0 you see a smaller amount of available memory on the MAX than was available to a unit that ran a previous TAOS release. This is because the software binaries have gotten bigger and the memory used to store those software binaries is greater.

## *What is in TAOS 10.0*

Following are the sections that describe what is in TAOS 10.0:


- "Features organized by type" on page 1
- "Changing operating system software" on page 4
- "Firmware versions" on page 14
- New features in TAOS 10.0 beginning with "New WAN access features" on page 15
- "Problems corrected in TAOS 10.0" on page 38
- "Notices and known issues" on page 40


## *Features organized by type*

TAOS 10.0 includes the following types of features:

- WAN access
- Tunneling
- RADIUS
- SNMP
- IP Routing

Where available, a feature identification (FID) is included.

## WAN access

The following table lists the WANaAccess features included in TAOS 10.0.

| FID | Description |
|---|---|
| NA | "Two new disconnect cause codes introduced" on page 15 |
| NA | "Enhanced support for the V.92 protocol in the MAX VT100 interface added" on page 15 |
| NA | "MultiDSP MAX slot card support for V.110 added" on page 20 |
| NA | "MultiDSP MAX slot card support for PHS added" on page 20 |
| NA | "X.28 PAD login modified" on page 20 |
| 510545 | "Number of characters in of Recv Name parameter value field increased" on page 22 |
| 510616 | "Support for Vietnamese R2 signaling added" on page 22 |
| 510633 | "Support for multiple compression protocols added" on page 22 |
| 261301 | "Manual control of Ethernet modes added" on page 23 |

## Tunneling

The following table lists the tunneling features included in TAOS 10.0.

| FID | Description |
|---|---|
| NA | "New traps added to indicate L2TP tunnel failure and deactivation" on page 24 |
| NA | "Limitation on the number of calls processed by an L2TP tunnel added" on page 25 |
| 261409 | "MAX unit support for IP fax removed" on page 27 |
| 510566 | "New Suppress Endpoint Disc parameter to disable end-point discriminators added" on page 27 |
| 510571 | "New Data PKT UDP parameter to disable L2TP packet checksum added" on page 28 |

## RADIUS

The following table lists the RADIUS features included in TAOS 10.0.

| FID | Description |
|---|---|
| NA | "Two new parameters that report NAS port type to RADIUS accounting added" on page 28 |
| NA | "Support for the Port Type List (44) vendor-specific attribute-value pair added" on page 30 |
| NA | "Nonzero IP address reporting for all channels added to accounting records" on page 31 |
| 261230 | "NAS-identifier support added to request packets" on page 31 |
| 261250 | "Outgoing attributes support added to diag radif command" on page 31 |
| 261438 | "Support for disabling RADIUS accounting and call logging for VoIP calls added" on page 33 |
| 510572 | "Event-Timestamp (55) attribute added to RADIUS accounting requests" on page 33 |
| 510647 | "Session timeouts and new syslog message added for L2TP, PPTP, and L2F calls" on page 34 |
| 510680 | "New RADIUS NAS-Port attribute value" on page 35 |

## SNMP

The following table lists the SNMP feature included in TAOS 10.0.

| FID | Description |
|---|---|
| NA | "New traps indicating L2TP tunnel failure and deactivation added" on page 35 |

## IP routing

The following table lists the IP routing feature included in TAOS 10.0.

| FID | Description |
|---|---|
| NA | "New command that temporarily disables IP addresses listed in address pools added" on page 37 |

# Changing operating system software

**Caution:** When you upgrade a MAX 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) 10.0 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. The MAX 3000 unit does not require an external PCMCIA flash card.

**Caution:** If possible, change a MAX unit's version of TAOS by using TFTP. Refer to "Using TFTP to upgrade or downgrade" on page 5 for further details.

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

## *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 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 10.0, 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 TAOS 10.0 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 unit might have a T1 interface. If you are attempting to transfer a build that is appropriate for an E1 interface, the MAX unit can display the following message:

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

When the build is intended for 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 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 unit now supports two copies of TAOS code. If the first version of software code becomes corrupted, the MAX 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 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 3000 unit



**Caution:** If you are upgrading from a TAOS release prior to 9.0.2, you must first upgrade to the 9.0.2 version using the steps below. In step 4 on page 7, ensure that the file name used for 9.0.2 is the same software binary file as is currently loaded. Refer to the `Sys Options` menu to find that software binary file. Then, repeat the steps to upgrade to 10.0 from 9.0.2 using a software binary file.

Since the MAX 3000 unit does not require an external PCMCIA flash card, you will use the unit's internal flash memory to upgrade to the 10.0 version of TAOS. The internal flash on a MAX 3000 provides automatic redundant support, so if you load a bad image, the unit will revert to the other saved image on the internal flash. No action is required by the user.

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

To upgrade system software 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 configuration used for TAOS 8.0.3 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 unit's internal flash storage is limited. Use the `tsave -m` command to ensure 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 10.0. The file you save with the `tsave` command contains all the passwords in clear text. Move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

**4** Enter the following command to load the software binary:

```
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 ebiv.m30
```

places `ebiv.m30` into flash from the machine named `tftp-server`.

**5** 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 3000 via telnet.

**6** 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 10.0.

## Using TFTP to upgrade a MAX 6000

**Note:** The following upgrade steps assume you have not used the MultiVoice® binaries to upgrade to release 10.0. If you used the MultiVoice® binaries, you must downgrade to a previous TAOS release (see "Using TFTP to downgrade" on page 10) 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 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 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 10.0. The file you save with the `tsave` command contains all the passwords in clear text. Move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4. Enter the following command:

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

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

   For example, the command

   **`tloadcode tftp-server ebixk.m60`**

   places `ebixk.m60` into external flash from the machine named `tftp-server`.
5. 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.
6. 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 10.0.

## 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. The MAX 3000 unit does not have an external PCMCIA flash 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 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 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 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 10.0. 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 10.0), your configuration might be corrupted.

This completes the procedure for upgrading to TAOS 10.0.

## 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 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 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 5.)

**Note:** The MAX 3000 currently does not support download via the serial console port.

**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 10.0 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 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 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 10.0.

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.

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

After the file transfer, the MAX 6000 unit resets. 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.

# Firmware versions

TAOS 10.0 supports the following firmware versions:

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

V.90 Series56 III modules—Mindspeed Technologies firmware version V5.8175 includes support for K56flex, K56plus, and all slower, standard modem speeds.

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

- V0.1.66 (Controller)
- V0.1905.0 (RAS)
- V3.0.51 (VoIP)

# New WAN access features

## Two new disconnect cause codes introduced

There are now two new disconnect cause codes in the `Syslog` output for V.92 calls terminated on a MAX unit's installed MultiDSP modules:

- `80`—Indicates a client modem disconnected while a MAX unit attempted to place the session on hold or while a unit kept the session on hold. This new code relates to the unit's support for the V.92 modem-on-hold feature.
- `81`—Indicates a client modem disconnected by sending a Link Access Protocol for Modems (LAPM) error correction disconnect frame.

