Lucent Technologies
Bell Labs Innovations



TAOS 9.0.9 Release Note

for MAX™ 6000/3000/800

April 2, 2002

Copyright © 2001, 2002 Lucent Technologies Inc. All rights reserved.

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

Notice

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

European Community (EC) RTTE compliance

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

Section 1 Changing system software versions 1-1

Preparing to change system software 1-1
- Enabling Field Service and Operations parameters 1-1
- Staying with the same software build 1-2
- Alternative software builds for a MAX 6000 unit 1-2

Using TFTP to upgrade or downgrade 1-3
- Creating redundant backup images for a MAX 6000 unit 1-3
- Using TFTP to upgrade 1-4
- Using TFTP to downgrade 1-5

Using the serial port to upgrade or downgrade 1-5
- Saving your current profiles 1-6
- Upgrading system software 1-6
- Restoring passwords 1-7

Section 2 Introducing TAOS 9.0.9 2-1

Support for Proxy ARP added for MAX 3000 BRI units 2-13

Notice of update to the MRU parameter 2-13

Syslog now reporting L2TP session up 2-14
- VT100 interface changes 2-14
- Sample syslog messages 2-14

RADIUS username no longer truncated in syslog messages 2-14

Disconnect-cause and progress codes in Stop, Call, and LAN session information records now consistent 2-15
- MAX syslog record 2-15
- RADIUS Accounting Stop record 2-15
- Additional code combinations and their possible meanings 2-16

Unencrypted RADIUS attribute accepted by MAX unit 2-18

Support for routing of MultiVoice® and modem calls to appropriate terminating resources 2-19
- Changes to MultiVoice® loads 2-19
- Requirements for MAX 6000 units 2-19
- Requirements for MAX 3000 units 2-20

POTS support for VoIP call processing on the MAX 6000 2-20
- Call process signaling features 2-20
- MAXPOTS VoIP call routing 2-21

Changing system software versions 1

Preparing to change system software 1-1

Using TFTP to upgrade or downgrade 1-3

Using the serial port to upgrade or downgrade 1-5



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. For this reason, create and save a backup copy of the configuration file in the older format in case you ever need to revert to a previous version of TAOS. If you fail to create and save a backup copy of the configuration before you change a MAX unit's version of TAOS, you might lose all configuration information.



Caution If possible, use Trivial File Transfer Protocol (TFTP) to change a MAX unit's version of TAOS. TFTP is the most reliable way to obtain, store, and then change the version of TAOS.



Caution The standard software files you use to upgrade to TAOS 9.0.9 require additional flash memory available to the MAX 6000 unit only by way of an external PCMCIA flash card. (No additional memory is required on a MAX 3000 or a MAX 800 unit.)

Preparing to change system software

As you prepare to change the system software on a MAX, you must verify that the `Field Service` and `Operations` parameters are enabled on the unit. When upgrading, try to stay with the same build. But you can use an alternative build to avoid having to add memory.

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, make sure that the `Security` profile you use as an administrator is configured to support `Field Service` and `Operations`. For example, the following `Full Access` profile of a

MAX 800 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
```

Staying with the same software build

When a particular build of the system software is updating, it retains the same file-name. If possible, you should always stay with the same software build when you upgrade or downgrade. If you install a different version, your unit might lose its configuration. If this happens, you might need to manually restore your configuration. You might have no automated way to restore configuration data from a backup when changing builds, if the file formats between the builds are incompatible, because no suitable backup exists.

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

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

When the build is intended for 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.
```

If the build is intended for another type of unit, Lucent Technologies recommends not forcing the download.

Alternative software builds for a MAX 6000 unit

With two exceptions, the software builds you can use to upgrade to TAOS 9.0.9 require additional flash memory, available to the MAX 6000 unit only, by way of an external PCMCIA flash card. In order to avoid this requirement, you can upgrade a MAX 6000 unit with one the following two recommended software builds:

- `eik.m60` (an ultra-thin load for E1 environments)
- `tik.m60` (an ultra-thin load for T1 environments)

TAOS 9.0.9 introduces these recommended software builds. In future releases, these software builds might not be available, and so use of the MAX 6000 unit's external flash memory will become a requirement. This release includes a new feature to prevent a build that is too large from being placed in the unit's internal flash memory. If a build is too large, the unit terminates the download to the unit and displays the following message:

```
tftp download aborted due to flash write error
```

The MAX unit then restarts with its previous TAOS version and configuration intact. In releases before TAOS 9.0.9, the process appeared to complete successfully although TAOS was corrupted and the configuration unusable.

The `eik.m60` and `tik.m60` builds do not include support for the following features:

- AppleTalk
- ISDN Basic Rate Interface (BRI)
- IPX
- Personal Handyphone System (PHS)
- Plain old telephone service (POTS)
- X.25

Using TFTP to upgrade or downgrade

If possible, use TFTP to change a MAX unit's version of TAOS. TFTP is a more reliable way to obtain, store, and then change the version of TAOS than is the serial port alternative. With TFTP, you can use a MAX 6000 unit's external memory to create redundant backup images, as well as to upgrade the unit's version of TAOS.

Creating redundant backup images for a MAX 6000 unit

MAX 6000 units now support two copies of TAOS code on the PCMCIA flash memory card. If the first version of code becomes corrupt, the unit can boot up the second version.

To create the redundant backup image, proceed as follows:



Note The order of these two steps is not important, but the MAX unit will be unable to recover from a failure in the primary code image until you have performed both steps.

1 Create a backup copy of the currently running binary on the PCMCIA flash card by using the `fBackupImage` debug command. For example:

```
> 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 memory, using 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 204.253.164.44:69
file lvs.m60...
.


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

Using TFTP to upgrade

To upgrade with 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 use TFTP to upgrade system software, proceed as follows:

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

- The configuration that is compatible with the version of TAOS to which you will upgrade
- The build of the system software version to which you will upgrade

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

3 At the `>` prompt, use the `tsave-m` command to create 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 named `config800.cfg` from the TFTP home directory of the server named `tftp-server`:

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



Caution A 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 you ever need to revert back to the earlier version after you upgrade the unit to TAOS 9.0.9. 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
```

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

For example, the command:

`tloadcode tftp-server ebixk.m60`

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

5 Use the command immediately after executing the `tload code` command. Enter the following command to save your configuration to flash memory:

> **`fsave`**

6 Enter the following command:

> **`nvramclear`**

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

This completes the upgrade to TAOS 9.0.9.

Using TFTP to downgrade

To use TFTP to downgrade system software, you must follow the same steps as for upgrading TAOS with one exception. Instead of using the `fsave` command, as described in step 5 in "Using TFTP to upgrade" on page 1-4," enter the following command to restore the compatible configuration to flash memory:

`trestore -f hostname savedConfig`

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

For example, the following command places `Config803`, a configuration compatible with TAOS 8.0.3, from the unit named `tftp-server`:

`trestore -f tftp-server Config803`

Note The `-f` argument is necessary for downgrading. 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.

