Lucent Technologies
Bell Labs Innovations



# MAX™ 6000/3000

## TAOS 9.1.0 Release Note

May 23, 2001

**Copyright © 2001 Lucent Technologies Inc. All rights reserved.**

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

#### Safety, Compliance, and Warranty Information

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

#### Security Statement

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

#### Trademarks

4ESS, 5ESS, 7R/E, AnyMedia, APX 8000, AQueView, B-STDX 8000, B-STDX 9000, CaseView, CBX 500, CellPipe, ChoiceNet, ClearReach, ComOS, cvMAX, DACS, DACSmate, Datakit, DDM 2000FiberReach, DSLMAX, DSLPipe, DSL Terminator, DSLPipe, DSLTNT, elemedia, elemedia Enhanced, EMMI, GRF, GX 550, HyperPATH, Inferno, InfernoDesign, IntragyAccess, IntragyCentral, IP Navigator, IPWorX, LineReach, LinkReach, MAX, MAXENT, MAX TNT, Metropolis, MetroView, Multiband, MultiLink Protocol Plus, MultiVoice, MultiVPN, Navis, NavisRadius, NetCare, NetLight, NetPartner, NetworkCare, NX64000, OneVision, Open Systems Innovations, OpenTrunk, PacketStar, PathStar, Pinnacle, Pipeline, PortMaster, QVPN, QVPN Builder, SecureConnect, Series56, SmoothConnect, SpringTide, Stinger, SuperLine, SuperPipe, SYSTIMAX, True Access, WaveLAN, WaveMANAGER, WaveMODEM, and WebXtend are trademarks of Lucent Technologies Inc. eSight is a service mark of Lucent Technologies Inc. Other trademarks, service marks, and trade names mentioned in this publication belong to their respective owners.

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

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

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

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

#### Ordering Information

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

#### Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this release note. Please send them to techcomm@lucent.com.

**Lucent Technologies**

# Contents


**What's new in TAOS 9.1.0 ..... vii**

Features organized by type ..... viii
Problems corrected ..... x
Customer service ..... xiv
Notice of TAOS license and upgrade changes ..... xv
Price change for base TAOS software ..... xv
Price change for upgrades and maintenance to TAOS 9.1 software ..... xv
Distribution change for TAOS 9.1 software ..... xvi
TAOS software license agreement change ..... xvi
Notice of new default value for the Log Call Progress parameter ..... xvi
Firmware versions ..... xvi

**Changing operating system software ..... 1**

Preparing to change system software ..... 1
Enabling Field Service and Operations parameters ..... 1
Keeping with the same software binary name ..... 1
Using TFTP to upgrade or downgrade ..... 2
Creating redundant backup images for MAX 6000 ..... 2
Using TFTP to upgrade a MAX 3000 ..... 3
Using TFTP to upgrade a MAX 6000 ..... 5
Using TFTP to upgrade a MAX 6000 for MultiVoice binaries ..... 6
Using TFTP to downgrade ..... 7
Using the serial port to upgrade or downgrade ..... 8
Saving the current system configuration ..... 9
Upgrading system software ..... 9
Restoring the configuration ..... 9
Downgrading the software ..... 10
Restoring passwords ..... 11

**WAN access features ..... 13**

Restricting the number of connected users using a shared profile ..... 13
New parameter ..... 13
New RADIUS attribute ..... 13
Example of a Syslog message ..... 14
Differentiated services code point (DSCP) support ..... 15
Overview ..... 15
Two new parameters ..... 15
RADIUS support ..... 16

**Authentication features ..... 17**

New value for Id Auth parameter ..... 17

Reversing the order of the authentication protocols ..... 17
RADIUS additions ..... 18

**AppleTalk and ARA feature, discontinued ..... 18**

Support for the AppleTalk protocol suite discontinued ..... 18
Names of loads changed ..... 18
Parameters modified or removed ..... 19

**Tunneling features ..... 20**

L2TP-related diagnostics command introduced ..... 20
Using the `l2tp -n[n]` diagnostics command ..... 22
L2TP authentication supports hostname verification ..... 22
New parameter added to L2TP Config menu ..... 24
253-character limit for L2TP tunnel server specification ..... 24
VT100 interface changes ..... 25
RADIUS changes ..... 25

**SNMP features ..... 25**

Enhancements provide SNMPv3 support and remove host list limitation ..... 25
Overview ..... 25
VT100 interface changes ..... 25
Configuring host security ..... 25
Parameter reference ..... 26
View Based Access Control Implementation ..... 27
Overview ..... 27
VT100 interface configuration ..... 27
Enabling VACM ..... 27
Mapping a security name and security model to a security group ..... 28
Specifying view names for different types of access ..... 28
Defining views ..... 29
MIB definitions ..... 30
Flash MIB supported ..... 32
Overview ..... 32
Changes to MIB objects ..... 33
Added MIB objects ..... 33
New MIB group ..... 34
New commands ..... 34
Link-status trap enhancements ..... 35
Overview ..... 35
VT100 interface changes ..... 35
Ascend Link Down ..... 35
Ascend Link Up ..... 36
SNMP changes ..... 36
Support for Virtual Routers (VRouters) ..... 37
Overview ..... 37
Using context names ..... 38
Interface changes ..... 38
New trap for unauthorized access ..... 38
Overview ..... 39
New trap ..... 39

New Syslog messages ..... 39
New attributes added to RADIUS accounting and call-logging packets ..... 40
New attributes ..... 40
Ascend-Dsl-Physical-Channel (10037) ..... 40
Ascend-Dsl-Physical-Line (10021) ..... 40
Ascend-Dsl-Physical-Slot (10020) ..... 40
Ascend-Line-Type (10017) ..... 41
Maximum number of SNMP host entries increased ..... 41
VT100 interface changes ..... 41
Remote PING MIB now supported ..... 42
Overview ..... 42
Supported tables ..... 42
Supported traps ..... 42
Changes to the Remote Ping MIB ..... 42
Unsupported features ..... 43

**Digital signal processor (DSP) features ..... 43**

Introducing MultiDSP modules for MAX units ..... 43
MultiDSP module installation constraints ..... 43
Upgrading a MAX unit to support MultiDSP modules ..... 44
Identifying a MultiDSP module ..... 45
Support for data services ..... 45
Support for Voice over IP (VoIP) services ..... 46
Configuring and administering the basics ..... 46
Using slot-configuration menus and Answer profiles ..... 46
Displaying the status of the port hosted on each DSP ..... 49
Using a MAX unit's diagnostics to administer MultiDSP modules ..... 50
Determining modem status with the Show Modem command ..... 52
MultiDSP module specifications ..... 54
MultiDSP modules and supported firmware versions ..... 54
Issuing commands to the unit's MultiDSP modules through Telnet ..... 55
Supporting V.92 and V.44 features for MAX units ..... 56
Using the AT Answer String parameter ..... 56
Using V.92-related command strings ..... 57
Using V.44-related commands ..... 58
Combining V.92- and V.44-related commands ..... 59
RADIUS support for V.92 ..... 59
Changed parameters ..... 59

**RADIUS features ..... 61**

Maximum accounting checkpoint interval increased ..... 61
VT100 interface changes ..... 61
Acct Checkpoint ..... 61
RADIUS Ascend-NAS-Port-Format (13) value included in Access-Request packets ..... 61
RADIUS session-based checkpoint accounting ..... 61
VT100 interface changes ..... 62
ChkPt Timer ..... 62
RFC 2867 RADIUS tunnel accounting support for L2F ..... 62
RADIUS changes ..... 62
New Acct-Status-Type values ..... 62
Sample accounting records for an L2F connection ..... 63

Command-line changes ... 66
RFC 2867 RADIUS tunnel accounting support for L2TP ... 67
VT100 interface changes ... 67
ATC Encoding ... 67
RADIUS changes ... 68

**MultiVoice features ... 68**

Sequential dialing (H.323 caller originated disconnect) ... 68
New Next Call parameter ... 69
Enabling next calls ... 69
Contingencies ... 70
H.323 (v2) fastStart support ... 70
H.323 (v2) fast connect call flow ... 71
Reverting to the H.245 connection ... 71
H.245 call flow ... 72
Using fastStart with H.245 tunneling ... 72
Terminating the H.323 V2 Fast Connect procedure ... 72
New Faststart Enable parameter ... 72
Enabling fastStart ... 73
External interface changes ... 73
New MAX MultiDSP modules supported ... 73
Voice over IP (VoIP) support on MAX 3000 ... 73
New MAX MultiDSP modules on MAX 6000, 3000 ... 74
Data services ... 75
Configuring and administering the basics ... 75
Displaying the status of ports for each DSP ... 78
Using MAX diagnostics to administer a MAX MultiDSP module ... 79
Using the Show Modem command ... 80
MAX MultiDSP module specifications ... 81
Reporting call failures in cause codes ... 82
Background ... 82
Implementation details ... 82
H.323 Annex D T.38 fax support ... 82
Feature definition ... 82
User interface ... 83
Additional Navis support for RTP payload information ... 84
Feature definition ... 84
User interface changes ... 84
External interface changes ... 85

**Known issues ... 88**

MAX data issues ... 88
MultiDSP module issues ... 89
MultiVoice issues for the MAX 3000 ... 89
MultiVoice issues for the MAX 6000 ... 90

**Caution:** The standard software binaries you use to upgrade to True Access™ Operating System (TAOS) 9.1.0 require additional flash memory available to the MAX™ 6000 unit only by way of an external PCMCIA flash card. See “Changing operating system software” on page 1 for details.

**Caution:** You must use the software loading procedure explained in “Changing operating system software” on page 1 to load this version of software onto your system. Read the instructions carefully before upgrading your system. When downgrading software, the MAX unit’s configuration could be lost. For complete information, refer to “Using TFTP to upgrade or downgrade” on page 2 and “Using the serial port to upgrade or downgrade” on page 8.

# What’s new in TAOS 9.1.0

This release note describes new features and corrections introduced in TAOS 9.1.0. 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.

**Note:** The MAX 6000 requires a Lucent-approved external PCMCIA card. The MAX 3000 unit does not have an external PCMCIA flash card.

As new features are added to TAOS, the amount of memory used by the operating system grows. Therefore, the products running later versions of TAOS will report less available memory. When you install TAOS 9.1.0 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 stored on the flash card have gotten bigger, and the memory used to store those software binaries is greater.

TAOS 9.1.0 no longer supports AppleTalk and ARA features. Do not upgrade to TAOS 9.1.0 if your network requirements include support for AppleTalk. Refer to “Support for the AppleTalk protocol suite discontinued” on page 18 for more details.

TAOS 9.1.0 supports the following types of features for MAX 6000 and MAX 3000:

- WAN access features
- Authentication features
- Tunneling features
- SNMP features
- Digital signal processor (DSP) features
- RADIUS features
- MultiVoice® features

# Features organized by type

In the following sections, Feature Identification (FID) numbers and/or descriptions are included for each feature in this release.

## WAN access features

| FID | Description |
|---|---|
| 260833 | “Restricting the number of connected users using a shared profile” on page 13 |
| 510444 | “Differentiated services code point (DSCP) support” on page 15 |

## Authentication features

| FID | Description |
|---|---|
| 261028 | “New value for Id Auth parameter” on page 17 |
| 510411 | “Reversing the order of the authentication protocols” on page 17 |

## AppleTalk and ARA feature (discontinued)

| FID | Description |
|---|---|
| N/A | “Support for the AppleTalk protocol suite discontinued” on page 18 |

## Tunneling features

| FID | Description |
|---|---|
| NA | “L2TP-related diagnostics command introduced” on page 20 |
| 510468 | “L2TP authentication supports hostname verification” on page 22 |
| 260794 | “253-character limit for L2TP tunnel server specification” on page 24 |

## SNMP features


| FID | Description |
|---|---|
| 510523 | “Enhancements provide SNMPv3 support and remove host list limitation” on page 25 |
| 51654 | “View Based Access Control Implementation” on page 27 |
| NA | “Flash MIB supported” on page 32 |
| 510425 | “Link-status trap enhancements” on page 35 |
| NA | “Support for Virtual Routers (VRouters)” on page 37 |
| NA | “New trap for unauthorized access” on page 38 |
| NA | “New attributes added to RADIUS accounting and call-logging packets” on page 40 |
| 510482 | “Maximum number of SNMP host entries increased” on page 41 |
| NA | “Remote PING MIB now supported” on page 42 |


## Digital signal processor (DSP) features


| FID | Description |
|---|---|
| NA | “Introducing MultiDSP modules for MAX units” on page 43 |
| NA | “Issuing commands to the unit’s MultiDSP modules through Telnet” on page 55 |
| NA | “Supporting V.92 and V.44 features for MAX units” on page 56 |


## RADIUS features


| FID | Description |
|---|---|
| 510400 | “Maximum accounting checkpoint interval increased” on page 61 |
| 261197 | “RADIUS Ascend-NAS-Port-Format (13) value included in Access-Request packets” on page 61 |
| 510320 | “RADIUS session-based checkpoint accounting” on page 61 |

| FID | Description *(continued)* |
|---|---|
| 510463 | “RFC 2867 RADIUS tunnel accounting support for L2F” on page 62 |
| 510463 | “RFC 2867 RADIUS tunnel accounting support for L2TP” on page 67 |

### MultiVoice features

| FID | Description |
|---|---|
| NA | “Sequential dialing (H.323 caller originated disconnect)” on page 68 |
| NA | “H.323 (v2) fastStart support” on page 70 |
| NA | “New MAX MultiDSP modules supported” on page 73 |
| 261021 | “Reporting call failures in cause codes” on page 82 |
| NA | “H.323 Annex D T.38 fax support” on page 82 |
| NA | “Additional Navis support for RTP payload information” on page 84 |