For example, the progress code of `40` combined with the new disconnect cause code `80` in the following `Syslog` output indicates that a terminal-server session was started and the client modem disconnected while the MAX unit attempted to place the session on hold.

```
June 22 12:00:00 example.lucent.com Conn=("?" 8885551212->4707
? 49333/28800 40/80) Auth=(26 0/0 0/
0) Sess=(4 0/0 0/0) Chan=(0 1 1 19) Modem=(0 6 7) [MBID 7]
```

A `Syslog` output with a progress code of `40` combined with the new disconnect cause code `81` indicates that a terminal-server session started and then the client modem disconnected by sending a LAPM error correction disconnect frame.

```
June 22 12:00:00 example.lucent.com Conn=("?" 8885551212->4707
? 49333/28800 40/81) Auth=(31 0/0 0/
0) Sess=(8 3/0 78/0) Chan=(0 1 1 15) Modem=(0 6 3) [MBID 3]
```

## Enhanced support for the V.92 protocol in the MAX VT100 interface added

TAOS 10.0 enhances support for the MAX unit's VT100 interface for V.92 dial-up modem and V.44 link-layer compression standards. V.92 and V.44 features are supported by MAX units with installed MultiDSP modules.

TAOS 10.0 makes the following changes to the MAX unit's VT100 interface:

- Adds a modem-on-hold parameter to `Connections` profiles
- Adds four parameters to the `TServ options` menu
- Modifies one parameter in the `TServ options` menu

You can change the settings for the parameters added or modified by TAOS 10.0 using a Simple Network Management Protocol (SNMP) manager.

You can use the Remote Authentication Dial-in User Service (RADIUS) attribute `Ascend-MOH-Timeout` attribute to specify a value for a `MDMonHold` parameter, located in any `Connections` profile.

## New `modem-on-hold` parameter added to `Connections` profiles

The `MDMonHold Timeout` parameter, added to `Connections` profiles, specifies whether a client modem can place a MAX unit on hold and the maximum duration that a client modem can place a MAX unit on hold. You can specify one of the following values:

- `Disabled (the default)`
- `10 Sec`
- `20 Sec`
- `30 Sec`
- `40 Sec`
- `1 Min`
- `2 Min`
- `3 Min`
- `4 Min`
- `6 Min`
- `8 Min`
- `12 Min`
- `16 Min`
- `Use global`

By specifying any value other than `Use global` for the `MDMonHold Timeout` parameter in any `Connections` profile, you can override the value specified in the TServ Options menu. For example, you might specify `1 Min` for the `MDMonHold Timeout` parameter in a `Connections` profile so the client modem can place a MAX unit on hold for one minute before the unit disconnects. The unit does this even though the `MDMonHold Timeout` parameter located in the `TServ options` menu specifies `Disabled`. Conversely, a `Connections` profile might disable a modem-on-hold timeout though the `TServ options` menu specifies a value.

Once the specified time limit passes, the unit disconnects the session. Following is an example of a `Connections` profile showing the parameter set to `Disabled`:

```
90-102 D90TDI
 Station=D90TDI
  ...
  Max Shared Users=N/A
 >MDMonHold Timeout=Disabled
  Encaps options...
  ...
```

`Disabled` specifies a client modem cannot place the MAX unit hold.

When `Enabled` is specified for the parameter and if a session exceeds the specified limit, the unit displays a progress code or a disconnect cause code:

- `34 (PR_MODEM_ONHOLD)`—The time a client modem placed the MAX unit on hold exceeded the specified value.

- `19 (DIS_MODEM_MOH_TIMER_EXPIRED)`— The MAX unit disconnected the session when the client modem did not come back online within the specified time.

## New and modified V.92 parameters in the `TServ options` menu

TAOS 10.0 adds four parameters to the `TServ options` menu and modifies the `MDM Modulation` parameter so you can now specify `V.92`. The sample `TServ options` menu shows the new and modified parameters, which are set to their default values:

```
90-E00 Mod Config
 TServ options...
  ...
 >MDM Modulation=V.90
  MDMonHold Timeout=Disabled
  MDM Quick-Connect=No
  MDM V.92 Rx Baud=48000
  MDM V.44 Enabled=No
  ...
```

Following table provides an overview of the five added or modified parameters located in the `TServ options` menu used to specify values related support for the V.92 dial-up modem and the V.44 link-layer compression standards.

| Parameter | Setting |
|---|---|
| `MDM Modulation` | Specifies a modem modulation the MAX unit uses. Specify one of the following values:<br>• K56<br>• V.34<br>• V.90 (the default)<br>• V.92<br>With TAOS 10.0 you can specify V.92. |

| Parameter | Setting |
|---|---|
| `MDMonHold Timeout` | Located both in the `TServ options` and the `Connections` profile. Specifies whether a client modem can place a MAX unit can be on hold and the maximum duration that a MAX unit on hold. Once the specified time limit passes, the unit disconnects the session. Specify a value measured in seconds (`Sec`) and minutes (`Min`) follows:<br>• `Disabled` (the default)<br>• `10 Sec`<br>• `20 Sec`<br>• `30 Sec`<br>• `40 Sec`<br>• `1 Min`<br>• `2 Min`<br>• `3 Min`<br>• `4 Min`<br>• `6 Min`<br>• `8 Min`<br>• `12 Min`<br>• `16 Min`<br>• `No Limit`<br>• `Use Global` (available in the `Connections` profile only)<br>If you specify `Use Global` for the `MDMonHold Timeout` parameter located in the `Connections` profile, the MAX unit refers to the value specified for the parameter located in the `TServ options` profile. Otherwise, the value you specify in the `Connections` profile overrides the value specified for the parameter in the `TServ options` profile. |
| `MDM Quick-Connect` | Specifies whether a client modem can connect to a MAX unit by reusing values determined from a prior modem negotiation. Specify `Yes` or `No` (the default). |
| `MDM V.44 Enabled` | Specifies whether the MAX unit supports the use of V.44 compression by client modems. Specify `Yes` or `No` (the default). |

| Parameter | Setting |
|---|---|
| `MDM V.92 Rx Baud` | Specifies the maximum upstream (or receive) baud rate that a MAX unit allows its modems to negotiate. Specify one of the following baud rates:<br>• `48000 (the default)`<br>• `46667`<br>• `45333`<br>• `44000`<br>• `42667`<br>• `41333`<br>• `40000`<br>• `38667`<br>• `37333`<br>• `36000`<br>• `34667`<br>• `33333`<br>• `32000`<br>• `30667`<br>• `29333`<br>• `28000`<br>• `26667`<br>• `25333`<br>• `24000`<br>The MDM V.92 Rx Baud parameter is applicable only if you specify V.92 for the MDM Modulation. |

## Using SNMP to specify values for V.92 and V.44 parameters

You can use a Simple Network Management Protocol (SNMP) manager to specify values for V.92 and V.44 parameters located in the `TServ options` menu and in each `Connections` profile.

The following table gives the SNMP Management Information Database (MIB) values that correspond with V.92 and V.44.

| Parameter | Location | MIB value |
|---|---|---|
| `MDM Modulation` | `TServ options` | `114.7` |
| `MDMonHold Timeout` | `TServ options` | `114.9` |
| `MDM Quick-Connect` | `TServ options` | `114.10` |
| `MDM V.92 Rx Baud` | `TServ options` | `114.11` |
| `MDM V.44 Enabled` | `TServ options` | `114.12` |
| `MDMonHold Timeout` | *any* `Connections` *profile* | `60.54` |

## Using RADIUS to specify a modem-on-hold value

The Remote Authentication Dial-in User Service (RADIUS) attribute `Ascend-MOH-Timeout` specifies a value for the `MDMonHold` parameter, located in a `Connections` profile. The attribute uses index 261 and requires a RADIUS server that can process 16-bit RADIUS attributes.

# *MultiDSP MAX slot card support for V.110 added*

The `V110 Ans N#` parameter now also applies to the MultiDSP MAX slot card.