Using the serial port to upgrade or downgrade



Caution Upgrading system software through the serial console deletes all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. For security reasons, password information is not stored in backup files. If you have many passwords, consider using TFTP to upgrade your software. (For instructions, see "Using TFTP to upgrade or downgrade" on page 1-3.)

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

- An IBM-compatible PC or Macintosh system with a serial port capable of connecting to the MAX unit's Console port.
- A straight-through serial cable.
- Data communications software for your system, with terminal emulation (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.



Caution If you use a Microsoft Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs that could interrupt the file transfer. Failure to do so might cause the file transfer to halt, and can render the MAX unit unusable.

Saving your current profiles

Verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to the same rate as the `Term Rate` parameter in the `Sys Config` profile. You can cancel the backup process at any time by pressing Ctrl-C.

To save the MAX unit's configuration (except passwords) to disk:

1. Open the `Sys Diag` menu.
2. Select `Save Config`, and press Enter.

   The following message appears:

   ```
   Ready to download - type any key to start....
   ```

3. Turn on the Capture feature of your communications program, and supply a filename for the saved profiles. (Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.)
4. Press any key to start saving your configured profiles.

   Rows of configuration information appear on the screen as the configuration file is created on your hard disk. When the file has been saved, your communications program displays a message indicating that 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 through the MAX 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 Esc key, the Left Bracket key, the Esc key, and the Minus key, in that order, in rapid succession.) The following string of Xmodem control characters appears:

   ```
   CKCKCKCK
   ```

   If these characters do not appear, you probably did not press the four-key sequence quickly enough. Try again. Most people use both hands and keep one finger on the Esc key.
2. Use the Xmodem file-transfer protocol to send the system file to the unit.

   A 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. You can safely ignore any "bad batch" messages displayed by your communication program.
3. From the MAX unit's VT100 interface, access the diagnostics monitor by pressing Ctrl-D to invoke the `DO` menu and selecting `D=Diagnostics`.

4 At the > prompt, enter the `fclear` command:

```
> fclear
```

5 At the > prompt, enter the `nvramclear` command:

```
> nvramclear
```

This command causes the system to reset. When it comes back up, proceed with restoring your configuration.

6 Enter **`quit`** to exit the Diagnostic interface.

7 Open the `Sys Diag` menu.

8 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.

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

9 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.

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

Restoring passwords

Edit your configuration file and enter the word `*SECURE*` (including the asterisks) in each instance of a password. Save the file as a text-only file. When you use the `restore config` command, the unit's configuration file and the passwords are restored to the unit.



Note If you do not save the configuration as a text-only file, you will not be able to transfer it into the MAX unit.

If you restored a complete configuration, one without the modifications described above, then all the passwords used in your `Security` profiles have been wiped out. To reset them:

1 Press Ctrl-D to invoke the `DO` menu.

2 Select `Password`, and choose the `Full Access` profile.

3 When you are prompted to enter the password, press Enter (the null password).

4 After you have restored your privileges by entering the null password, immediately open the `Connection` profiles, `Security` profiles, and `Ethernet` profile (`Mod Config` menu), and reset the passwords to their previous values.

Introducing TAOS 9.0.9

2

Problems corrected in TAOS 9.0.9 2-1

Firmware versions included with TAOS 9.0.9 2-3

Notice: Support to end for voice DSP modules 2-4

Known issues with TAOS 9.0.9 2-4

Problems corrected with releases prior TAOS 9.0 releases. 2-5

Enhancements introduced in previous releases. 2-12



Note With this release, True Access™ Operating System (TAOS) continues to include improved resistance to Denial of Service attempts.

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 9.0.9 you see a smaller amount of available memory on the MAX than was available to a unit that ran a previous TAOS release. This is because the software binaries have gotten bigger and the memory used to store those software binaries is greater.

This True Access™ Operating System (TAOS) maintenance release supports MAX 6000, MAX 3000, and MAX 800 units.

Problems corrected in TAOS 9.0.9



Note Previous release notes referred to problems corrected by a trouble report (TR) number. With this release, each trouble report is now referred to as a *change request* or *CR*.

Table 2-1 lists the problems corrected in TAOS 9.0.9 in numerical order by customer reports (CR).

Table 2-1. Problems corrected in TAOS 9.0.9

CR number	Problem corrected
6002335	A MAX unit configured to support RADIUS authentication did not correctly process user sessions.
6002471	A MAX 6000 unit displayed incorrect High-Level Data Link Control (HDLC) channel information when the unit processed the `show users` diagnostic command.
6002537	A MAX unit configured to support Ascend® Tunnel Management Protocol (ATMP) did not transfer RADIUS attribute 23 (IPX network node) as expected.
6002539	A MAX unit did not correctly support E1-PRI signaling for Taiwan.
6002567	Callers sometime heard clicking sounds immediately after the unit dialed a destination phone number.
7000018	A MAX unit's V.90 S56 III modem cards used Mindspeed firmware version 5.8177.
7000019	A MAX unit incorrectly rejected some RADIUS attributes' formats.
7000068	Under a heavy load consisting small packets sent at a high rate, a MAX 3000 unit's serial WAN did not transfer packets.
7000090	A MAX unit configured to support Q.922 and I.370 incorrectly cleared (reset to zero) the following frame relay-related bits: ■ Forward explicit congestion notification (FECN) ■ Backward explicit congestion notification (BECN) ■ Discard eligibility (DE)
7000099	A Max 3000 unit reset and displayed an `FE1` message.
7000126	A MAX unit incorrectly added routing entries and summarized pools although the unit's `Pool Summary` parameter specified `No`.
7006378	Point-to-Point Tunneling Protocol (PPTP) X.75 and V.120 asynchronous framing were not implemented.
7006382	See CR 7000099.
7006398	A MAX 6000 unit configured to support T1 inband signaling did not reliably process L2TP calls.