## *Problems corrected*

Following are the problem corrections for 9.1.0:

| TR | Problem corrected |
|---|---|
| 2493 | PIAFS call generated unknown event MIB record. |
| 5347 | In the terminal server, entering the `show fr dlci` command displayed this incorrect message: wrong `last time status changed`. |
| 258789 | On a MAX unit, authenticating a user against a local profile with MS-CHAP failed. |
| 6001049 | Nailed BRI card on MAX 3000 was not working properly. |
| 6001072 | Username was being truncated in the RADIUS accounting record from LAC. |
| 6001085 | Firewall was not refreshed for callback users defined in RADIUS. |
| 6001088 | OSPF AreaType parameter did not set Options bits in OSPF header correctly. |
| 6001089 | PPTP Control Connection stayed up after all sessions had ended. |

| TR | Problem corrected *(continued)* |
|---|---|
| 6001095 | MultiVoice: Gateway continuously called to phone that has been forwarded to the Gateway. When the same call ID was reused, the Gateway thought this was another redirecting call to that same phone. |
| 6001140 | MAX 6000 occasionally reset with FE1. |
| 6001141 | If the image on the MAX 6000 external PCMCIA flash card became corrupted, the unit's fallback to the image in the internal flash failed. |
| 6001154 | On a MAX 6000, IPX routing table was not properly updating the local connection profile. |
| 6001179 | On a MAX 6000 `ipxping` over a WAN interface failed because of a wrong source address. |
| 6001202 | MAX 6000 occasionally logged a WARNING 106 followed by a RESET 385. |
| 6001253 | On MAX 6000 units, the fragmentation bit in Telnet packets was set to 1, which prevented packet fragmentation. |
| 6001259 | MultiVoice: Busy Signal not played when cause codes not enabled. |
| 6001264 | Whenever a telnet session was initiated from Navis™ Access 4.3 with the MAX, the option negotiation phase during session establishment used to entered an endless loop. |
| 6001267 | Syslog cause codes did not match Stop information and Lan session information. |
| 6001300 | In RADIUS access requests, an empty attribute, Ascend-Third-Prompt (213) was being sent. |
| 6001312 | MAX 6000 occasionally logged a WARNING 106 followed by a RESET 385. |
| 6001324 | MultiVoice: When using a MAX with a 3rd party Alcatel gatekeeper generating 10 simultaneous calls at 60 seconds each, repeating every 90 seconds, WARNING 109 and Index 385 occur. |
| 6001326 | Unable to configure VROUTER when "Disable Route" software option is installed. Virtual Router functionality was incorrectly tied to the "Disable Routing" software option. |
| 6001360 | An end-of-call record was not being produced when a V110/PHS/modem call did not exist. |
| 6001443 | Username was missing from syslog when tunnel failed to establish. |
| 6001444 | L2TP username was truncated in Syslog messages. |
| 6001458 | MultiVoice: Egress GW populates P26 with CC = 16 for a busy call. This results in a stop record that shows normal call clearing for this call. The behavior for the ingress Gateway is normal. |

| TR | Problem corrected *(continued)* |
|---|---|
| 6001467 | A MAX did not report a disconnect code 11 for a CSM3 card when it was appropriate. |
| 6001488 | MultiVoice: Arbitrary announcement was cut-off when call is connected. |
| 6001498 | MultiVoice: E1/R2 - Fix sending of cmn subscriber category & I-15/I-12 signaling. It is not possible to discriminate at the destination the subscriber type or category of the originating party (common subscriber, testing equipment, payphone, etc.) because the TAOS unit always sends the "common subscriber " indication no matter the subscriber category sent by the originating switch. |
| 6001499 | MultiVoice: The TAOS unit can drive variable length numbering plans using the I-15 signal or Time-Out as "end of number". When you configure to use "number-complete = time-out", and "caller-id = get-caller-id" in the TAOS unit, the TAOS unit can't complete the signaling dialog and drop the call. |
| 6001513 | Unable to set country code to New Zealand. |
| 6001516 | MultiVoice: Use of G.728 offers no available busy signal, and use of G.729 offers a busy-buzz signal. |
| 6001525 | MAX 6000 occasionally logged a WARNING 109 followed by a RESET 385. |
| 6001581 | The MAX could not activate the second nailed BRI connection. |
| 6001606 | MultiVoice: T1 Inband Timer expired and Answer signal not sent when True Connect Enabled. |
| 6001690 | MAX 6000 `fVersionInfo` displayed 8.0.0 for 8.0-1xx.x. |
| 6001713 | When a MAX 6000 would receive a RIP update, the console would freeze or a low throughput was observed. |
| 6001723 | MAX did not log messages for connections through L2TP in its status window. |
| 6001742 | MAX 6048 could not recognize V.90 S56 III Modem cards. |
| 6001861 | TAOS 9.0 16-bit vendor-specific parameter was not authenticating the dial-up user. |
| 6001900 | Incomplete MIF commands caused the MAX to send Warnings 330 and crash with FE1. |
| 6001901 | On a MAX 6000, the MRU value in the Frame Relay profile could not be set beyond the default of 1524. |
| 6002017 | The MAX was dedicated to outgoing fax calls and telnetting to these units would occasionally create excessive ethernet traffic. |

| TR | Problem corrected *(continued)* |
|---|---|
| 1000143 | On a MAX 6000, `show dnis session` output displayed an incorrect number of sessions. |
| 6000541 | Outgoing modem calls would fail because the first available modem was found in a slot number different from the value found in the T1 configuration. |
| 6000632 | MAX unit occasionally rebooted with FE1 when using IDSL cards. |
| 6000657 | Acct-Authentic=Local for callback session authenticated by RADIUS was not being saved. |
| 6000712 | MAX replied with Configure-Reject when PC sent DNS server address in IPCP. |
| 6000928 | When a PIAFS call could not be connected because all ports on the PIAFS card were in use, the incoming call should have been disconnected with a USER_BUSY disconnect code rather than a NORMAL_CLEARING code. |
| NA | MultiVoice: The hairpin failed where trunk groups were in use. Current hairpin functionality and previous release bugs need to be documented. |
| NA | MultiVoice: The VoIP system sent erroneous and confusing (code used by the modem application) progress code and cause code to syslog. |
| NA | MultiVoice: Significant failure rate of calls occur between the Cisco gateway to the MAX, where gateway routing includes a 3rd party Alcatel gatekeeper. |
| NA | MultiVoice: We need to be able to configure the number of retries for PIN and DNIS in the VoIP profile, where there is no current capability. |
| NA | MultiVoice: Break-in announcements played improper messages in response to certain dialing or announcement conditions. Hanging up during an announcement triggered the “You have entered an invalid number...” message. When the called phone hung up, the entire break-in announcement replayed, indicating that the wrong message may be in the queue or buffer. |
| NA | MultiVoice: Hanging up the called phone during a break-in announcement generated an error message (two-stage call with PIN on TNT38, terminating on TNT 39, with originating gateway reporting error). |
| NA | MultiVoice: An announcement that was supposed to be continuous only played once from its gateway. |
| NA | MultiVoice: An announcement specified in a disengage request (DRQ) was not played on the ingress gateway. |
| NA | MultiVoice: An error in the process of receiving IRR resulted in multiple transmissions of IRQs. |

## Also in this release

The first section, “Changing operating system software” on page 1, describes how to upgrade or downgrade your system software. “Firmware versions” on page xvi describes the modem code versions supported in 9.1.0. “Known issues” on page 88 describes issues you should be aware of before installing this software.

# *How to use this release note*

To use this release note:

1. Read through the table of contents to determine which software releases apply to your environment.
2. Obtain the binary file from the Lucent Technologies eSight™ Service Center at `http://www.esight.com`. If you need Technical Assistance, see the next section.
3. Upgrade to the new software by following the instructions in “Changing operating system software” on page 1. Then configure the features that apply to your site.

# *Customer service*

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

## Finding information and software

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

## Obtaining technical assistance

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

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

- Active contract number, product name, model, and serial number
- Software version
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- Your local telephone company’s switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

### *Obtaining assistance through email or the Internet*

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

### *Calling the technical assistance center (TAC)*

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

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

# *Notice of TAOS license and upgrade changes*

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

## Price change for base TAOS software

With the release of TAOS 9.1, MAX 3000, MAX 6000, MAX TNT, and APX 8000 hardware and TAOS software are priced separately. The TAOS software license is now a mandatory item for any new order. The license grants licensees the right to use the base TAOS 9.1 software on the specific platform purchased. *The right to upgrade to a subsequent TAOS minor or major software release that includes new operating system software features is no longer included as part of the base TAOS software license.*

## Price change for upgrades and maintenance to TAOS 9.1 software

Upgrades to TAOS 9.1 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 Upgrade and Maintenance Service contract. These contracts are priced separately for each platform and include the following software and services:

- TAOS software updates, upgrades, and support
- TAOS software options (“hashcodes”), updates, upgrades, and support
- Remote technical support
- Hardware maintenance and return

*Only customers with an established Software Upgrade and Maintenance Service contract are authorized to upgrade designated TAOS-enabled units to TAOS 9.1 and to download the required TAOS 9.1 software files.*

## Distribution change for TAOS 9.1 software

TAOS 9.1 and subsequent general-availability TAOS software releases are no longer available from `ftp.ascend.com`. Upgrades to TAOS 9.1 and all subsequent releases and updates (maintenance releases) are available instead from the Lucent Worldwide Services software front-end Web site at `http://www.eSight.com`.

## 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 9.1 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.

# *Notice of new default value for the Log Call Progress parameter*

In order to maximize the efficiency of outbound and inband call placement, the default value of the `Log Call Progress` parameter has been set to No. This parameter is located in Ethernet > Mod Config > Log. If you have been using `Log Call Progress`, and want to continue to do so, you will need to reenable this feature after installing this version of TAOS. This release removes the default restriction on parallel-dialing. With this restriction removed, the number of calls per second which can be supported increases by 10% to 20%.

# *Firmware versions*

This release supports the following firmware versions:

Series56 digital modules—Mindspeed Technologies (a Conexant Systems company), V2.0982-K56_2M_DLP_CSM firmware includes support for V.90, K56flex, K56plus, and all slower, standard modem speeds.

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

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

- v0.1.46 (Controller)
- v0.1803.0 (RAS)
- v3.0.35 (VoIP)

# Changing operating system software



**Caution:** When you upgrade a MAX unit's version of TAOS, the newer version may 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 a MAX unit's version of TAOS, you may lose all configuration information.



**Caution:** If possible, change a MAX unit's version of TAOS by using TFTP. Refer to "Using TFTP to upgrade or downgrade" on page 2 for further details.

# *Preparing to change system software*

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

**Note:** The MAX 6000 requires a Lucent-approved external PCMCIA card. The MAX 3000 unit does not have an external PCMCIA flash card.

## Enabling Field Service and Operations parameters

The Field Service parameter in the Security profile enables or disables permission to perform Lucent-specific field service operations, such as changing the operating system software on a MAX 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, assure 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 with the same software binary name

If possible, you should always keep with the same software binary name when you upgrade or downgrade. For example, the MultiVoice binary for TAOS 9.0.2 is called `tbiv.bin`. Upgrading to release 9.1.0, you still will use `tbiv.bin` even though the contents have changed.

MAX TAOS 9.1.0 no longer supports AppleTalk and the binary file has changed. Refer to "Support for the AppleTalk protocol suite discontinued" on page 18 for further details.

If you install a different version, your unit may lose its configuration. If this happens, you may need to manually restore your configuration. There may be no automated way to restore configuration data from a backup when changing builds since, if the file formats between the builds are incompatible, no suitable backup exists.

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

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

When the build is intended for 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). Using 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 MAX 6000

The MAX 6000 now supports two copies of TAOS code on the PCMCIA flash memory card. If the first version of software code becomes corrupt, 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. 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 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



**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 4, ensure that the filename used for 9.0.2 is the same software binary name as is currently loaded. Refer to the Sys Options menu to find that Load name. Then, repeat the steps to upgrade to 9.1 from 9.0.2 using a software binary name.

Since the MAX 3000 does not have an external PCMCIA flash card, you will use the unit's internal flash memory to upgrade to the 9.1.0 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 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 will upgrade.
   - The builds 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 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 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 9.1.0. 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 may result in the loss of all previous configuration data (including the IP address) and you may not be able to access this MAX 3000 via telnet.
6. Enter the following command to clear NVRAM memory 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 memory, the unit automatically resets itself two times.

This completes the upgrade to TAOS 9.1.0.

## Using TFTP to upgrade a MAX 6000

**Note:** The following upgrade steps assume you have not used the MultiVoice binaries to upgrade to release 9.1.0. If you used the MultiVoice binaries, you will need to downgrade to a previous TAOS release (see "Using TFTP to downgrade" on page 7) before proceeding with the upgrade steps in this section.

To upgrade using TFTP, you must enter a few commands in the correct sequence. If you do not enter them in the correct sequence, you could lose the MAX 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 will upgrade.
   - The builds 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 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 9.1.0. 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 may result in the loss of all previous configuration data (including the IP address) and you may not be able to access this MAX 6000 via telnet.
6. Enter the following command to clear NVRAM memory 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 memory, the unit automatically resets itself two times.

This completes the upgrade to TAOS 9.1.0.