# *MultiDSP MAX slot card support for PHS added*

The MultiDSP MAX card now supports Personal Handy Phone functionality. You can enter a telephone number(s) into a new parameter, `PHS Ans N# (N=1-4)`, to route incoming PHS calls.

# *X.28 PAD login modified*

The X.28 packet assembler/disassembler (PAD) login process now includes

- A new terminal server security mode
- The ability to specify X.121 source address per call on the MAX interface and through RADIUS
- A modified PAD call command

## New terminal server security mode

Now you can set a new X.28 terminal server security mode specifically for X.25 PAD connections. The new mode requires a formatted login string containing username, password, and optionally an X.121 address to autocall and call user data for the X.25 Call request. The login string for the terminal server security mode is in the following format:

```
N<username>/<password>-[<X.121 Autocall Addr>[D<data>]]
```

Where

- The username can be up to 31 characters
- The password can be up to 64 characters
- The optional X.121 autocall address can be up to 15 characters
- The optional call user data can be up to 12 characters

This new option is intended for X.25 PAD dial-in sessions only.

**Note:** As with the existing `Partial` value for the `Security` parameter, you are only prompted for a login name and password for terminal mode and not for menu mode.

## New POS Auth parameter for terminal server security mode

The parameter POS Auth now appears in the Ethernet > Answer > PAD menu to facilitate the new security option POS (point of sale) in the Ethernet > Mod Config > TServ options > Security menu. POS Auth specifies that, for terminal security users, POS authentication can be used rather than the terminal server security mode as defined by the Ethernet > Mod Config > TServ options > Security parameter.

You can specify Yes, or No (the default) for the POS Auth parameter. And if the Ethernet > Answer > PAD > POS Auth is set to Yes, then Ethernet > Mod Config > TServ options > Security is N/A.

## Configuring the X.121 source address for X.25 PAD calls

The X.121 source address, for both local and remote authentication, can now be specified on a per call basis.

The parameter, X.121 src addr, located Ethernet > Connections > *Connection* profile > Encaps options, specifies the X.121 source address is the MAX unit's source address for logical links using this X.25 profile.

You can specify an X.121 address between 1 and 15 decimal digits. This string should contain numeric characters [0 through 9] only. If an entered character is out of range, the X.121 address is truncated at the character prior to the erroneous character. For example,

X.121 src addr=031344159782738 will be truncated to
X.121 src addr=031344159

You can also externally configure the following attribute in the RADIUS user record to specify a X.121 source address for X.25 PAD calls:

Ascend-X25-X121-Source-Address=X.121 Address

### Modified PAD Call command

You can now extend the syntax of the PAD Call command to accept Ddata in addition to the existing command line options.

Previously, the PAD Call string was call [?] | [[ address [*P|*D|*Fdata]] where the MAX inserts the data following the *P, *D or *F keywords into the user data field of the call packet. The actual way that the data is processed depends on which of the *P, *D or *F keywords is given.

The customers point of sales (POS) terminals could only generate D and not *D as the keyword, so the command syntax was modified to recognize D as a keyword as well as *D.

The command string now is call [?] | [[ address [*P|[*]D|*Fdata]]. So the only modification to the command is to recognize D and *D as the same keyword.

# Number of characters in of Recv Name parameter value field increased

Previously, if you were downgrading to an older version of TAOS and entered a name that was too long, the `Recv Name` parameter value field, used for bidirectional chap, would be truncated after 23 characters. With TAOS 10.0, you can now enter up to 64 characters in the `Recv Name` parameter value field before it is truncated. The `Recv Name` parameter is located in the `Ethernet` > `Connections` > `any Connection profile` > `Encaps Options` subprofile.

The RADIUS attribute `Ascend-Recv-Name (45)` also has an increased maximum length. You can now specify a string up to 64 characters.

# Support for Vietnamese R2 signaling added

You can now enter the value, `Vietnam`, in the `Ethernet` > `E1` > `Line Config` > *`any profile`* > `Line 1` > `Sig Mode` parameter.

# Support for multiple compression protocols added

With TAOS 10.0, if a remote unit call does not support the link compression protocol specified by a MAX unit's `Connection` profile, the MAX unit automatically attempts to complete a session with the remote unit using one of the following compression protocols:

- `MPPC`—Microsoft Point-to-Point Compression
- `MS-Stac`—Microsoft STAC
- `Stac-9`—Draft 9 of the STAC LZS Compression protocol
- `Stac`—Lucent-modification of draft 0 of the CCP protocol

For example, the specified `Connection` profile for a remote user might specify `MS-Stac` for the `Link Comp` parameter. MS-STAC is the protocol that the Windows 95 operating system uses to complete a connection with link compression. As long as the user continues to use Windows 95, the link compression protocol specified by the following `Connection` profile continues to be correct.

```
90-101 Landie
 Encaps options...
  LQM Min=600
  LQM MAX=600
  Link Comp=MS-Stac
  ...
  Target Util=70
  Idle Pct=0
  Split Code.User=N/A
```

However, if the remote user upgrades to a new operating system, the link compression protocol the MAX unit must use to complete the connection might change. For example, if the remote user upgrades to Windows 2000, the unit must use Microsoft Point-to-Point Compression (MPPC) to complete the connection with link compression. In this case, the MAX unit first

attempts the protocol specified in the `Connection` profile (MS-STAC), then the MAX unit attempts each of the supported link compression protocols and uses the protocol supported by the remote user's operating system (MPPC). The unit completes a remote user's connection without link compression only after attempting to utilize one of the supported protocols or if the value for the `Link Comp` parameter is `None` (the default).

# *Manual control of Ethernet modes added*

You can now disable auto negotiation and manually set the duplex and speed of the Ethernet on the MAX 6000. You can now manually set the `Duplex Mode` and `Media Speed Mbit` parameters for the Ethernet mode by disabling the `Auto Negotiate` parameter.

## New Parameters

### Auto Negotiate

**Description:** Enables the Ethernet hub and the MAX to exchange information to determine each other's capabilities and then decide a uniform way, 10Mbs or 100Mbs and full or half duplex, to communicate with each other.

**Usage:** Specify `Yes`, or `No`. `No` is the default.

`Yes`—Auto negotiation occurs automatically and the Ethernet hub and the MAX determine a common format for communication.

`No`—Auto negotiation is not automatic and the user manually configures the MAX and the Ethernet hub so that they are both using the same settings for communication.

**Dependencies:** If the value of the `Auto Negotiate` parameter is set to `Yes`, then both `Media Speed Mbit` and `Duplex Mode` parameters default to `N/A`. If the value of the `Auto Negotiate` parameter is set to `No`, then the value for `Media Speed` defaults to `100mb` and the value of the `Duplex Mode` parameter defaults to `Full-Duplex`.

**Note:** If Auto negotiate is set to `No`, then the Ethernet is forced to the mode indicated by `Media Speed` and `Duplex Mode`. If the forced mode is not compatible with the hub that the Ethernet is connected to, then communication does not work.

**Location:** `Ethernet > Mod Config > Ether options`

**See Also:** `Duplex Mode, Media Speed Mbit`

### Duplex Mode

**Description:** Specifies whether the physical Ethernet interface of the 100BaseT port uses full-duplex or half-duplex mode.

**Usage:** Specify one of the following settings:

- `Full-Duplex` (the default) provides increased throughput.
- `Half-Duplex` enables operation with older equipment that does not support full-duplex mode.

**Dependencies:** The `Duplex Mode` and `Media Speed Mbit` parameters each default to `N/A` if the value of the `Auto Negotiate` parameter is set to `Yes`. The value for `Duplex Mode` defaults to `Full-duplex` and the value for `Media Speed Mbit` defaults to `100mb` if the `Auto Negotiate` parameter is set to `No`.