Table 2-1. Problems corrected in TAOS 9.0.9 (Continued)

CR number	Problem corrected
7006406	A MAX unit's attempt to dial out using Basic Rate Interface Integrated Services Digital Network (BRI-ISDN) failed when the local telephone company did not support Layer 2 Q.921.
7006481	When a MAX 3000 unit's PRI switch type specified `Japan`, the unit failed to connect an Ascend® Inverse Multiplexing (AIM) call.
7006497	A MAX 6000 unit did not complete a T1 rollback test DSX CSU inband.
7006656	A MAX unit configured by means of a RADIUS server to use `Source IP` filters applied the filters incorrectly.
7006664	Calls failed when they originated from a MAX unit processing ingress Voice over Internet Protocol (VoIP) calls with E1-R2 signaling and terminated on a unit processing egress VoIP calls with Primary Rate interface (PRI).
7006696	During periods of heavy X.25 traffic, a Max 6000 unit corrupted Link Access Process, Balanced (LAPB) T1 timer information.
7006697	A MAX 6000 unit did not send a LinkDown SNMP trap packet as expected when the `Link Up` parameter specified `No`.
7006741	When a Max 6000 unit could not complete an Ascend® Tunnel Management Protocol (ATMP) connection, the unit reset and displayed several warning and `FE` messages.
7006937	When a MAX unit's `Immediate Service` parameter specified `Enabled`, the unit did not send a message indicating the unit was unable to establish a session with a dial-in client.
7006946	A MAX 6000 unit configured to support network address translation (NAT) reset with `Warning 104` when the unit received packets from a private network.

Firmware versions included with TAOS 9.0.9

This release supports the following firmware versions:

- Series56™ Digital Modem 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 S56 III modem cards (Series56™ III Digital Modem modules)—Mindspeed Technologies firmware version V5.8175 includes support for K56flex, K56plus, and all slower, standard modem speeds.

Notice: Support to end for voice DSP modules



Note This notice does not apply to MultiDSP modules which are not supported by TAOS 9.0.9. TAOS 9.1 will 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 units.

TAOS support for the previous generation of voice DSP modules (such as VDSP-16) 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. TAOS releases beginning with 9.2 will not support voice DSP modules and no further enhancements or problem corrections will be developed for these modules.

A voice DSP module's product warranty, repair, and technical support programs continue for the duration of existing contracts. However, the hardware is no longer available for sale.

Known issues for TAOS 9.0.9

Issues to be aware of before loading release 9.0.9 include the following:

- Logical gateways allow each incoming call to a Voice-over-IP (VoIP) Gateway to have its own set of Authentication, Dial Mode, and Announcements (ADMA) configuration parameters. At the ingress gateway, the incoming trunk group number is normally collected from, sent to and used by the Gatekeeper for appropriate call handling.

  When a VoIP call originates from a MAX 6000 unit, the unit does not correctly report ingress trunk group information. This issue adversely affects performance of the unit's ADMA rules and multiple logical gateway (MLG) controllers. Where ADMA rules rely on Access Trunk group information for incoming call treatment (for example, routing, announcements, and authentication) the rules will fail when using this release on a MAX 6000 unit.

  One exception to this issue is that when a MAX 6000 unit is operating as the far-end gateway, the information is reported correctly.

- When you attempt to initiate the terminal services TCP-clear, Rlogin, or Telnet using a scripted login, a MAX unit might occasionally terminate the call abnormally, displaying a disconnect-cause code `51` and progress code `40` in `syslog` or RADIUS Accounting records. This issue is aggravated by scripted logins where the responses are entered before the MAX solicits input.

- TAOS 9.0.9 for MAX does not support AppleTalk. Do not upgrade to TAOS 9.0.9 if your network requirements include support for AppleTalk.

- In TAOS 9.0.9, when the MAX unit experiences a long-term loss of communication to a RADIUS or call-logging server (with resulting loss of data), the unit reports the event by generating a `Warning 104` message.

- In releases prior to TAOS 7.2.0, the format of call-logging packet is identical to RADIUS Accounting packets. With the introduction of TAOS 7.2.0, call-logging is no longer compatible with RADIUS, although the Lucent Technologies NavisAccess™ product fully supports call logging. The MAX continues to support RADIUS Accounting, SNMP, and `syslog` functionality.

Because of the proprietary nature of and potential modification to call-logging packets, do not use call-logging packets with any application other than the Lucent Technologies NavisAccess™ software.

- The maximum total bandwidth supported by the Host/6 (AIM/6) inverse multiplexing slot card is 32 channels. This limit represents the total number of simultaneously supported active channels across all 6 ports. Attempts to exceed this 32-channel limit might cause the unit to reset.
- T1 PRI lines configured to use non-facility associated signaling (NFAS) are limited to 23 channels on the PRI line that does not utilize the D channel. Attempts to originate or terminate a call over channel 24 will fail to connect. Bandwidth must be limited to channels 1 through 23.
- In a previous release, the default value for the `CBCP Trunk group` parameter was out of the valid range. The default value has been changed from 0 to 4. This correction might cause a previously saved profile to yield a different value when this release is loaded.
- In MAX units, data flows between T1 or E1 WAN ports and host devices, such as modems and HDLC ports, using a limited group of internal data pathways. The capacity of these pathways is sufficient to accommodate the built-in WAN ports of the MAX. When ISDN BRI cards are installed in the system, pathways normally allocated for built-in T1 or E1 ports are used to support the BRI WAN ports and are not available for T1 or E1 usage. Table 2-2 summarizes how the addition of BRI cards affects the availability of built-in WAN ports in various MAX units. These limits apply regardless of the type of BRI card used (network-interface card, terminal-interface card, or IDSL card).

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

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

Problems corrected with releases prior to TAOS 9.0

Table 2-3 includes all problems corrected by previous TAOS 9.0 releases except those related to MultiVoice® support. (See Table 2-4 on page 2-11 for MultiVoice® problems

corrected by previous TAOS 9.0 releases.) The problems corrected are presented in order by trouble report (TR) number.

Table 2-3. Problems corrected with previous TAOS 9.0 releases

TR number	Problem corrected
5401	A MAX unit sent duplicate address-free requests when a PPP session ended.
5452	A MAX unit configured to support AppleTalk displayed a `Warning 104` message.
6000541	A MAX unit having two installed modem slot cards and configured to support switched T1 did not successfully utilize its second installed modem slot card to initiate calls.
6000632	A MAX unit configured to support ISDN Digital Subscriber Line (IDSL) reset and issued fatal-error 1 (FE1).
6000657	A MAX unit disconnected calls that required a callback style of authentication such as Callback Control Protocol (CBCP).
6000743	A MAX unit limited the maximum number of simultaneous X.25 sessions to 64.
6000928	When all ports on a PHS Internet Access Forum Standards (PIAFS) slot card were busy, a MAX unit did not send the correct `USER_BUSY` message for an incoming call.
6001036	When a PPP session timed out on a MAX unit, the unit sent duplicate `address-free` requests.
6001049	A MAX 3000 unit did not utilize the available BRI ports on an installed slot card to support nailed BRI.
6001059	A MAX unit configured to support R2 signaling in Egypt and Thailand did not process incoming calls correctly.
6001085	A MAX unit did not correctly authenticate users whose RADIUS-defined configuration enabled the callback feature.
6001088	A MAX unit's `Area Type` parameter did not set OSPF header information correctly.
6001140	A MAX unit reset and displayed an `Invalid modem selected` message.
6001141	When the software build stored on the MAX 6000 unit's external PCMCIA flash card became corrupted, the unit did not restore the previous software build from flash memory.