## *Using TFTP to upgrade a MAX 6000 for MultiVoice binaries*

**Note:** The MAX 6000 loads that support MultiVoice are too large to fit on the internal flash. In order to support the new features offered by this load, 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 will upgrade.
- The builds 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 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 will delete the voice announcements that are currently stored on the card. After completing the upgrade procedure, you will need to re-download your voice announcements (see *Appendix A, MultiVoice for the MAX 6000 Configuration Guide and Reference* for details).

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 for TAOS 9.0.2 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 9.1.0. 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 tbiv.m60 /current/tbiv.bin
```

where ***tbiv.bin*** is an arbitrary name but the name 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 may result in the loss of all previous configuration data (including the IP address) and you may not be able to access this MAX 6000 via telnet.

**9** Enter the following command to clear NVRAM memory 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 memory, the unit automatically resets itself two times.



**Caution:** While the unit resets, it searches for the image on the external PCMCIA flash card is examined first. If available, the unit uses the image. Otherwise, if it is not available (e.g., 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 9.1.0), your configuration may be corrupted.

This completes the upgrade to TAOS 9.1.0.

## 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 will delete the voice announcements that are currently stored on the card. After completing the upgrade procedure, you will need to re-download your voice announcements (see *Appendix A, MultiVoice for the MAX 6000 Configuration Guide and Reference* for details).

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

# Using the serial port to upgrade or downgrade

**Caution:** Upgrading system software by way of the serial console can only be used on the MAX 6000 and 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, you should consider using TFTP to upgrade your software. (See "Using TFTP to upgrade or downgrade" on page 2.)

**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 9.1 MultiVoice binaries.

The MAX 3000 currently does not support download via the serial console port. Before upgrading your MAX 6000 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 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 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 the System Profile (Sys Config menu).

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

## Saving the current system configuration

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

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

   The following message appears:

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

   Rows of configuration information appear on the screen as the configuration file is transferred to your hard disk. When the file has been saved, your communications program displays a message indicating the transfer is complete.
5. Turn off the Capture feature of your communications program.
6. Print a copy of your configured profile and examine the saved configuration file.

## Upgrading system software

To upgrade the software using the MAX 6000'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, Inc. (for example, a single filter stored in a special configuration file).

1. From the MAX unit's VT100 interface, access the diagnostics monitor by pressing Ctrl-D to invoke the DO menu, and select D=Diagnostics.
2. At the `>` prompt, enter the `fclear` command 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 9.1.0.

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 resets. Upon completion of the self-test, the MAX unit's initial menu appears in the Edit window with all parameters set to default values.

If the file transfer fails during the transfer, try obtaining another copy of the binary image from the Lucent Technologies, Inc. FTP server and downgrade the software again. If you continue to have problems, contact Lucent Technologies, Inc. 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 may have to re-enter all the passwords on your system. If you edit your saved configuration file, however, and enter passwords in the appropriate fields (by replacing the word *SECURE* in each instance), these passwords will be restored. But note that if you do choose to edit your configuration file, you must save it as text only or you will not be able to transfer it into your unit.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1. Press Ctrl-D to invoke the DO menu, select `Password`, and choose the Full Access profile.
2. When you are prompted to enter the password, press Enter (the null password).

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

# WAN access features

## *Restricting the number of connected users using a shared profile*

*Units affected: MAX 6000, MAX 3000*

The Max Shared Users parameter provides a direct way of restricting the number of connected users simultaneously using the same profile. An incoming call is compared to the value specified for this parameter. If the limit specified by this parameter has been reached, the MAX unit drops the incoming call.

### New parameter

#### Max Shared Users

**Description:** Specifies a limit on the number of users connected simultaneously, using the same shared profile.

**Usage:** Specify a number from 0 through Max_System_Calls, where Max_ System_Calls is the maximum number of calls that can be taken simultaneously on that platform. For both the MAX 6000 and the MAX 3000 units, the maximum is 136 calls. The default for this parameter is 0, which specifies that there is no limit on the number of users allowed to connect by using the same shared profile.

**Dependencies:** This parameter is enabled only if you set Shared Prof to Yes.

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

### New RADIUS attribute

#### Ascend-Max-Shared-Users

Following is an excerpt from the dictionary file on RADIUS:

```
#ATTRIBUTE  Ascend-Netmask —see Framed-Netmask

#ATTRIBUTE  Ascend-IPX-Network— see Framed-IPX-Network


# Maximum Number of Users connected using a shared profile

Ascend.attr Ascend-Max-Shared-Users— 2 integer (*, 0)


# Authentication delay in msec (minimum granularity 10 msec)
```

```
Ascend.attr Ascend-Auth-Delay— 28 integer (*, 0)


# Ascend IP Type of Service Attributes

Ascend.attr Ascend-IP-TOS— 87 integer

Ascend.attr Ascend-IP-TOS-Precedence— 88 integer
```

Following is an excerpt from a User file on RADIUS:

```
test-max  Password="ascend",
Service-Type=Framed,
Framed-Protocol=MP,
Ascend-Assign-IP-Pool=1,
Ascend-Maximum-Channels=3,
Port-Limit=3,
Ascend-Max-Shared-Users=2,
Ascend-Shared-Profile-Enable=Shared-Profile-Yes,
Framed-IP-Netmask=255.255.255.255
```

## Example of a Syslog message

Following is an example of a Syslog message from the MAX unit when a call is disconnected because the number of shared users has reached the limit.

```
>>>>----- extract

Oct 25 14:16:56 [210.210.210.251.2.2] ASCEND: slot 4 port 2,
Max Shared Users Ex

ceeded, shared [MBID 2; 52063]

Oct 25 14:17:00 [210.210.210.251.2.2] ASCEND: slot 4 port 2,
Call Terminated [MB

ID 2; 52063]

Oct 25 14:17:00 [210.210.210.251.2.2] ASCEND: call 2 CL 0K
u=shared c=104 p=40

s=50000 r=28800

>>>>----- END --------<<<<<<<
```

# *Differentiated services code point (DSCP) support*

*Units affected: MAX 6000, MAX 3000*

Differentiated services code point (DSCP) support enables a MAX unit to mark packets so that other network devices can make decisions on the basis of quality of service (QoS). To verify DSCP marking, you set parameters in Connection and Filter profiles. The unit does not support complete Differentiated Services (DS) node compliance defined in RFC 2474. For example, the unit does not support queuing strategies, per-hop behaviors, or any other QoS strategies.

## Overview

The second octet in the IP datagram header indicates type of service (TOS) parameters that are associated with the packet. Those parameters identify how the MAX unit handles the packet by using devices within the network that are capable of recognizing the packets and acting upon them. Previously, RFC 791 defined the first six bits in the second octet for TOS marking.

This release supports RFC 2474, which defines a less structured method of using these six bits in the second octet of the IP datagram header to differentiate services and identify how the software handles the packet. This less-structured method is known as DSCP marking.

**Note:** This version of TAOS allows DSCP information specified to be set so that it can be acted upon by other network devices. The current software does not support interpretation or utilization of DSCP information by the MAX unit.

## Two new parameters

Two parameters have been added to the Connections profile and the Filters profile.

### Marking Type

**Description:** Enables you to specify whether TOS or DSCP marking is being used.

**Usage:** Specify one of the following values: (the setting comes into effect once the profile has been saved for new calls.

| Value | Description |
|---|---|
| Precedence-TOS | The default. The precedence and type-of-service values are used to set the bits within the second octet of the IP packet header in accordance with RFC 791. |
| DSCP | Bits within the second octet of the IP packet header are set according to the hexidecimal value specified for the DSCP parameters. |

**Dependencies:** This parameter is N/A.

- In the Connection profile if Route IP=No or TOS-Enabled=No.
- In the Filters profile if Valid=No or Type!=TOS.

**Location:** Ethernet > Connections > *any Connection profile* > IP Options, Ethernet > Filters > Input Filters > *any Filter profile* > In Filter *NN* > IPTos, Ethernet > Filters > Output Filters > *any Filter profile* > Out Filter *NN* > IPTos

### DSCP

**Description:** Enables you to enter the hexadecimal (hex) value of the DSCP bits, if you choose DSCP marking.

**Note:** Although all eight bits of the second octet in the IP packet header can be set by entering hex values from 00 through FF, to stay compliant with RFC 2474 only the upper six bits should be set.

**Usage:** Specify a hex numeral from 00 to FF. The default is 00. The hexidecimal specified value entered sets the bits in the second octet of the IP packet header. The change comes into effect once the profile has been saved for new calls.

**Dependencies:** This parameter is N/A

- In the Connection profile if Route IP=No, or TOS-Enabled =No, or Route IP =Yes and TOS Enabled=Yes and Marking Type=Precedence-TOS
- In the Filter profile if Valid=No, or Type!=TOS, or Valid=Yes, and Type=TOS, and Marking Type=Precedence-TOS

**Location:** Ethernet > Connections > *any Connection profile* > IP Options, Ethernet > Filters > Input Filters > *any Filter profile* > In Filter *NN* > IPTos, Ethernet > Filters > Output Filters > *any Filter profile* > Out Filter *NN* > IPTos

## RADIUS support

A new VSA RADIUS attribute has been defined to support DSCP marking from RADIUS profiles and has been added to the RADIUS dictionary file:

```
ATTRIBUTE      Ascend-IP-DSCP                    3          integer
```

The following values are also defined in the dictionary file:

```
VALUE Ascend-IP-TOS IP-TOS-Dscp                              128
VALUE Ascend-IP-DSCP IP-DSCP-Default                           0
```

In order to choose `dscp` marking instead of the default `precedence-tos` value, the Ascend-IP-TOS RADIUS attribute must be set to IP-TOS-Dscp. The new Ascend-IP-DSCP RADIUS attribute is used to specify the value for the DSCP parameter in the Connection profile. The value specified in the RADIUS profile must be the decimal equivalent of the binary bit setting desired in the second octet of the IP packet header.

Following is an example of a RADIUS profile named `test`. The last two lines of this profile, show how you would specify the use of DSCP marking and value of 252 for the DSCP.

```
test    Password                =         "test"
        Ascend-Route-IP         =         Route-IP-Yes,
        Ascend-Bridge           =         Bridge-No,
        Ascend-Idle-Limit       =         0,
        Ascend-IP-TOS           =         IP-TOS-Dscp,
        Ascend-IP-TOS-DSCP       =         252
```

# Authentication features

## *New value for Id Auth parameter*

*Units affected: MAX 6000, MAX 3000*

If the RADIUS server is inoperable or is not responding during DNIS authentication, you can now continue the call setup protocol. The Id Auth parameter has a new value, Called Fallback which now enables calls to be accepted normally when DNIS authentication fails because of a timeout from RADIUS. This value is not applicable to DNIS authentication that uses local profiles.

If RADIUS is available, use the Called # value for authentication. Otherwise, fall back to using the encapsulation protocol's authentication. Depending on the condition, the Called Fallback value causes one of the following actions to occur:

| Condition | Action |
|---|---|
| No DNIS is received on the line. | The MAX unit drops the call. |
| RADIUS authentication fails. | The MAX unit drops the call. |
| RADIUS authentication succeeds. | The Call setup continues normally. |
| RADIUS authentication times out. | The Call setup continues normally. |

## *Reversing the order of the authentication protocols*

*Units affected: MAX 6000, MAX 3000*

Authentication protocols are usually offered in the order: CHAP, MS-CHAP, PAP. A new value for the Recv Auth parameter specifies that the reverse order for authentication protocols, PAP, CHAP, or MS-CHAP are acceptable for an incoming PPP connection. If the client does not accept PAP, the MAX unit offers CHAP and, if CHAP is rejected, MS-CHAP.

**Note:** This feature only supports one-way authentication of a dialin client. This feature does not support authentication between two MAX units, nor does it allow authentication for bidirectional CHAP or MS-CHAP Connection profiles.

### New Recv Auth value

The setting for Ethernet > Answer > PPP options > Recv Auth can be set to `PAP-Preferred` to set the MAX unit's preferred authentication method to PAP with CHAP and then MS-CHAP as the method used to receive and verify a password for an incoming PPP connection.

PAP-Preferred specifies PAP as the MAX unit's preferred authentication method, with CHAP as the second choice and then MS-CHAP as the third choice.

PAP-Preferred is similar to the `Recv Auth = Either` where CHAP is the preferred authentication method, MS-CHAP is the second choice, and PAP is the third. For both

`Either` and `PAP-Preferred`, the client and MAX must agree on an authentication protocol. If they do not agree to a valid authentication protocol, the MAX drops the call.

**Note:** When this parameter is set to `PAP-Preferred`, Bi-dir Auth becomes `N/A`.

## RADIUS additions

The RADIUS dictionary has been extended to allow PAP-Preferred to be set. The enumeration of PppAuthType now has the following allowed values:

```
Auth_None=0,
Auth_Default=1,
Auth_Any=2,
Auth_PAP=3,
Auth_CHAP=4,
Auth_MS_CHAP=5,
Auth_PAP_Preferred=6
```

# AppleTalk and ARA feature, discontinued

# *Support for the AppleTalk protocol suite discontinued*

*Units affected: MAX 6000, MAX 3000*



**Caution:** Save the configuration of your MAX unit to an external resource before you upgrade to TAOS 9.1.0. After you upgrade, the settings you specified to enable the AppleTalk protocol suite (AppleTalk) are available only in the configuration file you save beforehand.

This release discontinues support for AppleTalk. For MAX units, this change affects support for the following features:

- AppleTalk Remote Access (ARA)
- AppleTalk Remote Access Protocol (ARAP)
- AppleTalk router functions
- AppleTalk Control Protocol (ATCP)

The name of the load appropriate for your unit has changed with this release, as have the settings you can specify for the Encaps parameter. This release also removes five parameters from the unit's Ethernet menu.

Though this release does not support AppleTalk, a Macintosh device configured to use Internet Protocol (IP) can continue to access the Internet (or any IP-based network) through the MAX unit.

## Names of loads changed

Before this release, upgrading instructions advised you to stay with the same software load as you upgraded from one version of TAOS to another. This release changes the names of the

MAX 3000 and MAX 6000 loads to reflect the exclusion of support for AppleTalk. As a result, when you upgrade a unit from a previous release to TAOS 9.1.0, you must also change the load you use.

Use Table 1 to determine the name of the current load that corresponds with the load name in previous releases.

*Table 1. Determining the current load*

| Previous load | Current load |
|---|---|
| `tbaxkh.m60` | `tbxkh.m60` |
| `ebaxk.m60` | `ebxk.m60` |
| `tbaxkh.m30` | `tbxkh.m30` |
| `ebaxkh.m30` | `ebxkh.m30` |
| `baxkh.m30` | `bxkh.m30` |

## Parameters modified or removed

In previous releases, a MAX unit's interface included parameters that you used to enable the unit's support for the AppleTalk protocol suite. When you upgrade to TAOS 9.1.0 and restore the unit's configuration, the unit ignores settings that you specified for the AppleTalk-related parameters.

The Encaps parameter, located in Ethernet > *any Connection profile*, is modified so you can no longer specify ARA. The Profile Reqd parameter, located in Ethernet > Answer, is also modified. In previous releases, setting the Profile Reqd parameter to Yes disabled Guest access for ARA connections. Support for AppleTalk's Guest access discontinues with this release.

When you upgrade to the current release, the unit automatically changes any values that previously specified support for AppleTalk to the default values. For example, if you previously specified `ARA` for the Encaps parameter, the value changes to `MPP` (the default).

Table 2 lists the parameters removed and their previous location in the unit's interface.

*Table 2. Parameters removed and location(s) in previous releases*

| Location in previous releases | Parameters |
|---|---|
| Ethernet > Answer > AppleTalk Options | • AppleTalk Router |
| Ethernet > Answer > Encaps | • ARA |
| Ethernet > Mod Config | • AppleTalk |
| Ethernet > Mod Config > AppleTalk Options | • AppleTalk Router<br>• Default Zone<br>• Zone Name #N |

*Table 2. Parameters removed and location(s) in previous releases (continued)*

| Location in previous releases | Parameters |
|---|---|
| Ethernet > Connections > *any Connection profile* > AppleTalk options | • Net End<br>• Net Start<br>• Peer |
| Ethernet > Connections > *any Connection profile* > Encaps Options | • Max. Time<br>• Password |
| Ethernet > Answer > PPP options | • Route AppleTalk |
| Ethernet > Connections | • Route AppleTalk |

# Tunneling features

## *L2TP-related diagnostics command introduced*

*Units affected: MAX 6000, MAX 3000*

For MAX units that support Layer 2 Tunneling Protocol (L2TP), this release introduces a diagnostics command that enables you to display administrative status, version information, domain statistics, tunnel statistics, or call statistics. In previous releases, you could not display this information without configuring Simple Network Management Protocol (SNMP) and using an external SNMP management station.

This release adds a new command, `l2tp -n[n]`, to the MAX unit's diagnostics command-line interface. In the command syntax:

`-n` (preceded by a space), represents a modifier

and

`[n]` (no space), represents an additional, optional modifier.

If you enter the `l2tp` command without any modifiers, it displays a help screen:

```
 > l2tp
Usage: l2tp -[a|v|d|t[srct]|c[isnm]]
        -a: L2TP Administrative status
        -v: L2TP Version Information
        -d: L2TP Domain Statistics Table
        -t: L2TP Tunnel Statistics Table. Additional modifiers will:
              s: display tunnel states
              r: display remote information
              c: display capability information
              t: display totals/active sessions
        -c: L2TP Call Statistics Table. Additional modifiers will:
              i: display user name and call serial number
```

```
s: display call state, connection speed, and capability
n: display DNIS, CLID, and subaddress
m: display proxy LCP, auth method, and sequencing state
```

Table 3 describes the modifiers.

*Table 3. L2TP command modifiers*

| Modifier | Description |
|---|---|
| `-a` | Displays the status of L2TP support on the MAX unit. Indicates whether a unit is configured to support L2TP and, if so, whether it is enabled as an L2TP access concentrator (LAC), a L2TP network server (LNS), or both. |
| `-v` | Displays version information about the unit's L2TP protocol and firmware revision, as well as the L2TP vendor. |
| `-d` | Displays the total tunnels, failed tunnels, failed authentications, active tunnels, total calls, failed calls, and active calls for each virtual router's L2TP domain identification (ID). |
| `-t` | Displays a tunnel statistics table that includes local and remote tunnel identification (ID). Use one of the following tunnel statistics-related modifier combinations to display more tunnel statistics:<br>• `-ts`—Tunnel's state and whether it is a remote or a local tunnel. The tunnel's state can be reported as idle (Idle), connecting (`Conn`), established (`Estab`), disconnected (`Disconn`), or torn down (`Dstroyd`).<br>• `-tr`—Remote tunnel information including host name, vendor, firmware revision, L2TP version.<br>• `-tc`—Remote tunnel's capabilities.<br>• `-tt`—Total number of calls and active calls. |
| `-c` | Displays a call statistics table that includes the local tunnel identification (ID), local call ID, and remote call ID. Use one of the following modifier combinations to display more call statistics:<br>• `ci`—Call information, including username and serial number.<br>• `cs`—Current call's state, including type, connection speeds, bearer, and framing information.<br>• `cn`—DNIS, CLID, and subaddress information.<br>• `cm`—Proxy LCP, authentication method, and sequential state. |

## Using the `l2tp -n[n]` diagnostics command

The `l2tp` diagnostics command does not display information about the MAX unit's L2TP performance unless you include modifiers. You can issue the command with up to two modifiers. In the following example, the unit displays the version, revision, and vendor information in response to the command the user enters with one modifier ( `-v`):

```
 > l2tp -v
L2TP Protocol Version: 1.0
L2TP Firmware Revision: 1.0
Vendor name: Ascend
```

When an additional modifier is available, it is optional. In the following example, the unit responds to the command the user enters with one modifier ( `-t`), though four additional modifiers are available:

```
 > l2tp -t
LocalTID   RemoteTID
1           1
```

In the following example, the unit responds to the command the user enters with two modifiers ( `tt`):

```
 > l2tp -tt
                           Total     Active
LocalTID   RemoteTID       Calls     Calls
1           1                1         1
```

# *L2TP authentication supports hostname verification*

*Units affected: MAX 6000, MAX 3000*

This release introduces a tunnel authentication feature that enables MAX™ units configured to support the Layer 2 Tunneling Protocol (L2TP) and RADIUS authentication to verify a remote hostname. A new parameter, Verify Remote Name, is added to the unit's L2TP Config profile.

This new feature is active only if the L2TP Auth Enabled parameter, in the L2 Tunneling Options menu, is set to Yes, as in the following example:

```
90-E00 Mod Config
 L2 Tunneling options...
  PPTP enabled=No
  L2TP Mode=LNS
 >L2TP Auth Enabled=Yes
  L2TP RX Window=0
  L2TP System Name=Rover
  L2TP Config...
  UDP Queue Length=0
  L2F Mode=None
  L2F System Name=N/A
  L2F Retry Count=N/A
  L2F Retry Interval=N/A
  L2F Tunnel Secret=N/A
  L2F Ignore Mid Seq=N/A
```

In the preceding example, the L2TP Mode parameter specifies that the MAX unit is configured to operate as an L2TP network server (LNS). However, you must specify the same values on both the LNS unit and the L2TP access concentrator (LAC) unit.

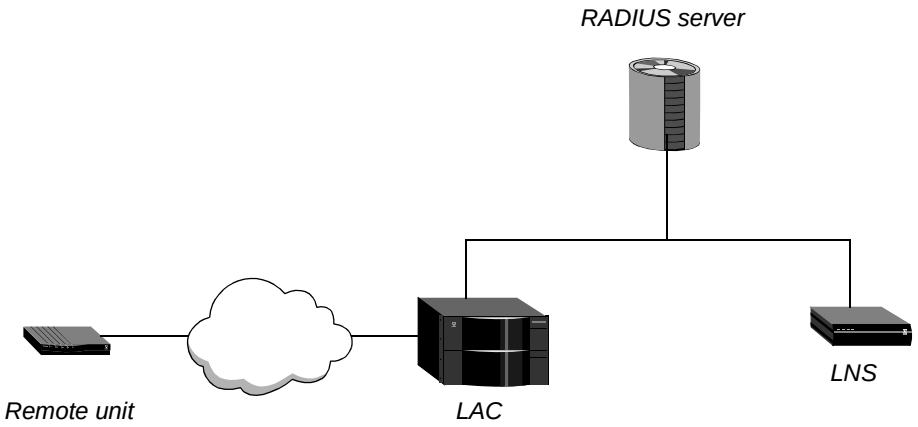
To enable a MAX unit to verify a remote host, specify Yes in the Verify Remote Name parameter of the L2TP Config menu, as in the following example:

```
L2 Tunneling options...
 L2TP Config...
  First Retry Timer (ms)=1000
  Retry Count=6
  Hello Timer=60
  CC Establish Timer=60
  LAC In Call Timer=60
  LNS In Call Timer=60
  Dialout Auth Lns=No
  Send Profile Name=No
 >Verify Remote Name=Yes
```

Setting the Verify Remote Name parameter to Yes enables the unit to refer to a Hostname (101) attribute-value pair provided by RADIUS. The Hostname (101) attribute-value pair is made up of two attributes: Tunnel-Client-Auth-ID (90) and Tunnel-Server-Auth-ID (91).

Figure 1 shows the devices that play a role in a remote unit's access to a network by way of a unit configured as a LAC.

*Figure 1. A remote unit accesses a network by way of a LAC.*




**Note:** In the preceding illustration, the LAC is a MAX TNT™ unit. However, a MAX unit can operate as a LAC or as a LNS.

When a remote user begins a session on an L2TP-authenticated network, an `access accept` message, sent to the LAC unit from the remote unit, contains both of the attributes that make up the Hostname (101) attribute-value pair. To successfully establish an L2TP tunnel, the remote unit's attribute-value pair must match the following:

- Tunnel-Client-Auth-ID (90) specified for the LAC unit
- Tunnel-Server-Auth-ID (91) specified for the LNS unit

A mismatch prevents the LAC unit from establishing an L2TP tunnel. In addition, the LAC unit issues a disconnect cause code 752, which is understood by external management resources such as NavisAccess™ as the following:

`DIS_L2TUNNEL_SERVER_AUTH_FAILED`

If the Hostname (101) attribute-value pair does not exist on either the remote unit or the LNS unit, the LAC unit attempts to match L2TP System Name (in the L2 Tunneling Options menu) or Name (in the unit's Sys Config profile) from the LNS unit.

In addition, the unit also performs the verification required by L2TP, such as the verification of L2TP-related passwords.

## New parameter added to L2TP Config menu

This release adds the Verify Remote Name parameter to the MAX unit's L2TP Config menu.

### Verify Remote Name

**Description:** Specifies whether a MAX unit configured as an L2TP access concentrator (LAC) sends a request to an L2TP network server (LNS) that verifies a remote hostname against one of the following, in the following order (and only if they are present in the configurations of both units):

- Hostname (101) attribute-value pair, composed of the Tunnel-Client-Auth-ID (90) on the LAC and Tunnel-Server-Auth-ID (91) on the LNS
- L2TP System Name (in the L2 Tunneling Options menu)
- Name (in the unit's Sys Config profile)

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

**Example:** `Verify Remote Name=No`

**Dependencies:** This parameter applies only if the following conditions apply:

- The L2TP Auth Enabled parameter is set to Yes.
- The unit is configured to support RADIUS authentication.
- The Tunnel-Server-Auth-ID (91) RADIUS attribute is specified in the RADIUS authentication profile.

**Location:** Ethernet > Mod Config > L2 Tunneling Options > L2TP Config

**See Also:** L2TP Auth Enabled

# *253-character limit for L2TP tunnel server specification*

*Units affected: MAX 6000, MAX 3000*

The number of characters you can specify for a Layer 2 Tunneling Protocol (L2TP) tunnel server has been increased from 31 to 253. In previous releases, an L2TP connection could not be established if the tunnel server name was composed of more than 31 characters.

## VT100 interface changes

You can now specify up to 253 characters for the following parameters:

- Ethernet > Connections > *profile* > Tunnel Options > Pri. Tunnel Server
- Ethernet > Connections > *profile* > Tunnel Options > Sec. Tunnel Server

## RADIUS changes

You can now specify up to 253 characters for the Tunnel-Server-Endpoint (67) attribute.

# SNMP features

# *Enhancements provide SNMPv3 support and remove host list limitation*

*Units affected: MAX 6000, MAX 3000*

In this release, you can specify read and write access for managers that use either SNMPv1 or SNMPv3.

## Overview

In previous releases, you could specify read and write access for up to 10 SNMPv1 managers. Now, you can now specify read and write access for up to 16 SNMPv1 or SNMPv3 managers.

## VT100 interface changes

The SNMP Manager menu, which has been added to the Ethernet menu, contains 16 profiles, each of which contains the following parameters:

- Name
- Active
- Write Access
- Message Type

### *Configuring host security*

To enforce host authentication, proceed as follows:

**1** Navigate to Ethernet > SNMP Manager and choose a new profile.

**2** For the Name parameter, specify the DNS hostname or IP address of an SNMP manager that will have access to the unit. If you specify a DNS hostname, you must enable DNS. If DNS is not enabled, Name will be set to 0.0.0.0 and the manager will not be authenticated.

**3** To enable the profile, set Active to Yes.

4 To enable read-only access, accept the Write Access default of No. To enable read and write access, set the Write Access parameter to Yes.

5 To specify SNMPv1 access only, set the Message Type parameter to V1-Only. To specify SNMPv3 access only, specify V3-Only. To specify both SNMPv1 and SNMPv3 access, accept the Message Type default of V1-and-V3.

6 Save your changes.

7 In the Ethernet > Mod Config > SNMP Options profile, set Security to Yes.

## Parameter reference

Following are descriptions of the Message Type and Write Access parameters in each profile of the new SNMP Manager menu.

### Message Type

**Description:** Specifies whether the unit accepts SNMPv1 messages only.

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

- V1-Only specifies that the unit accepts SNMPv1 messages only.
- V1-and-V3 (the default) specifies that the unit accepts SNMPv1 and SNMPv3 messages.

**Example:** `Message Type = V1-Only`

**Dependencies:** For Message Type to apply, Active must be set to Yes in the active profile of the SNMP Manager menu.

**Location:** Ethernet > SNMP Manager > *any profile*

**See Also:** Active, Name, Write Access

### Write Access

**Description:** Specifies whether the SNMP manager has read and write access.

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

- Yes specifies that the SNMP manager has read and write access.
- No (the default) specifies that the SNMP manager has read-only access.

**Example:** `Write Access = Yes`

**Dependencies:** For Write Access to apply, Active must be set to Yes in the active profile of the SNMP Manager menu.

**Location:** Ethernet > SNMP Manager > *any profile*

**See Also:** Active, Message Type, Name

# *View Based Access Control Implementation*

*Units affected: MAX 6000, MAX 3000*

This release implements View Based Access Control Model (VACM). As specified by RFC 2575, VACM defines a mechanism for SNMP entities to determine whether a specific type of access (read, write, or notify) to a particular object is allowed. RFC 2575 defines a structured configuration that can check accessibility for each GET/SET request received and NOTIFY request sent.

## Overview

The TAOS implementation of VACM enables you to perform the following tasks:

- Enable or disable VACM.
- Configure the system to control different types of access (read/GET, write/SET, notify/TRAP or TRAP2) to various objects in the system on the basis of the security name in the request, the security level specified for the request, or the context name and object identifier (OID) of the object for which access is being attempted.

## VT100 interface configuration

You configure VACM at the VT100 interface by carrying out the following steps:

**1** Enable VACM by setting Enable VACM to Yes in the Ethernet > Mod Config > SNMP Options profile.

**2** Map a security name and security model in an incoming or outgoing message to a security group by setting the parameters in the Ethernet > SNMPv3 Config > VACM Security To Grp profile.

**3** Specify view names for different kinds of access (read, write, notify) by setting parameters in the Ethernet > SNMPv3 Config > VACM Access Params submenu. A view specifies whether a given OID is accessible.

**4** Define views by setting parameters in the Ethernet > SNMPv3 Config > VACM View Trees profile.

**Note:** The SNMPv3 USM Users, SNMPv3 Notifications, and SNMPv3 Target Params subprofiles have been moved to the Ethernet > SNMPv3 Config profile in order to group all the SNMPv3 configuration options together.

### *Enabling VACM*

To enable VACM, set Enable VACM to Yes in the Ethernet > Mod Config > SNMP Options profile. Each object in each incoming request (GET/SET/GETNEXT/GETBULK) and each object contained in the sysTrapOID of each outgoing trap (TRAP2) is verified for VACM access.

The default value of No disables VACM, allowing access to all objects in the system. However, security based on SNMPv1 community strings and the SNMPv3 USM is still used to determine access.

## *Mapping a security name and security model to a security group*

To map a security name and security model to a security group, you must set parameters in the Ethernet > SNMPv3 Config > VACM Security To Grp profile. Following are the relevant parameters:

| Parameter | Description |
|---|---|
| Active | Enables or disables VACM. Specify Yes to enable VACM or No to disable it. The default is No. |
| Group Name | Specifies a group name. The default is null. |
| Security Model | Specifies the security model in use for an incoming or outgoing message. V1 (the default) specifies the SNMPv1 security model. V3-USM specifies SNMPv3 USM. For VACM support, specify V3-USM. |
| Security Name | Specifies the USM user name associated with an incoming or outgoing message. The default is null. |

For example, to specify SNMPv3 USM for a USM user called Joe and a group called GroupNY, proceed as follows:

1. Navigate to the Ethernet > SNMPv3 Config > VACM Security To Grp profile.
2. Set Active to `Yes`.
3. Set Group to `GroupNY`.
4. Set Security Model to `V3-USM`.
5. Set Security Name to `Joe`.
6. Save your changes.

## *Specifying view names for different types of access*

To map a group name, context prefix, context name, security model, and security level to a view name, you must set parameters in the Ethernet > SNMPv3 Config > VACM Access Params profile. Following are the relevant parameters:

| Parameter | Description |
|---|---|
| Active | Enables or disables the view. Specify Yes to enable the view or No to disable it. The default is No. |
| Group Name | Specifies a group name. The default is null. |
| Ctx Prefix | Specifies a prefix for a given context. The default is null. The Ctx Match Mthd value determines whether the context name is matched exactly or the prefix alone is matched. |
| Security Model | Specifies the security model in use. V1 (the default) specifies the SNMPv1 security model. V3-USM specifies SNMPv3 USM. For VACM support, specify V3-USM. |
| Security Level | Specifies the security level. None (the default) specifies that there is no authentication and no privacy. Auth and Priv specifies authentication and privacy. Auth and No Priv specifies authentication and no privacy. |

| Parameter | Description |
|---|---|
| Ctx Match Mthd | Specifies the context-match method. Exact-Match (the default) specifies that the entire context name must be matched. Prefix-Match specifies that only the prefix specified by Context-Prefix must be matched. |
| Read View | Specifies the name of the view for read access. The default is null. |
| Write View | Specifies the name of the view for write access. The default is null. |
| Notify View | Specifies the name of the view for notify access. The default is null. |

For example, to specify a view for read access for a group called GroupSF with SNMPv3 USM, authentication, and privacy enabled, proceed as follows:

1. Navigate to the Ethernet > SNMPv3 Config > VACM Access Params profile.
2. Set Active to `Yes`.
3. Set Group Name to `GroupSF`.
4. Set Security-Model to `V3-USM`.
5. Set Security Level to `Auth and Priv`.
6. Save your changes.

## *Defining views*

To define a view, you must set parameters in the Ethernet > SNMPv3 Config > VACM View Trees profile. Following are the relevant parameters:

| Parameter | Description |
|---|---|
| Active | Enables or disables the view. Specify Yes to enable the view or No to disable it. The default is No. |
| View Name | Specifies the name of the view. The default is null. The system determines whether the view contains a given OID by comparing it with View Tree OID. |
| View Tree OID | Specifies the OID in dotted decimal format. The default is null. |
| OID Mask | Specifies a mask (in hexadecimal format) for comparing subidentifiers in the OID. Comparison of a subidentifier can be omitted by setting the corresponding mask bit to 0 (zero). |
| Tree Type | Specifies whether the OID is accessible. If you specify Included (the default), the OID is accessible. If you specify Excluded, the OID is not accessible. |

For example, to define a view called View1 with an OID of 1.3.6.1.4.1.529, proceed as follows:

1. Navigate to the Ethernet > SNMPv3 Config > VACM View Trees profile.
2. Set Active to `Yes`.
3. Set View Name to `View1`.
4. Set OID Mask to 1.3.6.1.4.1.529.
5. Save your changes.

## MIB definitions

To configure VACM via SNMP, proceed as follows:

**1** Map USM user names to security groups by setting the parameters in the MIB table VacmSecurityToGroupTable.

**2** Specify view names for different kinds of access (read, write, notify) by setting parameters in the MIB table VacmAccessTable.

**3** Define views by setting parameters in the MIB table VacmViewTreeFamilyTable.

Following is the new MIB definition:

```
SNMP-VIEW-BASED-ACM-MIB
snmpVacmMIB       MODULE-IDENTITY
   DESCRIPTION  "The management information definitions for the
                 View-based Access Control Model for SNMP."
   OID :1.3.6.1.6.3.16.1
  x vacmContextTable  ( OID: 1.3.6.1.6.3.16.1.1 )
      DESCRIPTION
        This table provides information to SNMP Command
        Generator applications so that they can properly
        configure the vacmAccessTable to control access to
        all contexts at the SNMP entity.
      INDEX
        {
           vacmContextName
        }
      CONTAINS
        {
           vacmContextName
        }
  x vacmSecurityToGroupTable ( OID: 1.3.6.1.6.3.16.1.2 )
      DESCRIPTION
        This table maps a combination of securityModel and
        securityName into a groupName which is used to define
        an access control policy for a group of principals.
      INDEX
        {
           vacmSecurityModel,
           vacmSecurityName
        }
      CONTAINS
        {
```

```
            vacmSecurityModel,
            vacmSecurityName,
            vacmGroupName ,
            vacmSecurityToGroupStorageType,
            vacmSecurityToGroupStatus
          }
    x vacmAccessTable (OID: 1.3.6.1.6.3.16.1.3 )
        DESCRIPTION
          The table of access rights for groups.
          Each entry is indexed by a groupName, a contextPrefix,
          a securityModel and a securityLevel.  To determine
          whether access is allowed, one entry from this table
          needs to be selected and the proper viewName from that
          entry must be used for access control checking.
        INDEX
          {
            vacmGroupName,
            vacmAccessContextPrefix,
            vacmAccessSecurityModel,
            vacmAccessSecurityLevel
          }
        CONTAINS
          {
            vacmAccessContextPrefix,
            vacmAccessSecurityModel,
            vacmAccessSecurityLevel,
            vacmAccessContextMatch,
            vacmAccessReadViewName,
            vacmAccessWriteViewName,
            vacmAccessNotifyViewName,
            vacmAccessStorageType,
            vacmAccessStatus
          }
    x vacmMIBViews ( OID: 1.3.6.1.6.3.16.1.4 )
       ( Contains a vacmViewSpinLock and vacmViewTreeFamilyTable)
        DESCRIPTION
          Locally held information about families of subtrees
          within MIB views.
          Each MIB view is defined by two sets of view subtrees:
```