**Location:** `Ethernet > Mod Config > Ether options`

**See Also:** `Auto Negotiate, Media Speed Mbit`

### Media Speed Mbit

**Description:** Specifies the speed of the Ethernet port.

**Usage:** Specify one of the following settings:

- `10mb` specifies 10Mbps.
- `100mb` (the default) specifies 100Mbps.

**Dependencies:** The `Media Speed Mbit` and `Duplex Mode` parameters each default to `N/A` if the value of the `Auto Negotiate` parameter is set to `Yes`. The value for `Media Speed` defaults to `100mb` and the value for `Duplex Mode` defaults to `Full-duplex` if the `Auto Negotiate` parameter is set to `No`.

**Location:** `Ethernet > Mod Config > Ether options`

**See Also:** `Auto Negotiate, Duplex Mode`

# New Tunneling features

## *New traps added to indicate L2TP tunnel failure and deactivation*

In TAOS 10.0, two new Simple Network Management Protocol (SNMP) traps for Layer 2 Tunneling Protocol (L2TP) events have been implemented. One is generated when an L2TP tunnel-setup fails. The other is generated when a previously established L2TP tunnel is disconnected.

### New trap definitions

Following are the enterprise-specific traps added to `ascend.trp`:

```
asndL2tpTunnelSetupFailure  TRAP-TYPE
    ENTERPRISE      ascend
    VARIABLES       {
                    asndL2tpTunnelStatsIfIndex,
                    asndL2tpTunnelStatsInitiated,
                    asndL2tpTunnelStatsRemoteHostName,
                    asndL2tpDomainStatsIdentifier,
```

```
                        asndL2tpTunnelStatsLastResultCode,
                        asndL2tpTunnelStatsLastErrorCode,
                        asndL2tpTunnelStatsLastErrorMessage
                        }
        DESCRIPTION     "An asndL2tpTunnelSetupFailure trap signifies
                        that a failure happened during L2TP tunnel
                        establishment."
        ::= 52
```

and

```
    asndL2tpTunnelDisconnect  TRAP-TYPE
        ENTERPRISE      ascend
        VARIABLES       {
                        asndL2tpTunnelStatsIfIndex,
                        asndL2tpTunnelStatsInitiated,
                        asndL2tpTunnelStatsRemoteHostName,
                        asndL2tpDomainStatsIdentifier,
                        asndL2tpTunnelStatsLastResultCode,
                        asndL2tpTunnelStatsLastErrorCode,
                        asndL2tpTunnelStatsLastErrorMessage
                        }
        DESCRIPTION    "An asndL2tpTunnelDisconnect trap signifies that
                        an established L2TP tunnel was disconnected."
        ::= 53
```

The corresponding SNMPv3 definitions have been added to `ascendv3.trp`. For a description of the variables defined in each trap, refer to `asndl2tp.mib`.

## Enabling L2TP traps

To enable L2TP traps on a MAX unit, set `L2TP Traps` to `Yes` in the `Ethernet` > `SNMP Traps` > *`trap-name`* > `Enable Traps` subprofile.

# *Limitation on the number of calls processed by an L2TP tunnel added*

With TAOS 10.0, you can limit the number of calls that a MAX unit processes using Layer 2 Tunneling Protocol (L2TP) tunnels. The `Max Calls per Tunnel` parameter, added to the `L2TP Config` menu, enables you to limit the number of calls that are disconnected if one tunnel experiences problems and drops. You can specify this limit for an L2TP access concentrator (LAC) and an L2TP network server (LNS). If you specify `0` (zero, the default), there is no limit to the number of calls.

You can also use an SNMP manager's `snmpget` and `snmpset` commands to specify a value for the parameter. If the unit reaches a limit and must disconnect a call, the unit sends a message, including disconnect information, to the `Syslog` daemon. In the MAX unit's diagnostics interface, the unit displays information regarding the disconnect if `L2TPCM` is enabled at the time.

## New `Max Calls per Tunnel` parameter specifies a maximum number of calls per tunnel

Following is a sample configuration specifying a value of `2` that specifies that a MAX unit can process up to two calls by means of single a L2TP tunnel.

```
L2 Tunneling options...
 L2TP Config...
  ...
  Verify Remote Name=N/A
  ATC Encoding=Normal
  Suppress Endpoint Disc=No
 >Max Calls per Tunnel=2
  ...
```

In the example, the impact of specifying a value of `2` for the `Max Calls per Tunnel` parameter differs depending on whether the MAX unit is performing on the network, as an L2TP network server (LNS) or an L2TP access concentrator (LAC):

| L2TP Call Function | MAX unit process |
|---|---|
| LNS terminating incoming calls | The MAX unit counts the number of calls in the current L2TP tunnel. The unit does not process the third or subsequent incoming calls. The unit disconnects the call and sends the following message to the `Syslog` daemon:<br>`734 :- L2TUNNEL: Out of resources`<br>The unit also displays the message in the diagnostic interface if `L2TPCM` is enabled at the time, as follows:<br>`Incoming call dropped. Tunnel reached its maximum limit of 2 calls` |
| LNS placing outgoing calls | The MAX unit counts the number of calls in the current L2TP tunnel. The unit processes a third call by establishing another L2TP tunnel. |
| LAC processing incoming calls | The MAX unit counts the calls in the current L2TP tunnel. The unit processes a third call by establishing a second L2TP tunnel. |

## New SNMP commands can specify a maximum number of calls per tunnel

Use `snmpget` and `snmpset` commands to specify a value for the `Max Calls per Tunnel` parameter. Using an Simple Network Management Protocol (SNMP) manager, you can issue these commands for the following SNMP MIB:

```
.iso.org.dod.internet.private.enterprises.ascend.configuration
.mibl2TunnelGlobal.mibl2TunnelGlobalTable.mibl2TunnelGlobalEntr
y.
l2TunnelGlobal__l2tp_config__max_calls_per_tunnel.1 oid
```

For example, you can display the current setting for the `Max Calls per Tunnel` parameter by issuing the following command:

```
snmpget 110.110.110.138 public .1.3.6.1.4.1.529.23.90.1.1.34.1
```

In response, the SNMP manager displays the following if a value of `0` (zero, the default) is specified for the `Max Calls per Tunnel` parameter:

```
enterprises.529.23.90.1.1.34.1 = 0
```

In order to specify a value for the `Max Calls per Tunnel` parameter, you can issue the following command from the SNMP Manager:

```
snmpset 110.110.110.138 write .1.3.6.1.4.1.529.23.90.1.1.34.1 i
x
```

Where x is a numeric value from `0` through `65535`. If you attempt to specify a value that does not fall within that range, the SNMP Manager displays the following message:

```
Error in packet.
Reason: (badValue) The value given has the wrong type or length.
Failed object: enterprises.529.23.90.1.1.34.1
```

# *MAX unit support for IP fax removed*

With TAOS 10.0, the MAX no longer supports store and forward fax capability.

# *New Suppress Endpoint Disc parameter to disable end-point discriminators added*

For PPP connections, negotiating an end-point discriminator is unnecessary and increases the timeit takes to connect. Some terminal adapters send end-point discriminators during Link Control Protocol (LCP) negotiations even if the service type is PPP and not MP/PPP. When configured as an L2TP access concentrator (LAC), the MAX forwards the PPP service type L2TP network server (LNS). However, LNS rejects end-point discriminators because they are mismatched against PPP. Then renegotiation of LCP is started. By disabling end-point discriminators for a PPP session, the negotiations finish more quickly.