Table 2-3. Problems corrected with previous TAOS 9.0 releases (Continued)

TR number	Problem corrected
6001179	On a MAX 6000 unit's WAN interface, support for IPX ping did not function correctly.
6001202	A MAX configured as a fax server reset with a `Warning 106` message.
6001253	A Windows PC user could not establish a Telnet session to a MAX unit over a path that included at least one hop.
6001267	The disconnect reason and the progress code in a MAX unit's `syslog` were inconsistent or incorrect.
6001300	A MAX unit did not provide a correct value for RADIUS `Ascend-Third-Prompt (213)`.
6001311	A MAX 6000 unit did not present the IP address of each frame relay connection to an SNMP manager.
6001312	A MAX unit configured to use static routes issued Warning 106 and then reset.
6001317	A MAX reset and displayed FE1 when it attempted to process a call placed from another manufacturer's gateway.
6001326	A MAX unit did not support the optional virtual router feature when the unit's `Sys Options` profile indicated `Rte Ptls=Disabled`.
6001360	A MAX unit's `syslog` did not display the correct end-of-call messages for disconnected V.110, PHS, and modem calls.
6001443	A MAX unit did not report a username in the unit's `syslog` when an L2TP tunnel failed to establish.
6001449	A MAX unit configured to support SNTP did not include support for full range of Universal Time offset settings (-1130 to +1300).
6001467	A MAX unit configured to support V.90 S56 III modem cards (Series 56™ III Digital Modem modules) did not display disconnect-cause code 11.
6001496	A MAX unit configured to support R2 signaling did not clear links that remained active after a called party disconnected.
6001515	A raw TCP connection failed and issued a `No memory for session` message.
6001525	A MAX 6000 unit issued a `Warning 109` and then reset.
6001544	A MAX unit processed dial-in user sessions when the unit was configured to utilize MP, Callback, and RADIUS.

Table 2-3. Problems corrected with previous TAOS 9.0 releases (Continued)

TR number	Problem corrected
6001561	A MAX unit's `syslog` did not reflect messages when the control channel and the data channel of an L2TP tunnel were established.
6001581	A MAX 6000 unit's dedicated (or *nailed*) BRI connection drifted.
6001678	When a MAX unit reestablished a nailed MultiLink Protocol Plus™ (MP+) link, the unit did not correctly bundle the link's two channels.
6001690	A MAX 6000 unit did not display correct TAOS version information in response to the `fVersionInfo` diagnostic command.
6001708	A MAX unit dropped calls when configured to support non-facility associated signaling (NFAS) and the unit's line interface settings changed.
6001713	A MAX 6000 unit that received a RIP update stopped forwarding packets and updating the unit's VT100 interface for several seconds.
6001717	L2TP tunnel authentication failed on a MAX unit configured as an L2TP network server (LNS).
6001723	A MAX unit did not log messages for connections through L2TP in its Status window.
6001738	A MAX unit did not support Multicast RIP updates correctly.
6001742	A MAX unit did not recognize V.90 S56 III modem cards (Series 56™ III Digital Modem modules).
6001762	A MAX unit did not correctly reset the RADIUS permanent connection profiles it displayed.
6001768	A MAX unit configured to operate as a gateway reset without fatal error after issuing `Warning 179` and `Warning 104` messages.
6001773	TAOS software loads for MAX 3000 BRI units (`m30abxkh` and `m30bixkh`) did not include proxy ARP support.
6001861	MAX units did not authenticate a dial-in user's session when a unit was configured to support 16-bit vendor-specific RADIUS attributes.
6001900	MAX units did not support Ethernet machine interface (MIF) commands.
6001901	A MAX unit did not accurately process the values specified for the `Frame Relay MRU` parameter.

Table 2-3. Problems corrected with previous TAOS 9.0 releases (Continued)

TR number	Problem corrected
6001928	A MAX 3000 unit did not restore an ATMP profile after the unit processed an fsave nvramclear command sequence.
6001935	A MAX unit did not correctly set bits for the RADIUS Proxy Authen Type (AVP 29) and Proxy Authen ID (AVP 32) attributes and attribute-value pairs.
6001936	A stacked MAX unit configured to support MultiLink Protocol Plus™ (MP+) reset and displayed FE1 with FE385.
6001975	A MAX unit with V.90 S56 III modem cards (Series 56™ III Digital Modem modules) installed issued Warning 179 message.
6001980	MAX 6000 units running ebiwxk.m60 did not recognize installed V.90 S56 III modem cards (Series 56™ III Digital Modem modules).
6001989	A MAX unit did not support an Ethernet machine interface (MIF) dial command as expected.
6002016	A MAX unit's syslog displayed inaccurate lan session info messages.
6002017	A MAX unit did not correctly process a Telnet session to the unit's port 5000 when the session was initiated by means of an NT Telnet client.
6002076	L2TP-related parameters did not process RADIUS variables that were the maximum allowable length (253 characters).
6002091	A MAX unit's dedicated (or *nailed*) MultiLink Protocol Plus™ (MP+) channels inconsistently sent RIP updates after a call disconnected.
6002118	A MAX unit issued a Warning 179 message when the unit reset.
6002136	A MAX 3000 BRI unit configured to support an installed Host/6 (AIM/6) inverse multiplexing card did not correctly process a call when the Use Trunk Grps parameter specified No.
6002141	A MAX 3000 unit did not correctly process the settings specified for parameters related to immediate modem services.
6002142	The E1/R2 links remained inactive after a called party had terminated a call.
6002145	A MAX Multiband® unit, configured to support ISDN, incorrectly specified a Call-by-Call parameter setting of N/A.

Table 2-3. Problems corrected with previous TAOS 9.0 releases (Continued)

TR number	Problem corrected
6002155	A MAX 3000 unit configured to support MultiVoice® did not complete T1-to-PRI conversions.
6002163	A MAX 3000 BRI unit did not have the same analog encoding options as other MAX units.
6002170	When network traffic was heavy, a MAX unit did not correctly support BACP.
6002197	When a MAX unit processed a `diag -t` diagnostics command, it did not display the correct system date and time.
6002233	See TR 6002143.
6002261	A MAX unit did not send an alert when it was stacked with another unit that ran a different version of TAOS.
6002366	A MAX unit truncated longer `syslog` messages.
6002369	Two-channel MultiLink Protocol Plus™ (MP+) calls failed to connect over two nailed T1 lines.
6002416	A MAX unit's incorrect support for RADIUS Accounting lead the unit to refer to a secondary RADIUS server.
6002423	A MAX unit running MultiVoice® Gateway software and configured to use B3 for busy tones had its signaling mode set for Brazil. When functioning as an egress gateway, the unit did not recognize a busy tone and returned a cause code 17.
6002456	The process of upgrading corrupted a MAX 6000 unit's internal flash memory.
6002457	A MAX 6000 E1 unit displayed a `corrupted load id` message.
6002494	See TR 6002366.
6002506	A MAX unit's routing table did not reflect (Routing Information Protocol (RIP) updates.
7000112	Changes to `X.3 Param Prof` parameter settings did not modify `X.25/PAD Connection` profiles as expected.