The new parameter Suppress Endpoint Disc configures the MAX unit to run without acknowledging end-point discriminators. If you disable acknowledgement by specifying Yes, PPP connections made more quickly. If end-point discriminators are not disabled by specifying No (the deafult), PPP connections will still be successful, but will take longer to connect.

## New Data PKT UDP parameter to disable L2TP packet checksum added

To reduce packet processing time, you can disable the creation of a UDP checksum for transmitted Layer 2 Tunneling Protocol (L2TP) data packets. However, if the MAX unit receives a L2TP data packet, it still calculates the UDP checksum.

You disable or enable L2TP packet checksum creation by setting the new parameter Data Pkt UDP Cksum, located in Ethernet > Mod Config > L2 Tunneling options > L2TP Config. The default, yes, disables the checksum creation.

# New RADIUS features

## Two new parameters that report NAS port type to RADIUS accounting added

You can now specify how an L2TP network server (LNS) unit reports the NAS Port Type attribute to RADIUS accounting. TAOS 10.0 adds the two new parameters LNS Acct NPT and LNS NPT D-A Default to the L2TP Config menu. The LNS Acct NPT parameter applies when the L2TP Mode parameter specifies Both or LNS and the Acct parameter specifies RADIUS. The LNS NPT D-A Default parameter is applicable when the LNS Acct NPT parameter specifies AVP.

When you specify Virtual (the default) for the LNS Acct NPT parameter, an LNS unit reports NAS Port Type to RADIUS accounting as Virtual and does this without referring to the Port Type List attribute-value pair (AVP) available from the L2TP access concentrator (LAC) unit.

```
90-E00 Mod Config
 L2 Tunneling options...
  L2TP Config...
    ...
    Verify Remote Name=N/A
    ATC Encoding=Normal
   >LNS Acct NPT=Virtual
    LNS NPT D-A Default=N/A
    Suppress Endpoint Disc=No
    Pre-SCCRQ Secret Lookup=No
    ...
```

When you specify AVP for the LNS Acct NPT parameter, you must also specify a default digital asynchronous rate adaption standard for the LNS unit to use to refer to the Port Type List attribute-value pair located on the LAC unit. The available default rate adaption standards are V.110 and V.120. Following is a sample configuration that reports NAS Port Type to RADIUS after it refers to the LAC unit's Port Type List using the V.120 rate adaption standard:

```
90-E00 Mod Config
 L2 Tunneling options...
  L2TP Config...
    ...
    Verify Remote Name=N/A
    ATC Encoding=Normal
   >LNS Acct NPT=AVP
    LNS NPT D-A Default=V120
    Suppress Endpoint Disc=No
    Pre-SCCRQ Secret Lookup=No
    ...
```

In the previous example, the LNS unit receives an incoming call request and refers to Port Type List information from the LAC unit.

If the LNS unit does not receive Port Type List information from the LAC, the LNS uses Bearer Type and Framing Type attribute-value pairs to report NAS Port Type. One exception to Bearer Type and Framing Type attribute-value pairs is that the MAX LNS unit uses the LNS NPT D-A Default parameter setting you specify (V110 or V120) to report digital asynchronous calls.

LNS units apply attribute-value pairs to report modem session information to a RADIUS server, as follows:

| Bearer Type | Framing Type | NAS Port Type |
|---|---|---|
| Analog | Asynchronous | Asynchronous (Asynch) |
| Analog | Synchronous | Synchronous (Synch) |
| Digital | Synchronous | ISDN Synchronous (ISDN_Synch) |
| Digital | Asynchronous | ISDN Asynchronous V.110 or V.120 (ISDN_Asynch_V110 or ISDN_Asynch_V120) |

# *Support for the `Port Type List (44)` vendor-specific attribute-value pair added*

With TAOS 10.0, a MAX unit configured as Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) conforms with recommendations included in the Internet Engineering Task Force (IETF) draft titled *L2TP Session Information* (`draft-ietf-l2tpext-sesinfo-03.txt`.)

**Note:** Tunnel switching or *multihop*, also described in *L2TP Session Information*, is not implemented with TAOS 10.0.

The working draft specifies additional attribute-value pairs to enable a LAC unit to provide port type and port identification information to a terminating L2TP network server (LNS). In particular, the draft specifies that when a LAC unit receives an incoming call request (ICRQ) from a remote user, the unit can send the `Port Type List` (`44`) attribute-value pair to the LNS unit. If `l2tpcm debug` is enabled on the LNS unit, the unit outputs the information to its accounting and debugging records.

The `Port Type List` attribute-value pair indicates whether ports used to complete calls are physical (`0`) or virtual (`1-`*`n`*) using formats specified by Remote Authentication Dial In User Service (RADIUS) Accounting. The physical port type is the channel defined in the `Physical Channel ID` attribute-value pair. All the other port types are optional and are channels defined in the corresponding position of the `Virtual Channel ID` attribute-value pair, a list of four octet values, representing the channel IDs of all the virtual channels that the session has processed.

Support for the attribute-value pair makes no change to the unit's VT100 interface, nor does it require any change to the configuration of the MAX unit. However, you can verify support for the `Port Type List` attribute-value pair by enabling `l2tpcm debug` on a LNS unit which receives the information from a LAC unit.

An LNS unit for which `l2tpcm debug` is enabled reports the following information from the LAC unit when an asynchronous call is placed to the LAC unit:

```
...
L2TPCRX-2 [111.222.33.444:7019/2] (task "L2tpTransportTask" at
0xb08dbf20, time: 3092.47) 77 octets @ 0xb0a06fc8
[0000]: c8 02 00 4d 00 02 00 00  00 02 00 01 80 08 00 00...M .......
[0010]: 00 00 00 0a 80 08 00 00  00 0e 00 19 80 0a 00 00............
[0020]: 00 0f 00 00 00 02 80 0a  00 00 00 12 00 00 00 02............
[0030]: 80 0a 00 00 00 15 34 37  33 33 80 0b 00 00 00 16....47 33...
[0040]: 38 35 30 36 35 00 08 09  30 00 2c 00 00      85065... 0.,...
L2TPCTX-2 [111.222.33.444:7019/2] (task "L2tpTransportTask" at
0xb08dbf20, time: 3092.47) 12 octets @ 0xb09f23c0
[0000]: c8 02 00 0c 00 02 00 00  00 01 00 03              ........ ....
L2TPCM-2: transportRxCallback from [111.222.33.444:7019/2] on VR0
L2TPCM-2: Event = RxInCallReq
L2TPCM-2: parse ICRQ
L2TPCM-2: .. peersCallId = 25
L2TPCM-2: .. peersCallSerialNumber=0
L2TPCM-2: .. Bearer Type = 0x00000002
L2TPCM-2: .. Dialed Number = 4733, mbit =  ON
L2TPCM-2: .. Dialing Number = 85065, mbit =  ON
```

```
L2TPCM-2: .. nasPortType = 0
```

# Nonzero IP address reporting for all channels added to accounting records

Previously, in RADIUS accounting Start and Stop records, the value of the `Framed-IP-Address` attribute was set to 0.0.0.0 for all channels except the initial one. In TAOS 10.0, the `Framed-IP-Address` attribute indicates the correct IP address associated with each channel.

# NAS-identifier support added to request packets

The network access server (NAS) in RADIUS Access Request and Accounting Request packets. The value of `NAS-Identifier` attribute is the value of the `System` > `Sys Config` > `Name` parameter plus the value of the `Ethernet` > `Mod Config` > `DNS` > `Domain Name` parameter: `system name.domain name`. If a system name is not specified, the `NAS-Identifier` attribute is set to the string `noname`.

For example, suppose that the system name is MARCMAX1 but no domain name is configured. The `NAS-Identifier` value would be the following:

```
NAS-Identifier = "MARCMAX1"
```

If the system name is MARCMAX1 and the domain name is `sophia.eng.com`, the `NAS-Identifier` value would be the following:

```
NAS-Identifier = "MARCMAX1.sophia.eng.com"
```

If the domain name is `sophia.eng.com`, but no system name is specified, the `NAS-Identifier` value would be the following:

```
NAS-Identifier = "noname.sophia.eng.com"
```

If there is neither a system name nor a domain name specified, the `NAS-Identifier` value would be the following:

```
NAS-Identifier = "noname"
```

# Outgoing attributes support added to `diag radif` command

Previously, the `diag radif` command displayed the number and value of each attribute in incoming RADIUS authentication responses only. Now, the `diag radif` command displays the number and value of each attribute in outgoing RADIUS accounting and authentication requests as well. To display incoming and outgoing attributes, you enter the `diag radif` command with the new *`level`* option.

## Using the `level` option

The `diag radif` command now accepts a *`level`* option. The level option enables or disables the diplay of different types of information by using the following bitwise operands:

| Level | Displays |
|---|---|
| 1 | General `diag radif` progress messages |
| 2 | Incoming RADIUS attributes |
| 4 | Outgoing RADIUS attributes |

**Note:** You can combine the bitwise operands by simply adding the values together. For example, to display progress messages (level 1)and incoming RADIUS attributes (level 2), enter:

```
admin> diag radif 3
```

To display all messages (level 1 and level 2 and level 4, enter:

```
admin> diag radif 7
```

To disable all messages, enter:

```
admin> diag radif 0
```

When you enter `diag radif` without the *`level`* option, you can use the command as a simple on/off toggle switch that defaults to level 1. Note that level 1 no longer includes incoming RADIUS attributes. You must specify `diag radif 3` to display the equivalent of the `diag radif` command in previous implementations.

## Attribute displays

When you use the `diag radif` command, the system displays incoming and outgoing attributes. The incoming attributes appear exactly as before, except that you must enable level 2 to display them. For example, information for an incoming attribute might look like the following:

```
RADIF: vendor 0 attr 25, len 11, 54 65 73 74
```

The information includes the vendor ID, the attribute ID, the attribute length, and the first four octets of the attribute data.

Outgoing attributes are displayed in one of three formats, depending on the type of data the attribute contains:

| Value | Display | Example |
|---|---|---|
| Integer | `RADIF: Vendor` *`num1`*`, Attribute` *`num2`*`, Value=`*`num3`* | `RADIF: Vendor 529, Attribute 255, value=28800` |
| IP address | `RADIF: Vendor` *`num1`*`, Attribute` *`num2`*`, Value=`*`ip_address`* | `RADIF: Vendor 0, Attribute 4, Value=192.168.21.85` |

| Value | Display | Example |
|---|---|---|
| String | `RADIF: Vendor num1, Attribute num2, Value=0x## 0x## 0x## 0x## 0x## ... [len=num3]`<br><br>The `0x##` value denotes a hexadecimal number. The `len=num3` value indicates the length of the data and appears only if the string is longer than five octets. | `:RADIF: Vendor 0, Attribute 1, Value=0x6a 0x69 0x6d 0x74 0x65 ... [len=7]` |

# Support for disabling RADIUS accounting and call logging for VoIP calls added

In TAOS 10.0, you can enable or disable RADIUS accounting and call logging for Voice over IP (VoIP) calls.

## New Voip Accounting and Voip Call Logging parameters added

Following are the new VT100 parameters and their settings:

| Parameter | Settings |
|---|---|
| `Accounting > Voip Accounting` | Specify `Yes` (the default) to enable RADIUS accounting for VoIP calls. Specify `No` to disable RADIUS accounting for VoIP calls. |
| `Call Logging > Voip Call Logging` | Specify `Yes` (the default) to enable call logging for VoIP calls. Specify `No` to disable call logging for VoIP calls. |

# `Event-Timestamp (55)` attribute added to RADIUS accounting requests

After RADIUS authentication and authorization are complete, the MAX unit sends a Start packet to the RADIUS server, notifying it that the connection is established. In the past, the time between the moment that the connection was established and the moment that the RADIUS server received the notification was not recorded. Now, the new `Event-Timestamp (55)` attribute specifies the exact time that the connection is established as the number of seconds since January 1, 1970 00:00:00 UTC.

The `Event-Timestamp` attribute appears in the following Accounting Request packets:

- Accounting Start
- Accounting Stop
- Accounting Checkpoint
- Accounting On
- Accounting Off

The `Event-Timestamp` attribute also appears in the following Call Logging packets:

- Accounting Start
- Accounting Stop
- Accounting On
- Accounting Off

# Session timeouts and new syslog message added for L2TP, PPTP, and L2F calls

The following `Connection` profile parameters and analogous RADIUS attributes now apply to Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F) calls:

| Connection profile parameter | RADIUS attribute |
|---|---|
| `Idle` | `Idle-Timeout (28)`<br>`Ascend-Idle-Limit (244)` |
| `Max Call Duration` | `Session-Timeout (27)`<br>`Ascend-Maximum-Time (194)`<br>`Ascend-Maximum-Call-Duration (125)` |

In addition, a new `syslog` message is generated for L2TP, PPTP, and L2F calls.

For details about RADIUS attributes, see the *TAOS RADIUS Guide and Reference*. For details about `Connection` profile parameters, see the *MAX Reference*.

## Specifying the amount of time before an idle call is disconnected

The `Connection` profile parameter `Idle` and the RADIUS attributes `Idle-Timeout (28)` and `Ascend-Idle-Limit (244)` specify the amount of idle time that must elapse before a call is disconnected. For L2TP, PPTP, and L2F calls, any data packet is considered activity, including LCP Echo packets or other PPP link-level packets. If more than one of the attributes is included in the RADIUS response, the last attribute in the response overrides all the previous ones.

## Specifying the maximum amount of time for a call

The `Connection` profile parameter `Max Call Duration` and the RADIUS attributes `Session-Timeout (27)`, `Ascend-Maximum-Time (194)`, and `Ascend-Maximum-Call-Duration (125)` specify the maximum amount of time that a call remains connected. For L2TP, PPTP and L2F calls, all three RADIUS attributes work identically.

### New syslog message

When an L2TP, PPTP, or L2F call connection is established, a new `syslog` message is generated. This message is issued only on the modem side of the tunnel. The format for the message is

`LAN session up, `*`user`*` (`*`protocol`*` S=`*`ip_address`*` V=`*`vrouter`*`) [MBID 5; 541->4739]`

The fields in parentheses identify the tunneling protocol, and the IP address and virtual router (VRouter) associated with the remote tunnel-server end point. The VRouter clause is omitted if the VRouter feature is disabled or if the VRouter is the main router.

## *New RADIUS NAS-Port attribute value*

In TAOS 10.0, the RADIUS `NAS-Port` attribute has a new value that enables you to determine the channel, line, slot, and shelf on which a call is received without having to do the calculations required for other values. In addition, TAOS 10.0 implements a new parameter that enables you to specify the format required for the new RADIUS value. An existing parameter for specifying the `NAS-Port` format has been deprecated.