Table 2-4 includes all MultiVoice® problems corrected by previous TAOS 9.0 releases. (See Table 2-3 on page 6 for all other problems corrected by previous TAOS 9.0

releases.) Where possible, the problems corrected are presented in numerical order by change request (CR) number.

Table 2-4. MultiVoice® problems corrected with previous TAOS 9.0 releases

CR number	Problems corrected
N/A	A MAX unit issued a `Warning 106` message and reset on T1 ISDN, running G.711 protocol.
N/A	No media were available after a MAX unit received Request Modify Packet Pass-Through Call (RMPC) messages.
N/A	The H.245 open logical channel (OLC) procedure needed alteration so that it could handle the dialpad Gateway.
N/A	Receiving interrupt request registers (IRRs) were not processing, resulting in multiple transmissions of Information Request (IRQ) messages.
N/A	Internet Call Waiting was not working when the Multiple Logical Gateway was added to the gateway.
6001095	The ingress gateway was not informing MultiVoice® Access Manager (MVAM) through the remote access server (RAS) admission request (ARQ) message when the call was being redirected to the gateway.
6001324	A MAX unit issued a `Warning 109` message and reset with index 385 when it was configured to interact with another manufacturer's gatekeeper.
6001330	A Max unit did not set the mandatory bit for `Rx Connection Speed` attribute-value pair (AVP).
6001444	The end-0f-call record in a A MAX unit's `syslog` did not display all 253 possible characters of the username.
6001447	A MAX unit could not complete a fax between fax machines in high latency mode.
6001458	A MAX unit recorded busy calls incorrectly as having cleared normally.
6001487	There was excessive delay between announcements in the play list.
6001488	A MAX unit did not allow a complete message to be announced to a caller at the time that they connected.
6001498	Calling party category was not sent transparently from ingress to egress.

Table 2-4. MultiVoice® problems corrected with previous TAOS 9.0 releases

CR number	Problems corrected
6001499	E1/R2 calls did not complete when the `Number Complete` was set to `Timeout`.
6001513	A MAX unit did not enable a user to set the `Country` parameter in the unit's `Sys Config` profile to `New Zealand`.
6001516	A MAX unit configured to support two-stage calling and set to `g728` did not return a busy signal as expected.
6001574	A MAX unit did not propagate a configured calling line ID (CLID) through the egress gateway when the calling number started with a zero (`0`).
6001606	This CR includes two related issues: ■ A MultiVoice® ingress gateway configured to support E1 CAS single stage dialing with True Connect timed out if a call is was not answered in 12 seconds. ■ When the `Near End Cut Through` parameter specified `No` on a MultiVoice® ingress gateway, the MultiVoice® egress gateway timed out if a call was not answered in 60 seconds.
6001694	A large number of call failures occurred after six days' operation of a MAX 6000 unit.
6002143	A MultiVoice® Gateway did not successfully place fax calls to some destinations. The MultiVoice® Gateway failed to report fax V.21 flags after it detected a phase-reversal CED that prevented completion of T.38 faxes placed to (or from) some manufacturer's fax machines.
6009891	Prompting for and collecting dual-tone multi-frequency (DTMF) with break-ins caused periods of silence.

Enhancements introduced in previous releases

The following enhancements were introduced in previous TAOS 9.0 releases:

■ "Support for Proxy ARP added for MAX 3000 BRI units" on page 2-13
■ "Notice of update to the MRU parameter" on page 2-13
■ "Syslog now reporting L2TP session up" on page 2-14
■ "RADIUS username no longer truncated in syslog messages" on page 2-14
■ "Disconnect-cause and progress codes in Stop, Call, and LAN session information records now consistent" on page 2-15
■ "Unencrypted RADIUS attribute accepted by MAX unit" on page 2-18

■ "Support for routing of MultiVoice® and modem calls to appropriate terminating resources" on page 2-19

■ "POTS support for VoIP call processing on the MAX 6000" on page 2-20

Support for Proxy ARP added for MAX 3000 BRI units

Lucent units affected: MAX 3000 BRI

Introduced in: TAOS 9.0.3

If Proxy Address Resolution Protocol (Proxy ARP) is enabled on a MAX unit, it can handle address resolution requests for another device. This release adds support for Proxy ARP to the following TAOS software binaries:

■ `m30abxkh`

■ `m30bixkh`

As in previous TAOS releases, these software binaries include features that support ISDN BRI for MAX 3000 units.

The `Proxy Mode` parameter specifies support for Proxy ARP. Following is a sample setting of the `Proxy Mode` parameter specifying that Proxy ARP is active on a MAX unit:

```
90-D00 Mod Config
 Ether options...
  IP Adrs=208.211.252.19/24
  2nd Adrs=0.0.0.0/0
  RIP=Off
  2nd RIP=Off
  RIP2 Use Multicast=No
  Ignore Def Rt=Yes
 >Proxy Mode=Active
  Filter=1
  IPX Frame=None
```

For more information on Proxy ARP and configuring a unit to support the protocol, see the documentation supplied for your MAX unit.

Notice of update to the MRU parameter

Lucent units affected: MAX 6000, MAX 3000, MAX 800

Introduced in: TAOS 9.0.3

The `MRU` parameter value, located in `Ethernet > Frame Relay`, now has a maximum value of 1532 (bytes). The minimum number of bytes that a MAX unit can receive in a single frame remains at 128.

Syslog now reporting L2TP session up

Lucent units affected: MAX 6000, MAX 3000, MAX 800

Introduced in: TAOS 9.0.3

In previous releases, a MAX unit did not log any messages when the control channel and the data channel of an L2TP tunnel were established. Now, each unit generates the appropriate messages.

VT100 interface changes

A MAX unit logs new messages to the `syslog` server. The log-message level is `informational`.