### New NASPort Format parameter added

In the `System > Sys Config` profile, the `New NASPortID` parameter has been deprecated, and the `NASPort Format` parameter has been added. The value of the `New NASPortID` parameter is used only if the `NASPort Format` parameter is set to N/A (not-applicable).

### RADIUS changes

Following are the RADIUS changes that support the new `NAS-Port` format:

- The `NAS-Port` attribute can now have a value from 0 through 4294967296.
- The value `1_2_3_3` is added to the list of possible values for the `Ascend-NAS-Port-Format` attribute.

# New SNMP features

## *New traps indicating L2TP tunnel failure and deactivation added*

In TAOS 10.0, two new SNMP traps for Layer 2 Tunneling Protocol (L2TP) events have been implemented. One is generated for an L2TP tunnel-setup failure. The other is generated when a previously established L2TP tunnel is disconnected.

## New trap definitions

Following are the enterprise-specific traps added to `ascend.trp`:

```
    asndL2tpTunnelSetupFailure  TRAP-TYPE
        ENTERPRISE      ascend
        VARIABLES       {
                        asndL2tpTunnelStatsIfIndex,
                        asndL2tpTunnelStatsInitiated,
                        asndL2tpTunnelStatsRemoteHostName,
                        asndL2tpDomainStatsIdentifier,
                        asndL2tpTunnelStatsLastResultCode,
                        asndL2tpTunnelStatsLastErrorCode,
                        asndL2tpTunnelStatsLastErrorMessage
                        }
        DESCRIPTION     "An asndL2tpTunnelSetupFailure trap signifies
                        that a failure happened during L2TP tunnel
                        establishment."
        ::= 52
```

and

```
asndL2tpTunnelDisconnect  TRAP-TYPE
        ENTERPRISE      ascend
        VARIABLES       {
                        asndL2tpTunnelStatsIfIndex,
                        asndL2tpTunnelStatsInitiated,
                        asndL2tpTunnelStatsRemoteHostName,
                        asndL2tpDomainStatsIdentifier,
                        asndL2tpTunnelStatsLastResultCode,
                        asndL2tpTunnelStatsLastErrorCode,
                        asndL2tpTunnelStatsLastErrorMessage
                        }
       DESCRIPTION    "An asndL2tpTunnelDisconnect trap signifies that
                       an established L2TP tunnel was disconnected."
        ::= 53
```

The corresponding SNMPv3 definitions have been added to `ascendv3.trp`. For a description of the variables defined in each trap, refer to `asndl2tp.mib`.

## Enabling L2TP traps

To enable L2TP traps on a MAX unit, set L2TP Traps to `Yes` in the `Ethernet` > `SNMP Traps` > *`trap-name`* > `Enable Traps` subprofile.

# New IP routing features

## *New command that temporarily disables IP addresses listed in address pools added*

A denial of service (DoS) attack is a deliberate attempt to interfere with network performance by directing forged Internet Control Message Protocol (ICMP) Echo Request packets to IP broadcast addresses. On a MAX unit configured to support dial-in access to the Internet, a DoS might be directed against one of the IP addresses specified by the unit's IP address pool. If this occurs, a dial-in user's access request cannot be processed if the unit attempts to utilize the IP address that is the object of the attack. The new diagnost`ic command ip-pool-addr -x [vRouterName]IP address` permit you to temporarily disable an IP address that is the object of an attack. The unit can continue to process calls. Afterwards, you can re-enable the address for the unit's IP address pools.

**Note:** If the MAX unit resets, the unit automatically re-enables any IP addresses you disabled using this feature.

From the MAX unit's diagnostic interface, you can issue a new diagnostics command using the following format:

**`ip-pool-addr -`*`x`*` [`*`vRouterName`*`]`*`IP address`*

| Command | Setting |
|---|---|
| **`ip-pool-addr -d [`*`vRouterName`*`]`*`IP address`* | Specifies that the MAX unit does not allocate the IP address for dial-in connections. In addition to the IP address, you can specify a virtual router name to which the command applies. |
| **`ip-pool-addr -e [`*`vRouterName`*`]`*`IP address`* | Enables a previously disabled IP address. The unit allocates the IP address for dial-in connections. In addition to the IP address, you can specify a virtual router name to which the command applies. |
| **`ip-pool-addr -l`** | Lists IP addresses in the unit's IP address pool that are disabled. The command does not change the status of any address specified in the unit's IP address pool. |
| **`ip-pool-addr -?`** | Displays information about command usage. |

In the following example, the IP address 192.168.0.1 is disabled using a diagnostic command:

```
> ip-pool-addr -d 192.168.0.1
Disabling 192.168.0.1 pool address
```

After you disable `192.168.0.1`, the unit responds as follows when you issue an **`ip-pool-addr -l`** command:

```
> ip-pool-addr -l
Disabled ippool addresses:
192.168.0.1
```

Suppose that `192.168.0.1` is the only IP address that is currently the object of a DoS attack. The MAX unit would no longer allocate the IP address to process dial-in connections to the unit. Despite the attack, however, the unit would be able to continue to process dial-in connections.

The unit cannot continue to process calls if any of the IP addresses in its IP pool are objects of the attack. If the unit continues to be unable to process dial-in connections due to a suspected DoS attack, you can issue the command for other IP addresses in the unit's IP address pools. Keep in mind that you can issue the `ip-pool` command to see the addresses listed in the unit's IP address pool. In addition, you might need to consider the IP addresses assigned to IP address pools used by virtual routers configured on the unit. You can use the `ip-pool-addr -l` command to see which IP addresses are currently disabled and, possibly, that list compare it to the results listed produced by the `ip-pool` command.

In the following example, the IP address `192.168.0.1` is enabled again:

```
> ip-pool-addr -e 192.168.0.1
Enabling 192.168.0.1 pool address
```

# Problems corrected in TAOS 10.0

All problems corrected are associated with a Change Request (CR). The following table includes all problems corrected. They are listed in numerical order by CR.

| CR | Problem corrected |
|---|---|
| NA | Improved resistance to denial of service attempts. |
| NA | ATMP: If the HA-HR connection was MP or MPP, only one channel was working. |
| NA | `sysConfigChangeTrap` was not generated when the configuration was modified through SNMP. |
| NA | On a MAX 6000, L2TP was occasionally resetting with Warning 179. |
| 6000743 | A MAX used for terminating AO/DI connections could not handle more that 64 simultaneous X.25 sessions. |
| 6001365 | The `callCurrentAnalogOutgoing` counter was being incremented when an immediate modem telnet session was established. Only when a call is established should the counter be incremented. |