When the control channel is established and the unit is acting as an L2TP access concentrator (LAC) or an L2TP network server (LNS), the unit logs the following message:

`TUNNEL-`*`session_ID`*`, L2TP Control Channel up with `*`peername`*

When the data channel is established and the unit is acting as a LAC or an LNS, the unit logs the following message:

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

When the tunnel is deactivated and the unit is acting as a LAC or an LNS, the unit logs the following message:

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

Sample syslog messages

Following are sample `syslog` messages that can appear when a MAX unit is operating as a LAC:

```
Feb 9 12:09:26 englab30-63.dev.eng.ascend.com TUNNEL-1, L2TP Control Channel
up with pjmax2

Feb 9 12:09:26 englab30-63.dev.eng.ascend.com TUNNEL-1, L2TP Data Channel up
with pjmax2 [MBID 1]

Feb 9 12:11:26 englab30-63.dev.eng.ascend.com TUNNEL-1, L2TP Tunnel Cleared:
result code 0, error code 0
```

Following are sample `syslog` messages that can appear when a MAX unit is operating as an LNS:

```
Feb 9 11:17:42 englab30-82.dev.eng.ascend.com TUNNEL-4, L2TP Control Channel
up with tnt

Feb 9 11:17:42 englab30-82.dev.eng.ascend.com TUNNEL-4, L2TP Data Channel up
with tnt [MBID 2]

Feb 9 11:18:42 englab30-82.dev.eng.ascend.com TUNNEL-4, L2TP Tunnel Cleared:
result code 0, error code 0
```

RADIUS username no longer truncated in syslog messages

Lucent units affected: MAX 6000, MAX 3000, MAX 800

Introduced in: TAOS 9.0.3

In a `syslog End-of-Call` message, the username associated with a RADIUS-authenticated dial-in session can now contain up to 253 characters. Formerly, the username was truncated at 31 characters.

Following is a sample `syslog End-of-Call` record display:

```
01-26-2001 14:52:34  Local0.Info  200.168.21.70   ASCEND: shelf 1 slot 1
port 2, LAN session info, Conn=("l2tp-test112345678921234567893
12345678941234567895" ?->? PPP 46000/28800 60/1 192.168.21.71) Auth=(22
335/11 291/12) Sess=(33 335/11 291/12) Chan=(1 1 1 21) Modem=(1 4 2)
Tunn=(L2TP s=204.253.164.1) [MBID 2]
```

Disconnect-cause and progress codes in Stop, Call, and LAN session information records now consistent

Lucent units affected: MAX 6000, MAX 3000, MAX 800

Introduced in: TAOS 9.0.3

The disconnect-cause and progress codes appearing in different records are now consistent with each other.

Previously, at the end of a call, the disconnect-cause and progress codes listed in a Stop record or Call record sometimes differed from those listed in a `LAN session info` record or RADIUS Accounting Stop packet. In addition, sometimes disconnect-cause code 1 (which should not be listed for any call) appeared. These problems have now been fixed.

MAX syslog record

The following `syslog` record shows the disconnect-cause and progress codes as 2:

```
Nov 28 11:44:26 mytnt ASCEND: shelf 1 slot 8 port 1, Assigned to port, MBID
026 [MBID 26]

Nov 28 11:44:26 mytnt ASCEND: ENCAP-3: Outgoing call, no interface for host
dialout.

Nov 28 11:44:26 mytnt ASCEND: CL 0K u=dialout c=2 p=2 h=0.0.0.0 [MBID 26]

Nov 28 11:44:26 mytnt ASCEND: shelf 1 slot 1 port 3, LAN session info,
Conn=("?" ?->? ? 56000/56000 2/2) Auth=(0 0/0 0/0) Sess=(0 0/0 0/0) Modem=(1
8 3) [MBID 26]
```

RADIUS Accounting Stop record

The following RADIUS Accounting Stop record shows the disconnect-cause and progress codes as 2.

```
Tue Nov 28 11:44:26 2000
      NAS-Identifier = 210.210.210.236
      NAS-Port = 0
      NAS-Port-Type = Sync
      Acct-Status-Type = Stop
      Acct-Delay-Time = 0
```

```
Acct-Session-Id = "344185618"
Ascend-Disconnect-Cause = 2
Ascend-Connect-Progress = 2
Ascend-Xmit-Rate = 56000
Ascend-Data-Rate = 56000
Ascend-PreSession-Time = 0
Ascend-Pre-Input-Octets = 0
Ascend-Pre-Output-Octets = 0
Ascend-Pre-Input-Packets = 0
Ascend-Pre-Output-Packets = 0
Ascend-Modem-PortNo = 3
Ascend-Modem-SlotNo = 8
Ascend-Modem-ShelfNo = 1
```

Additional code combinations and their possible meanings

A MAX unit applies a disconnect-cause code and progress code to each call. Combinations of disconnect-cause and progress codes might indicate similar causes. Following is a list of additional code combinations and their possible causes. See the documentation that came with the unit for more complete lists of disconnect-cause codes, progress codes, and code combinations.

Disconnect-cause code	Progress code	Possible cause
1	10	The MAX unit had detected and accepted the call, but the call was not completed. A disconnect-cause code 1 is typical in Accounting Checkpoint records. In any other case, contact technical support at `http://www.lucent.com/support` if a unit displays disconnect-cause code 1.
2	2	A disconnect-cause code 2 or progress code 2 are default values than mean *unknown*. The unit displays 2 for disconnect and progress events for which it has no definition.
11	66	After successfully negotiating PPP Compression Control Protocol (CCP), the MAX unit's modem lost the carrier signal that a modem connection requires. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or, the modems might be incompatible.
22	40	During an active terminal-server session, the user forced a disconnect from the client's terminal-server application when exiting a Telnet session. Typically, the call was established successfully.

Disconnect-cause code	Progress code	Possible cause (Continued)
39	60	During an active session, the unit closed the PPP session because all active Network Control Protocols (NCPs) were closed. During a PPP session, the unit's must negotiate successful NCPs, either Bridging Network Control Protocol (BNCP), Internet Control Protocol (IPCP), or IPX Control Protocol (IPXCP), or some other Network Control Protocol (NCP). If either unit closes all open NCPs, the other unit closes the PPP session. Typically, the call was a successful session.
45	67	Before a PPP session was completely established, the units had begun negotiating the IP Network Control Protocol (NCP). The MAX unit received a Terminate Request packet from the client application, requesting that PPP negotiations stop. The MAX unit complied with the request.
181	66	During PPP negotiation, the MAX unit and client application successfully negotiated PPP Compression Control Protocol (CCP). Because of inferior line quality or modem incompatibilities, the unit disconnected the call. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.
185	2	Shortly after answering a call, the MAX unit could not detect any signal from the computer's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.
185	32	Shortly after answering a call, while the MAX unit's modem was awaiting result codes from the client's modem, the unit could not detect any signal from the computer's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.
185	44	Shortly after making a successful connection to the Telnet host, the MAX unit could not detect any signal from the computer's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.

Disconnect-cause code	Progress code	Possible cause (Continued)
185	47	During a terminal-server session, the MAX unit could not detect any signal from the user's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.
185	66	The MAX unit and client application successfully negotiated PPP Compression Control Protocol (CCP). During PPP negotiation, the MAX unit could not detect any signal from the user's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.
185	67	The MAX unit successfully negotiated Link Control Protocol (LCP) and authentication with the dial-in client. During Internet Protocol Control Protocol (IPCP) negotiation, the unit could not detect any signal from the user's modem. Typically, the modems had marginal line quality. This problem usually results from poor line quality between the user's modem and its local central office (CO), because the unit's modem has a digital connection to the CO. Or the modems might be incompatible.

Unencrypted RADIUS attribute accepted by MAX unit

Lucent units affected: MAX 6000, MAX 3000

Introduced in: TAOS 9.0.3

A new parameter named `Allow Unencryp Tun Passw` enables you to specify whether a MAX unit accepts a Remote Authentication Dial-in User Service (RADIUS) `Tunnel-Password` attribute that is not encrypted. The `Allow Unenryp Tun Passw` parameter is located in the `Ethernet > Mod Config > Auth` profile. The parameter applies only when the `Auth` parameter, also located in the `Ethernet > Mod Config > Auth` profile, specifies `RADIUS` or `RADIUS/LOGOUT`.

In previous releases, a MAX unit accepted a Remote Authentication Dial-in User Service (RADIUS) `Tunnel-Password` attribute only when the RADIUS server encrypted the attribute, as specified by RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*. The `Allow Unencryp Tun Passw` parameter enables you to comply with the RFC or to accommodate a unique case where the RFC does not apply.

Allow Unencryp Tun Passw

Description Specifies whether a MAX unit accepts a Remote Authentication Dial-in User Service (RADIUS) `Tunnel-Password` attribute that is not encrypted.

Usage Specify `Yes` or `No` (the default).

Example `Allow Unencryp Tun Passw=No`

Dependencies The `Allow Unencryp Tun Passw` parameter applies only when the `Auth` parameter, located in the `Ethernet > Mod Config` profile, specifies `RADIUS` or `RADIUS/LOGOUT`.

Location `Ethernet > Mod Config > Auth`

Support for routing of MultiVoice® and modem calls to appropriate terminating resources

Lucent units affected: MAX 6000, MAX 3000

Introduced in: TAOS 9.0.1

With this release, you can configure support for routing of MultiVoice® and modem calls to appropriate terminating resources. The terminating resources can now be MultiVoice® DSP 16-port slots and V.90 S56 III modem cards (Series56™ III Digital Modem modules) installed in a single MAX unit.

Changes to MultiVoice® loads

MultiVoice® loads of the True Access™ Operating System (TAOS) now support termination of modem access services, including full terminal server and framed protocol support. Following are other modem access services supported by these loads:

- Bandwidth Allocation Control Protocol (BACP)
- Multilink Protocol Plus™ (MP+)
- Multilink PPP (MP)
- Point-to-Point Protocol (PPP)
- `rlogin` utility
- Store-and-Forward Fax
- TCP-Clear
- Telnet
- Termination of High-Level Data Link Control (HDLC) protocol

MultiVoice® loads now provide the following diagnostics commands:

- `modemdrv debug`
- `modemdiag (AT&V2)`

Requirements for MAX 6000 units

A single MAX 6000 unit with the following options installed can support MultiVoice® and modem access features:

- 32MB DRAM
- One V.90 Series56™ III Digital Modem module (or Series56™ Digital Modem module)
- One VDSP-16 module

The following loads support MultiVoice® and modem access features for MAX 6000 units:

- `m60t1bikv`
- `m60e1bikv`

Requirements for MAX 3000 units

A single MAX 3000 unit with the following options installed can support MultiVoice® and modem access features:

- One V.90 Series56™ III Digital Modem module
- One VDSP-16 module

The following loads support MultiVoice® and modem access features for MAX 3000 units:

- `m30t1bikv`
- `m30e1bikv`

POTS support for VoIP call processing on the MAX 6000

Lucent units affected: MAX 6000 T1, MAX 6000 E1

Introduced in: TAOS 9.0.1

The MAXPOTS foreign exchange station (FXS) slot card provides a plain old telephone service (POTS) interface for initiating Voice over IP (VoIP) calls on a MAX 6000 unit configured as a MultiVoice® Gateway. VoIP call processing enables a MAX 6000 to route VoIP calls between

- Analog and digital (T1 PRI or E1 PRI) telephone devices
- Two analog telephone devices
- Two digital telephone devices

Call process signaling features

The MAXPOTS card utilizes a digital signal processor (DSP) modified to recognize and respond to Q.931 call process signaling messages. This includes the following support for ISDN PRI call process signaling features:

- DTMF dial digit detection.
  - Minimum detection level of -26 decibels referred to 1 milliwatt (dBm).
  - DTMF dial digit detection is enabled for a minimum of 40ms.
- Pulse dial digit detection.
  - 7.5 to 12 pulses per second.
  - Break ratio 40% to 80%.
- Call progress tone generation.

  - Output level at -20dBm per tone.
- On-hook and off-hook detection.
  - On-hook-to-off-hook qualification time of 100ms.
  - Off-hook-to-on-hook qualification time of 600ms.
- Ringback tone generation.
  - Output level at -15dBm.
- Caller-ID generation.
  - Send date, time, and calling number information.
  - Output level at -15dBm.
- Ringing generation.
  - Two seconds on (active cycle) and four seconds off (inactive cycle).
  - At most three telephones in an active ring cycle simultaneously.
- Ground start or loop start.
- Configurable transmit and receive gain. Actual ranges available to the user are determined by the configuration screen in core software. “Receive” is the direction from the connecting device to MAXPOTS. “Transmit” is the direction from MAXPOTS to the connecting device.
- Forward disconnect. In loop start, a loop is opened for 1 second during forward disconnect.

Call process signaling caveats

The following limitations and caveats apply to MAXPOTS call process signaling features:

- With a receive gain of 0db, MAXPOTS converts an analog signal of 0dBm to μ-law pulse-code modulation (PCM) samples of 0dBm level.
- Receive signal level plus the receive gain must not exceed 0 dBm. For example, the receive gain for a signal of -2dBm should be less than 2dB (-2 + 2 = 0).
- With a transmit gain of 0dB, MAXPOTS converts μ-law PCM samples of 0dBm level to an analog signal of 0dBm level.

  Output levels of the call progress tone and caller ID signal are relative to a transmit gain of 0dB. Changing the transmit gain changes these output levels. For example, setting the transmit level to -10dB changes the call progress output level to -30dB (-20 - 10) and caller ID level to -25dBm (-15 - 10).

MAXPOTS VoIP call routing

VoIP calls originating from telephone devices attached to MAXPOTS ports execute basic call setup—using no gatekeepers—as defined by ITU Telecommunication sector standard (ITU-T) H.323, *Packet-based multimedia communications systems* (Feb. 1998), International Telecommunications Union. The ingress MAX 6000 communicates directly with the egress MAX 6000 during call setup. The call routing to the destination MultiVoice® Gateway is defined in an active `Call Route` profile that contains the network address for that gateway. Call step messages are exchanged when the ingress MAX 6000 successfully locates the destination gateway.