| CR | Problem corrected |
|---|---|
| 6001678 | When a MAX unit reestablished a nailed MPP link, the unit did not correctly bundle the link's two channels. |
| 6001773 | A MAX unit did not allow you to specify `Always` or `Active` for the `Proxy Mode` parameter. |
| 6001936 | MAX 6000 unit running MPP and stacking occasionally reset with FE 40 and a Warning 179. |
| 6001989 | MIF `Dial` command did not work. |
| 6002100 | When the first call connected to a K56 modem in slot 6, slot 7, or slot 8, the MAX 6000 using MPP was not able to connect additional calls. |
| 6002141 | The immediate modem service on the MAX 3000 only worked with the default port value of 5000. |
| 6002170 | The MAX unit ignored the subaddress in Bandwidth Allocation Control Protocol (BACP) callback to add MP channels. |
| 6002240 | The MultiDSP card does not support the thermal MIB and incorrectly reported a temperature value for `watchdogReadingUnits` attribute. |
| 6002245 | The MAX 3000 BRI units occasionally experienced firmware corruption when the BRI line configuration was changed often. |
| 6002315 | MAX units with MultiDSP installed did not accept analog calls from the BRI card. |
| 6002352 | With the `Shared Prof` parameter set to `No` on a MAX 3000, two users could login to the unit using the same ID. |
| 6002366 | A MAX unit truncated long Syslog messages. |
| 6002369 | A nailed MPP call over back-to-back T1s on a MAX 6000 occasionally failed to establish a connection. |
| 6002456 | Upgrading to TAOS 9.1.0 caused internal flash code corruption on a MAX 6000. |
| 6002457 | A MAX 6000 E1 unit displayed a corrupted `load id error` message. |
| 6002471 | MAX unit displayed wrong HDLC channel information from the `show users` command. |
| 6002477 | A MAX 6000 unit with installed MultiDSP modules did not correctly support the `modemdiag` command. |
| 6002496 | MAX unit displayed incorrect source and destination information in the Telnet `TERMINATE` syslog message. |
| 7000018 | Conexant CSMX/CSM3V 5.8177 firmware caused occasional resets. |

| CR | Problem corrected |
|---|---|
| 7000090 | Incoming frame relay packets with the FECN, BECN and DE bits set to 1, are reset to 0 when resent on a second frame relay circuit. |
| 7000099 | MAX 3000 occasionally reset with FE 1, FE18, and FE16. |
| 7000112 | When authenticating using local profiles, regardless of what value was set in the local X25/PAD `connection` profile for the `X.3` parameter profile to use, it always returned to the value CRT. |
| 7006378 | V.120 and x.75 PPTP sessions failed to connect to a NT PPTP server. |
| 7006382 | MAX 3000 units occasionally reset with Fatal Error 1 message. |
| 7006398 | MAX 6000 L2TP failed with channelized T1s. |
| 7006432 | MAX 6000 units' interface-based routing table removed remote LAN host/network address. |
| 7006497 | Loopback test was not working with a MAX 6000 units running software 9.1.x. |
| 7006524 | MAX 6000 was sending incomplete RADIUS accounting information. |
| 7006672 | After several days, users could ping MAX 6000 but not telnet to it. |
| 7006697 | When you set `LinkUp=No`, the MAX 6000 did not send the `LinkDown` SNMP trap packet. |
| 7006849 | When booting up the MAX 6000, occasionally the Smart Modular 8MB flash card was not working, causing the modems to appear to fail. |

# Notices and known issues

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

## *Notice of end of sale for MAX Slot card*

January 7, 2002

Effective immediately, INS Universal Gateway, Product Management team is serving three months notice of the end of sale of the Personal Handyphone Service (PHS) and V.110 slot cards for the MAX 6000 and the BRI slot cards on the MAX 800. Orders for these slot cards will be accepted only until April 7, 2002 or until supplies last and will not be accepted thereafter. Software support ends January 7, 2003.

## Product codes impacted

The product codes effected by this end of sale notice are:

| Model# | Comcode | Description |
|---|---|---|
| MXHP-SL-DSP8 | 300280872 | PHS 8-port slot card |
| MXHP-SL-DSP12 | 300280856 | PHS 12-port slot card |
| MXHP-SL-DSP16 | 300280864 | PHS 16-port slot card |
| MX-SL-DSP16-CO | no comcode | PHS 16-port PHS Slot card, can opened |
| MX-SL-8V110 | 407591262 | V110 8-channel processor slot card |
| M20-SL-BRIS | 407591288 | BRI S PCMCIA MODULE |
| M20-SL-BRIU | 407591270 | BRI U PCMCIA MODULE |

Product warranty, repair and technical support programs will continue for the duration of existing contracts.

The 48- and 60-port MAX MultiDSP slot cards running under TAOS Release 10.0 or later provide ongoing support for PHS and V.110 applications on the MAX 6000 platforms.

## Replacement products

Replacement products may be priced higher than the products they replace. If so, existing contracts should be adjusted to reflect new prices.

| Discontinued product | Replacement product |
|---|---|
| MXHP-SL-DSP8 | MX-SL-48M-DSP or MX-SL-60M-DSP and TAOS 10.0 |
| MXHP-SL-DSP12 | MX-SL-48M-DSP or MX-SL-60M-DSP and TAOS 10.0 |
| MXHP-SL-DSP16 | MX-SL-48M-DSP or MX-SL-60M-DSP and TAOS 10.0 |
| MX-SL-DSP16-CO | MX-SL-48M-DSP or MX-SL-60M-DSP and TAOS 10.0 |
| MX-SL-8V110 | MX-SL-48M-DSP or MX-SL-60M-DSP and TAOS 10.0 |
| 300280872 | 300331550 or 300331543 and TAOS 10.0 |
| 300280856 | 300331550 or 300331543 and TAOS 10.0 |
| 300280864 | 300331550 or 300331543 and TAOS 10.0 |
| 407591262 | 300331550 or 300331543 and TAOS 10.0 |

| Discontinued product | Replacement product |
|---|---|
| 407591288 | No replacement |
| 407591270 | No replacement |

# Notice of end of sale for MAX 3000

January 25, 2002

Effective immediately, INS Edge Access Universal Gateway product management is serving sixty (60) days notice of the end of sale of the MAX 3000 remote access concentrator. Orders for these products will be accepted only until March 31, 2002 or until supplies last and will not be accepted thereafter. Software support ends January 25, 2003.

## Product codes impacted

The product codes effected by this end of sale notice are:

| Product code | Comcode |
|---|---|
| MX30-2E1-AC | 300268844 |
| MX30-2E1-AC-30 | 300268851 |
| MX30-2T1-AC | 300268885 |
| MX30-2T1-AC-24 | 300268893 |
| MX30-6BST-AC-12 | 300268927 |
| MX30-6BU-AC-12 | 300268935 |
| MX30-OSLIC | 300350980 |
| MX30-1E1-AC | no comcode |
| MX30-1T1-AC | no comcode |
| MX30-2T1-D48NA | no comcode |
| MX30-2E1-D60IX | no comcode |
| MX30-6BST-DEMO | no comcode |
| MX30-2E1-60-DEMO | no comcode |
| MX30-2E1-AC-60-P | no comcode |
| MX30-6BST-AC-12-P | no comcode |

| Product code | Comcode |
|---|---|
| MX30-HO-EC | 300268596 |
| MX30-HO-750E1 | 300268588 |

Product warranty, repair and technical support programs will continue for the duration of existing contracts.

## Replacement products

Replacement products may be priced higher than the products they replace. If so, existing contracts should be adjusted to reflect new prices. The replacement product for the MAX 3000 is the MAX 6000.

# *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 the 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 include the following:

- Always check a MAX 3000 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 for MAX does not support AppleTalk. Do not upgrade to TAOS 10.0 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, 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 are identical to RADIUS Accounting packets. With the introduction of 7.2.0, Call Logging is no longer compatible with RADIUS, although Lucent Technologies' Navis™Access product fully supports Call Logging. The MAX continues to support RADIUS accounting, SNMP and SYSLOG functionality.

  Because of the proprietary nature of and potential modification to Call Logging packets, you should not use Call Logging packets with any application other than Lucent Technologies' Navis™Access.

- Some multimedia enhancements are not supported in TAOS 10.0. Customers using the following enhancements should not upgrade to TAOS 10.0:

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

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

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

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

# MultiVoice® known issues

Known issues you should be aware of before upgrading a MAX 6000 unit to TAOS 10.0 include the following:

- 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 is 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.