Using the MAXPOTS card allows a MAX 6000 to perform both gatekeeper-directed and gatekeeperless call routing. This configuration imposes the following restrictions on routing VoIP calls:

- MultiVoice® Gateways that do not register with a MultiVoice® Access Manager (MVAM) can perform both ingress and egress call processing. These MAX 6000 units can accept inbound calls from the public switched telephone network (PSTN) and connect outbound calls to the PSTN.
- MAX 6000 units operating as MultiVoice® Gateways which register with a MultiVoice® Access Manager (use Gatekeeper-directed call routing) can perform ingress call processing for gatekeeperless routed calls. When a matching `Call Route` profile is found on a MAX 6000 for an ingress call, the system routes that call across the packet network without sending a call admission request (ARQ) to MVAM. When no matching `Call Route` profile is found, a MAX 6000 sends a call admission request (ARQ) to MVAM. The destination IP of the egress MultiVoice® Gateway is determined by the MVAM, then sent to the ingress MAX 6000.

MAXPOTS call routing dependencies

Gatekeeperless routing of VoIP calls has the following dependencies

- If the ingress MultiVoice® Gateway is configured to collect a PIN (`VPN Mode=NO`), and a matching `Call Route` profile exists, the PIN is collected and ignored. The call is routed to the egress MultiVoice® Gateway specified in the matching `Call Route` profile without using authentication.
- If the ingress MultiVoice® Gateway is configured to use Multiple Logical Gateways (`GK MLG Control=Yes`), gateway-to-gateway routing of VoIP calls is ignored. When a MAX 6000 unit is using Multiple Logical Gateways, MVAM controls the call routing at the DS0 level. To avoid conflicts and inconsistencies in call processing and gateway-to-gateway call routing, the `Call Route` profiles are ignored.
- If the egress MultiVoice® Gateway registers with MVAM, and an incoming VoIP call was routed using the `Call Route` profile, the call is rejected. MVAM does allow any call to complete without end-to-end knowledge of that call.

When performing VoIP call processing, the IP network serves as the network backbone. Each MAX 6000 requires call routes that perform the following tasks:

- Send out calls across the IP network
- Receive calls from the IP network and link them to a T1 or POTS connection

Configuring Call Route profiles for egress across the IP network

To configure egress routing across the IP network, you create a `Call Route` profile for each MAX 6000 unit on the IP network that is configured as a MultiVoice® Gateway. These egress `Call Route` profiles must have values assigned for the following parameters:

```
Name=609NPA
Active=Yes
```

```
Phone Number=^1609
Rmt VoIP GW=192.168.19.221
```

Parameter	Setting
Active	Enable/disable the selected Call Route profile. The Call Route profile is not used unless this parameter is set to Yes.
Phone Number	This parameter specifies the user-entered dial string associated with this profile. This may be a full E.164 address or partial destination telephone number prefixed by a caret (^). This number, which is compared to the caller-entered dial sting, can be up to 24 characters, and can include a subaddress. You must limit your specification to these characters: 1234567890()[]!z-*#|
Rmt VoIP GW	IP address of the MAX 6000 to be used as the egress MultiVoice® Gateway for calls matching this Call Route profile.

The following Call Route profile routes calls beginning with a 9 to the MAX 6000 at IP address 192.168.35.16:

```
Name = start w/9
Active = Yes
Phone Number = ^9
Call Rte Type = Trunk-any
Rmt VoIP GW = 192.168.35.16
```

Configuring Call Route profiles for ingress calls from the IP network

To configure ingress routing from the IP network to a T1 or POTS connection, you create a Call Route profile to the desired network connection on the MAX 6000. These ingress Call Route profiles must have values assigned for the following parameters:

```
Name=VOIP1
Active=Yes
Src Slot=9
Call Rte Type=Trunk-any
Dst Slot=1
```

Parameter	Setting
Active	Enable/disable the selected Call Route profile. The Call Route profile is not used unless this parameter is set to Yes.
Src Slot	Call's source slot number. For VoIP calls received across the IP network connection this value is normally 9, the slot number associated with the LAN/UTP connection on the MAX 6000.
Dst Slot	Call's destination slot number. This points to the T1/E1 or MAXPOTS slot used to forward this call to a public switched telephone network (PSTN) or analog device.

The following `Call Route` profile routes all calls received from the IP network to the PSTN using the T1 connection attached to either WAN port 1 or 2 on the MAX 6000.

```
Name=VOIP1
Active=Yes
Src Slot=9
Call Rte Type=Trunk-any
Dst Slot=1
```

These `Call Route` profiles can direct VoIP calls to egress on either a T1/E1 or MAXPOTS connection. If a `Call Route` profile does not exist, or fails to provide a valid destination, the VoIP call is connected over the first available trunk interface. To egress a VoIP call on a specific MAXPOTS port, both the `Dst Slot` and `Dst Port` parameters must be used.

Reporting availability of the MAXPOTS port to MVAM

A MultiVoice® gateway reports MAXPOTS port availability to the MultiVoice® Access Manager (MVAM) in both initial and keep-alive registration request (RRQ) messages. The status of all enabled POTS ports is reported in the full RRQ message sent when a gateway is initialized, and reports the status of all enabled POTS ports in subsequent RRQ messages.

This status information is used by MVAM for determining gateway availability. MVAM uses both the number of enabled POTS ports and T1 channels to determine whether a gateway has assets available to complete a VoIP call. However, MVAM does not route calls to POTS ports. Only the information found in the `Call Route` profiles determine whether a call gets routed to a POTS port.

MAXPOTS ports are reported to MVAM as enabled or disabled according to how you set the values of `Dial Enabled` and `Answer Enabled` parameters found in `Main > Analog FXS > FXS Config > FXS Configuration > Line`. Table 2-5 shows the POTS port statuses a MultiVoice® gateway reports.

Table 2-5. POTS port statuses

Configuration	Reported status

`FXS Config profile 1`
`Line 1`
`Dial-Enabled=Yes`
`Answer-Enabled=Yes`
	The POTS port is reported as enabled to the MVAM. It is considered available for connecting VoIP calls.

`FXS Config profile 1`
`Line 1`
`Dial-Enabled=Yes`
`Answer-Enabled=No`
	The POTS port is reported as out-of-service to the MVAM. It is considered not available for connecting VoIP calls.

`FXS Config profile 1`
`Line 1`
`Dial-Enabled=No`
`Answer-Enabled=No`
	The POTS port is not reported to the MVAM. It is not included among the available gateway assets for connecting VoIP calls.