```
            - the included view subtrees, and
            - the excluded view subtrees.
      Every such view subtree, both the included and the
      excluded ones, is defined in this table.
    INDEX
      {
         vacmViewTreeFamilyViewName,
         vacmViewTreeFamilySubtree
      }
    CONTAINS
      {
         vacmViewTreeFamilyViewName,
         vacmViewTreeFamilySubtree,
         vacmViewTreeFamilyMask,
         vacmViewTreeFamilyType,
         vacmViewTreeFamilyStorageType,
         vacmViewTreeFamilyStatus
      }
```

# *Flash MIB supported*

*Units affected: MAX 6000, MAX 3000*

The Flash MIB provides an interface to various aspects of the system configuration and the images stored on the internal and external flash cards. This MIB has been enhanced to operate with FAT-formatted flash cards. In addition, the units that support FAT file systems now have access to the Flash MIB.

## Overview

This release includes the following enhancements:

- You can use the Flash MIB to access FAT-formatted flash cards.
- When you save and restore profiles or other configuration information, you can either select a subset of profiles to save or exclude certain profiles from being saved.
- To provide more advanced error handling when you upload or download configuration information, you can now display error codes with detailed information.
- You can now query the load name version information on the internal flash card.
- You can use SNMP to specify encryption for configuration files, enabling the system to provide a secure transfer of configuration information.

## Changes to MIB objects

The following objects have been changed:

| Object | Description |
|---|---|
| `flashDeviceWriteProtect` | Enables write-protect detection of active PCMCIA devices in the `flashDeviceTable`. If the value of the object is `true`, the write protection of the flash card is enabled. |
| `flashDeviceType` | Identifies the type of flash card in use. |
| `flashFileAttributes` | Renamed from `flashFileAccess`, which always returned `read_write(2)`, to more accurately refer to a file attribute object like those used on file systems. The new implementation provides special file attribute values that indicate, for example, that the entry is a directory. This information was not available in the previous implementation. The values are returned in a bitmask and can be one of the following:<br>`readOnly(1)`—Indicates a read-only file entry.<br>`hidden(2)`—Indicates a file marked as hidden.<br>`system(4)`—Indicates a system file.<br>`volumeLabel(8)`—Indicates the volume label.<br>`subDirectory(16)`—Indicates a subdirectory.<br>`archived(32)`—Indicates that the file has been archived.<br>A normal file has an attribute value of 0 (zero). |
| `flashFileLoadName` | Identifies the TAOS load name of the file listed in the entry. The FAT file system can have multiple loads and versions of the system software stored on the flash card. For this reason, the filename of a particular load might not reflect the version and load name information for a particular file. Because the information is stored in the file itself, retrieving the information is rather costly and might take several seconds. |
| `flashOperationStatus` | Provides operational status and additional error codes for all types of flash operations and all TFTP operation errors. Almost all possible error conditions can be uniquely identified by this code. For new operations, `active` codes enable you to follow the progress of the current operation. |
| `fileTable`<br>`cardTable` | Provides additional details about the files and cards present in the system. |

## Added MIB objects

The following MIB objects were added to `flashOperationGroup` to specify how configuration profiles are stored:

| Object | Description |
|---|---|
| `flashOperationConfigSaveDefaults` | Specifies whether default values are stored. |
| `flashOperationConfigSaveAsMIB` | Specifies that the configuration should be stored as a MIB. |
| `flashOperationConfigProfileRule` | Specifies the profiles to be stored. |

## New MIB group

The `flashSystem` group has been added in this release. This group contains the following objects that enable you to obtain system load and version information:

| Object | Description |
|---|---|
| `flashSystemInternalLoadName` | Specifies that the name of the load is stored in internal flash memory. |
| `flashSystemInternalVersion` | Specifies the version of the load that is stored in internal flash memory. |
| `flashSystemExternalLoadName` | Specifies the name of the load stored on the PCMCIA card. |
| `flashSystemExternalVersion` | Specifies the version name of the load stored in flash memory. |
| `flashSystemCurrentLoadName` | Specifies the name of the load currently running on the system. |
| `flashSystemCurrentVersion` | Specifies the version of the load being executed. |

## New commands

The `flashOperationCommand` object includes the following new commands:

| Command | Description |
|---|---|
| `format-card-fat(6)` | Specify FAT format. |
| `format-card-fat-no-mbr(7)` | Specify FAT format without Master Boot Record (MBR). This command is valid only for an ATA flash memory device. |
| `format-card-fat-boot(8)` | Specify FAT format with boot section. |
| `format-card-erase(9)` | Erase card without formatting. |
| `format-card-erase-boot(10)` | Erase boot region only. |
| `move-file(11)` | Move file on flash card. This command requires the source (`flashOperationSrcFileName`) and destination (`flashOperationDestFileName`) to be set. |
| `remove-file(12)` | Remove file from flash card. This command requires the source (`flashOperationSrcFileName`) to be specified. |
| `make-directory(13)` | Create directory on flash card. This command requires the source (`flashOperationSrcFileName`) to be specified. |
| `internal-copy-load(14)` | Copy load to or from internal flash memory. This command requires the source (`flashOperationSrcFileName`) to be specified. |
| `reset-attributes(15)` | Reset `flashOperationGroup` to its defaults. |
| `tftp-download(16)` | Download file from flash card. This command requires the host (`flashOperationHost`), source (`flashOperationSrcFileName`), and destination (`flashOperationDestFileName`) to be specified. |

| Command | Description |
|---|---|
| `restore-config(17)` | Restore saved configuration from internal flash memory or a PCMCIA flashcard. |
| `backup-config(18)` | Locally save current configuration. |
| `load-mate (19)` | Transfer files to a peer controller in a dual-controller system. |

# *Link-status trap enhancements*

*Units affected: MAX 6000, MAX 3000*

Two new traps, `ascendLinkDown` and `ascendLinkUp`, provide capabilities not offered by the generic `linkDown` and `linkUp` traps defined in RFC 1215.

## Overview

The `ascendLinkDown` and `ascendLinkUp` traps are alarm-class traps. They provide the following information about the interface on which the trap is generated:

- Administrative status
- Operational status
- Name
- Slot number
- Item number

## VT100 interface changes

The Ethernet > SNMP Traps > Enable Traps profile contains the following new parameters:

- Ascend Link Down
- Ascend Link Up

### *Ascend Link Down*

**Description:** Specifies whether the MAX unit generates an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the Simple Network Management Protocol (SNMP) manager.

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

- Yes (the default) specifies that the MAX unit generates an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the SNMP manager.
- No specifies that the MAX unit does not generate an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the SNMP manager.

**Example:** `Ascend Link Down = No`

**Dependencies:** You can set Ascend Link Down to Yes only if Link Down is set to Yes. If Ascend Link Down is set to Yes and Link Down is set to No, the following error message appears:

```
xMessage #330                ??x
xAscend Link Down              x
xcan be enabled only           x
xif Link Down is enabled       x
x                              x
```

**Location:** Ethernet > SNMP Traps > Enable Traps

**See Also:** Ascend Link Up, Link Down

### *Ascend Link Up*

**Description:** Specifies whether the MAX unit generates an `ascendLinkUp` trap when the communication link between the unit and the Simple Network Management Protocol (SNMP) manager is reestablished.

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

- Yes (the default) specifies that the MAX unit generates an `ascendLinkUp` trap when the communication link between the unit and the SNMP manager is reestablished.
- No specifies that the MAX unit does not generate an `ascendLinkUp` trap when the communication link between the unit and the SNMP manager is reestablished.

**Example:** `Ascend Link Up = No`

**Dependencies:** You can set Ascend Link Up to Yes only if Link Up is set to Yes. If Ascend Link Up is set to Yes and Link Up is set to No, the following error message appears:

```
xMessage #331                ??x
xAscend Link Up                x
xcan be enabled only           x
xif Link Up is enabled         x
x                              x
```

**Location:** Ethernet > SNMP Traps > Enable Traps

**See Also:** Ascend Link Down, Link Up

## SNMP changes

The new `AscendVrouterName` object has been added to `ascend.mib`. Following is the object definition:

```
ascendVrouterName                    OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  not-accessible
   STATUS      mandatory
```

```
   DESCRIPTION
   "The Name of the vrouter. The Empty string is the global vrouter."
```

Two new traps have been added to `ascend.mib`:

```
ascendLinkDown    TRAP-TYPE
   ENTERPRISE     ascend
   VARIABLES      { ifIndex, ifAdminStatus, ifOperStatus, ifType,
                    ifName, slotIfSlotIndex, slotIfItemIndex,
                    ascendVrouterName }
   DESCRIPTION    "This trap is in addition to the generic
                  linkDown trap defined in RFC1215. This trap
                  provides additional information such as
                  ifOperStatus, ifName, slotIfSlotIndex,
                  slotIfItemIndex. This is an Alarm class
                  trap and it can be enabled/disabled via
                  alarmEnabled and/or ascendLinkDownTrapEnabled
                  in trap profile."
   ::= 50


ascendLinkUp      TRAP-TYPE
   ENTERPRISE       ascend
   VARIABLES      { ifIndex, ifAdminStatus, ifOperStatus, ifType,
                    ifName, slotIfSlotIndex, slotIfItemIndex,
                    ascendVrouterName }
   DESCRIPTION    "This trap is in addition to the generic
                  linkUp trap defined in RFC1215. This trap
                  provides additional information such as
                  ifOperStatus, ifName, slotIfSlotIndex,
                  slotIfItemIndex. This is an Alarm class
                  trap and it can be enabled/disabled via
                  alarmEnabled and/or ascendLinkUpTrapEnabled
                  in trap profile."
   ::= 51
```

# *Support for Virtual Routers (VRouters)*

*Units affected: MAX 6000, MAX 3000*

This release includes Simple Network Management Protocol (SNMP) support for VRouters. Previously, you could not use SNMP to find VRouter-specific information.

## Overview

Until the current release, an SNMP manager could not request information for a specific VRouter. Now, information about routing tables, ARP tables, statistics, and interfaces can be queried for a specific VRouter on the basis of SNMPv3 context names.

## Using context names

By treating each VRouter as a different context, you can use SNMPv3 context names to query the following MIB II elements for a specific VRouter:

- `system`
- `interfaces`
- `at`
- `ip`
- `cmp`
- `tcp`
- `udp`

Consider the following:

- If no context name is specified, information is reported only for the VRouter on which the SNMP request was received.
- Because context names can be specified only by means of SNMPv3 requests, SNMPv1 queries result in information specific to the source VRouter. For example, if the IP interface on which the SNMPv1 request is received belongs to VRouter1, then only VRouter1-specific information is reported.
- If you use SNMPv3 on an interface belonging to the main VRouter, you can query information for any active VRouter by specifying the correct context name.

## Interface changes

Following are the SNMP changes made for VRouter support:

- No new MIB has been added for reporting VRouter information. Instead, the `vacmContextTable` in `rfc2575.mib` now contains a list of active VRouters, including the main VRouter.
- If a non-null context name specified in an SNMPv3 request is not present in the `vacmContextTable`, no SNMP response is generated.
- The `ifTable` now contains information for a specific VRouter (rather than for all the VRouter interfaces).

# *New trap for unauthorized access*

*Units affected: MAX 6000, MAX 3000*

A new trap, `ascendSecurityAlert`, enables you to detect the source of an intruder who attempts to gain access to the system by means of SNMP. New `syslog` messages report any unauthorized access.

## Overview

The new `ascendSecurityAlert` trap contains the following information:

- IP address from which access was attempted
- The SNMPv1 community string or SNMPv3 USM username that was used to request access

## New trap

Following is the new trap defined in `ascend.trp`:

```
ascendSecurityAlert           TRAP-TYPE
  ENTERPRISE      ascend
  VARIABLES       {
                    ascendNotificationRelatedIpAddress,
                    ascendSecurityBreachUserName
                  }
  DESCRIPTION     "This trap indicates that an unauthorized SNMP
                  request has been made, from
                  ascendNotificationRelatedIpAddress using
                  ascendSecurityBreachUserName as the V1 password
                  or V3 USM user name."
  ::= 49
```

Following is the new variable defined in `ascend.mib`:

```
ascendSecurityBreachUserName       OBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESS  not-accessible
   STATUS mandatory
   DESCRIPTION    "The community string in SNMP V1 packet and the user
                  Name in SNMP V3 packet that sent an un-authorized
                  request."
   ::= { ascendNotificationObjects 2 }
```

## New Syslog messages

The system logs an Alert message if it detects an unauthorized request. The following `syslog` format is used for SNMPv1:

```
LOG alert, Shelf 1, Controller, Time: hour:minute:second--
 Security Alert: attempt to query system from Host ipaddress
```

The following `syslog` format is used for SNMPv3:

```
LOG alert, Shelf 1, Controller, Time: hour:minute:second--
 SNMPV3 Security Alert: attempt to query system from Host ipaddress
```

# New attributes added to RADIUS accounting and call-logging packets

*Units affected: MAX 6000, MAX 3000*

In this release, RADIUS accounting and call-logging Start, Stop, and Checkpoint packets contain new attributes indicating the line type, slot, line, and channel on which a call is established.

## New attributes

The following attributes have been added to the RADIUS accounting and call-logging Start, Stop, and Checkpoint packets:

- Ascend-Dsl-Physical-Channel (10037)
- Ascend-Dsl-Physical-Line (10021)
- Ascend-Dsl-Physical-Slot (10020)
- Ascend-Line-Type (10017)

These attributes apply only to 16-bit VSAs.

### *Ascend-Dsl-Physical-Channel (10037)*

**Description:** Indicates the channel on which a line is established.

**Usage:** The value of Ascend-Dsl-Physical-Channel is an integer.

**Example:** `Ascend-Dsl-Physical-Channel = 3`

**See Also:** Ascend-Dsl-Physical-Line, Ascend-Dsl-Physical-Slot, Ascend-Line-Type, Ascend-NAS-Port-Format

### *Ascend-Dsl-Physical-Line (10021)*

**Description:** Indicates the line on which a call is established.

**Usage:** The value of Ascend-Dsl-Physical-Line is an integer.

**Example:** `Ascend-Dsl-Physical-Line = 1`

**See Also:** Ascend-Dsl-Physical-Channel, Ascend-Dsl-Physical-Slot, Ascend-Line-Type, Ascend-NAS-Port-Format

### *Ascend-Dsl-Physical-Slot (10020)*

**Description:** Indicates the slot on which a call is established.

**Usage:** The value of Ascend-Dsl-Physical-Slot is an integer.

**Example:** `Ascend-Dsl-Physical-Slot = 1`

**See Also:** Ascend-Dsl-Physical-Channel, Ascend-Dsl-Physical-Line, Ascend-Line-Type, Ascend-NAS-Port-Format

### *Ascend-Line-Type (10017)*

**Description:** Indicates the type of line on which a call is established.

**Usage:** Ascend-Line-Type always has the value DS0 (11), which specifies the DS0 channel of a T1 or T3 line.

**Example:** `Ascend-Line-Type = DS0`

**See Also:** Ascend-Dsl-Physical-Channel, Ascend-Dsl-Physical-Line, Ascend-Dsl-Physical-Slot

# *Maximum number of SNMP host entries increased*

*Units affected: MAX 6000, MAX 3000*

In the Ethernet > Mod Config > SNMP Options profile, up to 10 IP addresses of SNMP managers that have Read permission and up to 10 IP address of SNMP managers that have Write permission are available. Formerly, the limit was 8 IP addresses for each type of permission.

**Note:** Be aware that these parameters are deprecated. Although they might appear under certain circumstances, they should not be used. To assign read-only and/or read-write access to SNMP hosts, you must set parameters in the new Ethernet > SNMP Manager profile. For information on this new profile, see "SNMP: Enhancements provide SNMPv3 support and remove host list limitation."

## VT100 interface changes

On a MAX unit, you can now specify up to 10 IP addresses for the RD Mgr*N* parameter and up to 10 IP addresses for the WR Mgr*N* parameter in the Ethernet > Mod Config > SNMP Options profile. Following is a listing of the profile:

```
90-B00 Mod Config
   SNMP options...
      Read Comm=public
      R/W Comm Enable=Yes
      R/W Comm=write
      Security=Yes
      RD Mgr1=0.0.0.0
      RD Mgr2=0.0.0.0
      RD Mgr3=0.0.0.0
      RD Mgr4=0.0.0.0
      RD Mgr5=0.0.0.0
      RD Mgr6=0.0.0.0
      RD Mgr7=0.0.0.0
      RD Mgr8=0.0.0.0
      RD Mgr9=0.0.0.0
      RD Mgr10=0.0.0.0
      WR Mgr1=0.0.0.0
      WR Mgr2=0.0.0.0
      WR Mgr3=0.0.0.0
```

```
WR Mgr4=0.0.0.0
WR Mgr5=0.0.0.0
WR Mgr6=0.0.0.0
WR Mgr7=0.0.0.0
WR Mgr8=0.0.0.0
WR Mgr9=0.0.0.0
WR Mgr10=0.0.0.0
Queue Depth=0
```

# *Remote PING MIB now supported*

*Units affected: MAX 6000, MAX 3000*

This release includes support for the Remote Ping MIB as specified by the Internet Engineering Task Force's (IETF's) Distributed Management Group.

## Overview

Ping MIBs allow the creation of Ping tests that can be set up to periodically issue a series of operations and generate traps or event notifications to report test results.

## Supported tables

In this release, the MAX unit supports the following tables in the Remote Ping MIB:

- Ping Control Table (`pingCtlTable`)
- Ping Results Table (`pingResultsTable`)

## Supported traps

The MAX unit supports the following traps (event notifications) in the Remote Ping MIB:

- `pingProbeFailed`. Generated when a probe failure is detected.
- `pingTestFailed`. Generated when a Ping test is determined to have failed.
- `pingTestCompleted`. Generated at the completion of a Ping test.

## Changes to the Remote Ping MIB

The following changes are made to the standard MIB:

- All the definitions have been changed for compliance with Simple Network Management Protocol version 1 (SNMPv1) Structure of Management Information (SMI).
- The syntax MAX-ACCESS has been changed to ACCESS for all the fields.
- All the MIB fields that had STATUS value as Current have been assigned the Mandatory value instead.
- Fields with read-create access were changed to read-write.

Currently, you cannot modify the following variables, so they have been changed to read-only:

- `pingMaxConcurrentRequests`
- `pingCtlDataFill`
- `pingCtlMaxRows`
- `pingCtlStorageType`
- `pingCtlType`
- `pingCtlIfIndex`
- `pingCtlByPassRouteTable`

### Unsupported features

Currently, the Ping Probe History Table (`pingProbeHistoryTable`) in the Remote Ping MIB is not supported.

# Digital signal processor (DSP) features

## *Introducing MultiDSP modules for MAX units*

*Units affected: MAX 6000, MAX 3000*

MultiDSP for MAX™ provides a set of highly versatile digital signal processor (DSP) modules that support multiple services or applications.

For a unit hosting a MultiDSP module, Lucent Technologies recommends that the number of enabled DSP services be limited to one, either Data (analog and/or digital) service or VoIP service. Though the current release supports Data and VoIP services, it supports just one of the available services on a particular unit. Downloaded software licenses, also known as *hash codes*, determine which DSP services are supported by a particular unit and module combination.

The DSP support provided by a particular MultiDSP module or MAX unit depends on

- The type of module installed in the unit
- Software licenses (hash codes) the host unit supports
- Installation constraints

### MultiDSP module installation constraints

If you intend to enable the MultiDSP module's support for V.92, you must first disable other types of installed modem modules (including modems in the MAX 3000 base unit). Once you enable V.92, the MAX unit cannot support any other type of modem than the MultiDSP for MAX.

If you do not intend to enable V.92, the mix of MultiDSP modules that you can install depends on whether you have a MAX 6000 or a MAX 3000. This section provides you with guidelines to use for each type of unit.

You can install up to two MultiDSP modules in a MAX 6000 unit that already has

- Series56 Digital Modem Modules (or *CSM-1*)
- v.90 S56 Series III Digital Modem module
- No other types of modules

You can install one MultiDSP module in a MAX 3000 unit that already has

- A v.90 S56 Series III Digital Modem module
- No other types of modules

If you intend to enable the MultiDSP module's support for V.92, you must first disable other types of installed modem modules (including modems in the MAX 3000 base unit).

## Upgrading a MAX unit to support MultiDSP modules



**Caution:** A MAX unit does not recognize the MultiDSP module until you have successfully changed the operating system to the current release.

To change a MAX unit's operating system software so that the unit can be configured to support a MultiDSP module, follow these steps:

**1** Acquire TAOS 9.1.0 at `http://www.esight.com`.

**2** Change the unit's operating system software to TAOS 9.1.0 by applying the instructions in the "Changing operating system software" on page 1 of these release notes.

In most cases, stay with the same type of software binary file (also known as a *build* or a *load*). For example, upgrade a MAX unit currently running `ebixk.m60` to the 9.1.0 version of the file named `ebixk.m60`. If you used a software binary file that supported AppleTalk, the following applies:

**Note:** This release discontinues support for AppleTalk. This release changes the names of the MAX 3000 and MAX 6000 loads to reflect the exclusion of support for AppleTalk. As a result, when you upgrade a unit from a previous release to TAOS 9.1.0, you must also change the load you use.

**3** Change the unit's operating system software, once more, to TAOS 9.1.0 (using the instructions in the "Changing operating system software" on page 1.

For a MAX 3000 unit to support a MultiDSP module, use one of the following software binaries files:

- `ebiv.m30`
- `ebixk.m30`
- `ebxk.m30` (previously `ebaxk.m30`)
- `tbiv.m30`
- `tbixkh.m30`
- `tbxkh.m30` (previously `tbaxkh.m30`)

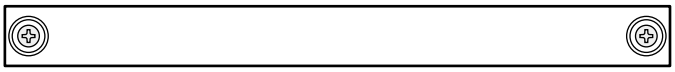
Use one of the following software binaries for a MAX 6000 unit to support up to two MultiDSP modules:

- `ebiv.m60`
- `ebixk.m60`
- `ebxk.m60` (previously `ebaxk.m60`)
- `tbxkh.m60` (previously `tbaxkh.m60`)
- `tbiv.m60`
- `tbixkh.m60`

## Identifying a MultiDSP module

MAX 6000 and MAX 3000 units currently support two types of MultiDSP modules, MultiDSP-48 (labelled *MX-SL-48M-DSP*) and MultiDSP-60 (labeled *MX-SL-60M-DSP*). Figure 2 shows the MultiDSP module. Other than labels, there are no external interfaces or visual indicators to differentiate the versions.

*Figure 2. MultiDSP module*



In a MAX unit's profiles and parameters, the MultiDSP module is identified as `MultiDSP-48` or `MultiDSP-60`. The unit automatically detects the number of ports and displays them in the Main Edit Menu. For example:

```
Main Edit Menu
  00-000 System
  10-000 Net/T1
 >20-000 MultiDSP-60
  30-000 Empty
  40-000 Ethernet
  50-000 Ether Data
  60-000 Serial WAN
  70-000 V.90 S56 III Modem-24
```

In this example, the unit has detected a MultiDSP-60 module.

## Support for data services

A MultiDSP module supports calls made through analog modems that comply with standards such as v.90. Digital calls can come from an ISDN Primary Rate Interface (PRI) line, a Signaling System 7 (SS7) network, or an E1 line with R2 signaling.

Although analog modem service is enabled by default, additional software licenses might be required for support of digital calls that use particular signaling schemes or protocols. For example, R2 call-setup signaling protocol requires an additional license, and so do Access SS7 Gateway Control Protocol (ASGCP) and the IP Device Control (IPDC) protocol, which are the call setup intermachine trunk (IMT) protocols for SS7.

For information about configuring a unit for specific types of calls, see the *MAX 6000/3000 Network Configuration Guide*.

## Support for Voice over IP (VoIP) services

VoIP is a service that offers voice telephony across IP network infrastructures. The MultiDSP module's VoIP implementation relies on the MAX MultiVoice Gateway to connect calls to public and private packet networks. The module's VoIP implementation supports the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard for H.323 signaling and messaging.

VoIP features supported by a MultiDSP module include the following:

- ITU-T H.323 signaling and messaging.
- Voice compression and packetization.
- Connection of each port to a single DS0 channel (voice calls).
- Cut-through of progress tone signals from the distant Public Switched Telephone Network (PSTN).
- Encoding schemes G.711 A-Law, G.711 μ-Law, and G.729.
- Silence suppression and detection for G.729, configured through the MAX unit's VoIP profile. Silence suppression is automatically enabled for G.723.1.
- Real-time fax (T.38 fax).

A VoIP software license is required for DSP support of the VoIP service. An additional software license is required for support of the real-time fax function.

VoIP functions, including real-time fax, are configured through the unit's VoIP profile.

## Configuring and administering the basics

When a MAX unit detects the presence of a module in one of its slots, it creates default profiles appropriate for that type of module. Some default profiles might need to be reconfigured when a new module is installed in a slot.

For a MultiDSP module, minimal configuration is required to set up DSP services on the unit. Depending on the type of module installed, 48 or 60 default call routes are created for each enabled service when the module is installed.

Additional configuration might be required for implementing VoIP MultiVoice functions.

The following sections describe module configuration and administration tasks.

## Using slot-configuration menus and Answer profiles

MultiDSP module configuration includes the following tasks:

- Confirming that the call routes are correct for the desired DSP services. The Mod Config profile controls call routing in the MAX unit. A unit that is running the current software release automatically generates call routes for modem calls or all licensed services, such as MultiVoice, when you install the module.

- Verifying that all other configurations associated with DSP services have been implemented. For example, for Voice-over-IP (VoIP) DSP support, all required configurations for VoIP and other desired MultiVoice features must also be implemented.
- Adding support for an additional DSP service, if necessary.

Perform the following configuration tasks by editing the MAX unit's Mod Config profile:

- Enable or disable a MultiDSP module.
- Enable or disable an individual DSP on a module.
- Specify a default call type.
- Specify up to four answer numbers per call type.

Following is an example of a Mod Config profile that supports DSP services:

```
20-100 Mod Config
 >Module Name=
  Call Numbers...
  Default Call=modem
  Support Complex Coders=No
  MultiDSPSlot=Enable Slot
  DSP #1=Enable DSP
  DSP #2=Enable DSP
  DSP #3=Enable DSP
  DSP #4=Enable DSP
  DSP #5=Enable DSP
  DSP #6=Enable DSP
  DSP #7=Enable DSP
  DSP #8=Enable DSP
  DSP #9=Enable DSP
  DSP #10=Enable DSP
  DSP #11=Enable DSP
  DSP #12=Enable DSP
```

Table 4 describes the parameters you can use to configure support for DSP services.

*Table 4. MultiDSP module-related parameters*

| Parameter | Settings | Description |
|---|---|---|
| MultiDSPSlot | `Enable Slot` (the default) or `Disable Slot` | Specifies whether a MultiDSP module is enabled or disabled. If the module is disabled, all DSPs are disabled and the module will not answer any calls. The default is `Enable Slot`.<br>**Note:** The DSP #*x* parameters all show `N/A` when the MultiDSPSlot parameter specifies `Disable Slot`. |

*Table 4. MultiDSP module-related parameters (continued)*

| Parameter | Settings | Description |
|---|---|---|
| Support Complex Coders (MultiVoice only) | `Yes` (the default) or `No` | Specifies whether the MAX unit supports one port per DSP driver instead of the default (two).<br>**Note:** Specify `Yes` to ensure that the DSP is capable of handling the extra processing required by complex voice coders such as G.723 and G.728. Complex coders require a single port per DSP. |
| Module Name | Accepts the characters you specify. | Specifies a name for a MultiDSP module. The default setting is a blank field. |
| Default Call | `Modem` or `VOIP` (the default) | Specifies the call type a MultiDSP module uses for an unmatched call. The default value varies, depending on the MAX base unit's implementation, as follows:<br>• `VOIP`—MultiVoice<br>• `Modem`— Data/RAS |
| DSP #*x* | `Enable DSP` (the default) or `Disable DSP` | Specifies whether an individual DSP (on a specified MultiDSP module) is enabled or disabled. If an individual DSP is disabled, it will not be allocated to accept any incoming calls. However, any other DSP that is enabled continues to accept incoming calls. |

Use a Call Numbers subprofile, in the unit's Mod Config menu, to specify the answer numbers for each call type a module supports, as in the following example:

```
20-100 Mod Config
 Call Numbers...
 >Modem Ans 1#=
  Modem Ans 2#=
  Modem Ans 3#=
  Modem Ans 4#=
  VoIP Ans 1#=
  VoIP Ans 2#=
  VoIP Ans 3#=
  VoIP Ans 4#=
```

MAX units support both modem calls and VoIP calls. The menu can expand in future releases to include answer numbers for other supported call types. Each entry is of the standard telephone number type as found in the MAX unit's modem configuration menu.

## Displaying the status of the port hosted on each DSP

You can use the MDSP Stat status window to display the status of the logical port hosted on each DSP of a MultiDSP module. To do so, set the Status *x* Config parameter, in the unit's Sys Config profile, to specify that the MAX unit displays the information in the VT100 interface.

Here is an example of the MDSP Stat status window on a unit configured to support the module:

```
+====================+
| x20-000 MDSP Stat  |
| 123456789012345    |
| +**+++++++++++    |
| ++++a++++++****    |
+====================+
```

Table 5 describes the information provided in the MDSP Stat display.

*Table 5. MDSP Stat display*

| Character | Description |
|---|---|
| + | The DSP driver is currently processing two active calls. |
| - | Unused. Available for use. |
| * | Carrier established. |
| . | DSP does not exist. Unavailable for use. |
| a | Outgoing connection pending. |
| A | Connected. No end-to-end data yet. |
| f | DSP failed POST. Unavailable for use. |
| o | DSP disabled. Unavailable for use. |
| p | VoIP carrier. |
| r | Release pending. |
| u | Assigned but not in use. |
| v | Virtual connection up. |

If a DSP driver is currently processing just one active connection, the display reports the status of the active connection. While the MAX unit sets up or releases the second of the DSP driver's two possible connections, the display indicates this activity.

## Using a MAX unit's diagnostics to administer MultiDSP modules

The Lanport Madd diagnostic command, in the MAX unit's Diagnostic command line interface, displays a report on the status of the availability of ports in the MultiDSP module. Each time you enter `lanport madd`, you get a snapshot of current port states and the recent history for each modem. The command is particularly helpful in troubleshooting connection problems, for which you must focus on the ability of individual ports to successfully connect with users.

Each port can be placed in one of six lists the unit generates when you enter the `lanport madd` diagnostic command:

- Available—The unit places a port in its list of available ports whenever none of the other conditions apply.
- Suspect—A port is moved to the Suspect list if its first four calls fail, or if it experiences eight failed (bad) calls in a row. Ports on the Suspect list can still be used if all available ports are in use. Any subsequent successful call to a suspect port places that port back on the available ports list.
- Disabled—If the unit's administrator removed the port from the unit's list of available ports, the port appears in the Disabled list. The port is not available until the unit's administrator changes the status of the port to available.
- Dead—A port that failed at the time of the power-on self test (POST) or during the course of processing calls appears in the Dead list.
- Busy—A port that is currently processing an active call appears in the Busy list. This port becomes available when the active call is cleared and the port is added to the Available list. The `dir` parameter indicates the direction of the last call into each modem. It can have one of the following settings:

  1—Call direction unknown.

  2—Call was outgoing.

  3—Call was incoming.
- Downed—Calls to this port failed and the port is not reliable for normal call processing. A port is moved to the Downed list if it experiences 12 bad calls in a row.

A call is noted as successful if modem handshaking (training) and authentication are successful. A call is noted as bad if modem handshaking fails at any point in the initial call set up, or if the dial-in user does not successfully log in.

**Note:** A call that has been categorized as bad does not necessarily indicate a port problem with the MultiDSP module. Poor line quality, software problems with the calling port, wrong numbers, and forgotten passwords all can generate calls that appear as bad calls but that have nothing to do with ports on the module.

In the following example, the only ports unavailable are those that are busy:

```
> lanport madd
Dump of Available ports list
02:58    67       unused      89 calls,     0 bad, last 32:ffffffff
Dump of Suspect ports list
Dump of Disabled ports list
Dump of Dead ports list
Dump of Busy ports list
02:01    10      carrier      90 calls,     0 bad, last 32:fefbeffe inc
```

```
02:10    19      carrier      83 calls,     0 bad, last 32:ffffffff inc
02:16    25      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:02    11      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:25    34      carrier      88 calls,     0 bad, last 32:ffffffff inc
02:20    29      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:06    15      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:15    24      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:08    17      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:03    12      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:09    18      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:05    14      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:13    22      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:22    31      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:04    13      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:18    27      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:11    20      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:17    26      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:24    33      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:07    16      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:12    21      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:23    32      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:27    36      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:30    39      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:19    28      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:14    23      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:21    30      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:46    55      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:33    42      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:31    40      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:35    44      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:39    48      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:26    35      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:40    49      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:28    37      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:48    57      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:45    54      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:32    41      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:43    52      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:37    46      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:29    38      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:57    66      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:34    43      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:44    53      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:38    47      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:49    58      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:41    50      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:59    68      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:47    56      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:42    51      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:55    64      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:52    61      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:56    65      carrier      90 calls,     0 bad, last 32:ffffffff inc
```

```
02:50    59      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:60    69      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:36    45      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:51    60      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:54    63      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:53    62      carrier      87 calls,     0 bad, last 32:ffffffff inc
Dump of Downed ports list
>
```

To evaluate, for example, port one in slot two (designated 2:01), you must convert the eight-character hexadecimal number to binary to indicate how many of the last 32 calls were successful:

```
fefbeffe = 11111110111110111110111111111110
```

The zeroes show that port 2:01 has had four unsuccessful calls, including the last call.

## Determining modem status with the Show Modem command

The MAX unit's terminal-server command-line interface includes a Show Modem command, which can display a MultiDSP module's possible 48 or 60 ports. An example of the information provided by the Show Modem command issued on a unit configured to support a MultiDSP-48 module follows:

```
ascend% show modem
slot:item   modem   status
3:1         1       idle
3:2         2       idle
3:3         3       idle
3:4         4       idle
3:5         5       idle
3:6         6       idle
3:7         7       idle
3:8         8       idle
3:9         9       idle
3:10        10      idle
3:11        11      idle
3:12        12      idle
3:13        13      idle
3:14        14      idle
3:15        15      idle
3:16        16      idle
3:17        17      idle
3:18        18      idle
3:19        19      idle
3:20        20      idle
3:21        21      idle
3:22        22      idle
3:23        23      idle
3:24        24      idle
3:31        31      idle
3:32        32      idle
3:33        33      idle
```

```
3:34        34      idle
3:35        35      idle
3:36        36      idle
3:37        37      idle
3:38        38      idle
3:39        39      idle
3:40        40      idle
3:41        41      idle
3:42        42      idle
3:43        43      idle
3:44        44      idle
3:45        45      idle
3:46        46      idle
3:47        47      idle
3:48        48      idle
3:49        49      idle
3:50        50      idle
3:51        51      idle
3:52        52      idle
3:53        53      idle
3:54        54      idle
7:1         61      idle
7:2         62      idle
7:3         63      idle
7:4         64      idle
7:5         65      idle
7:6         66      idle
7:7         67      idle
7:8         68      idle
7:9         69      idle
7:10        70      idle
7:11        71      idle
7:12        72      idle
7:13        73      idle
7:14        74      idle
7:15        75      idle
7:16        76      idle
7:17        77      idle
7:18        78      idle
7:19        79      idle
7:20        80      idle
7:21        81      idle
7:22        82      idle
7:23        83      idle
7:24        84      idle
```

## MultiDSP module specifications

Table 6 lists the specifications for the MultiDSP module.

*Table 6. MultiDSP module specifications*

| Specification type | Description or operating requirement |
|---|---|
| Physical interfaces | 48 ports of supported application per MultiDSP-48 module, 60 ports of supported application per MultiDSP-60 module. |
| Power requirements | 4.2 amps maximum at 5 volts |
| Module weight | Approximately 0.584 pounds (0.265kg) |
| Hot swap capability | No |
| Operating altitude | 0 to 14,764 feet (0 to 4500 meters) |
| Operating humidity | Up to 95%, noncondensing |
| Storage humidity | Up to 95%, noncondensing |
| Operating temperature | 23°F to 131° F (-5°C to 55° C) |
| Storage temperature | -40°F to 176° F (-40°C to 80° C) |
| Short-term temperature | 23°F to 131° F (-5°C to 55° C) for a period of not more than 96 consecutive hours and a total of not more than 15 days in one year |
| Maximum rate of temperature change | 86° F per hour (30° C per hour) |

**Note:** Because of the relatively moderate power consumption requirements, a MultiDSP module does not require additional cooling beyond that provided by its host unit.

## MultiDSP modules and supported firmware versions

A MultiDSP module and the current release support the following Analog Devices, Inc. (ADI) firmware versions:

- `v0.1.30` (Controller)
- `v0.1618.1` (RAS)
- `v3.4.2` (VoIP

See MAX TAOS release notes available at `http://www.esight.com` for the latest information about supported firmware versions for MAX units and MultiDSP modules.

# Issuing commands to the unit's MultiDSP modules through Telnet

*Units affected: MAX 6000, MAX 3000*

By means of a Telnet session to a MAX unit's port 5000, you can issue commands to the unit's MultiDSP modules that enable you to display the product code name, controller code version, data pump version, and the least significant byte of controller code.

Once you establish a Telnet session to a unit's port 5000, you can issue commands to the unit's MultiDSP modules. Issue the command in the following format:

`ati`*`n`*

where *n* is a numeric value from 0 to 7.

In the following example, an administrator of a MAX unit establishes a Telnet session to the unit's port 5000 and issues a supported command (`ati1`).

```
telnet 111.222.3.444 5000
Trying 111.222.3.444...
Connected to 111.222.3.444.
Escape character is '^]'.
*** ABCDEFG server ABCDEFG ***
Server ready.

  Connected to modem 6:1...

ati1
229


OK
```

Table 7 describes the commands that you can issue to a MultiDSP module after establishing a Telnet session.

*Table 7. Commands available through Telnet*

| Command (s) | Response from modem |
|---|---|
| `ati` and `ati0` | Product code of installed MultiDSP modules. |
| `ati1` | Least significant byte of controller code, expressed in decimal number format. |
| `ati2` | Returns OK. |
| `ati3` | Returns controller code version. |
| `ati4` | Returns OK. |
| `ati5` | Returns OK. |

*Table 7. Commands available through Telnet (continued)*

| Command (s) | Response from modem |
|---|---|
| `ati6` | Returns modem data pump version. |
| `ati7` | Returns OK. |

# *Supporting V.92 and V.44 features for MAX units*

*Units affected: MAX 6000, MAX 3000*

With this release, a MAX unit's MultiDSP modules support the V.92 modem standard. This is the modem standard that extends the existing V.90 standard with new features that include modem-on-hold and quick-connect. In addition, this release supports the V.44 compression specification. This is a compression specification that is expected to be incorporated as a feature into V.92-capable modems.

By default, V.92 and V.44 are disabled on MAX units and the MultiDSP modules. Use the AT Answer String parameter to issue commands which enable, configure, or disable V.92 and V.44 features for modules installed in the unit.



**Caution:** Only MultiDSP modules support V.92 and V.44. Before you issue AT Answer String commands, disable all other types of installed modem modules (including modems installed in the MAX 3000 base unit). If you do not, the modems will fail to process calls.

Although pulse-code modulation (PCM) upstream is also a V.92 feature, it is not supported with this release.

## Using the AT Answer String parameter

The AT command set provides a set of standard instructions used to activate functions on a modem or a digital signal processor (DSP). Originally developed by Hayes Microcomputer Products, the AT command set is now used by many manufacturers, including Analog Devices, Inc. (ADI), the provider of the firmware version used for the MultiDSP module.

The AT Answer String parameter is located in the System > Sys Config profile. A MAX unit adds a prefix to values you specify for the AT Answer String parameter. In the following example, `+ABC=`*n* represents a value that the unit processes as `AT+ABC=`*n*.

```
00-100 Sys Config
 AT Answer String:
  [+ABC=n]
```

For the entry to be a part of the unit's system configuration, press Enter, press Esc, and then confirm it is to be saved, as in the following example:

```
EXIT?
 0=Esc (Don't exit)
 1=Exit and discard
>2=Exit and accept
```

After a few moments, the unit responds with the following message:

```
Message #117
Profile Stored
```

You can specify a value of up to 36 characters. The unit does not prevent you from entering incorrect characters, and the unit does not respond differently when the string you specify is not a valid part of the AT command set.

When the unit receives an incoming call, it uses the system configuration and the value(s) you specified in the AT Answer String parameter to establish the connection. If the entry you specify in the parameter is invalid, the MultiDSP module does not recognize the command and might fail to process calls altogether.

## Using V.92-related command strings

**Note:** The V.92 modem standard's features apply only when the client modems (as well as the MAX unit and its MultiDSP modules) support the modem standard. If the client modems do not, modem sessions use the V.90 modem standard. Contact the client modem's manufacturer to determine if V.92 support is available.

By default, quick-connect is disabled on the MAX unit and the MultiDSP module. Enable the the feature to shorten the time normally taken by V.90 modems to establish a connection (by reducing the duration of phase 1 and phase 2 modem negotiations). Quick-connect might not function properly if the local loop changes in subsequent calls.

Issue a `+AQC=1` command to enable the quick-connect feature. Issue a `+AQC=0` command to disable the quick-connect feature. For example:

```
00-100 Sys Config
 AT Answer String:
  [+AQC=0]
```

By default, the modem-on-hold feature is also disabled on the unit and the module. Enable the feature to allow a user to use call waiting while engaged in a modem session. The modem connection can be put on hold without being disconnected, and can be resumed when the voice call is completed. An amount of time comparable to the time required for a regular modem handshake can elapse before the modem is reconnected.

Enable the modem-on-hold feature by issuing a command in the following format:

`+AMH=`*`n`*

where *n* is a numeric value from `1` to `13` and specifies the time the unit waits until a modem-on-hold times out. Table 8 describes supported *n* values for the command.

*Table 8. Specifying the time until a modem-on-hold times out*

| Value | Time until modem-on-hold times out |
|---|---|
| 1 | 10 seconds |
| 2 | 20 seconds |
| 3 | 30 seconds |

*Table 8. Specifying the time until a modem-on-hold times out (continued)*

| Value | Time until modem-on-hold times out |
|---|---|
| 4 | 40 seconds |
| 5 | 1 minute |
| 6 | 2 minutes |
| 7 | 3 minutes |
| 8 | 4 minutes |
| 9 | 6 minutes |
| 10 | 8 minutes |
| 11 | 12 minutes |
| 12 | 16 minutes |
| 13 | No limit |

Issue the `+AMH=0` command to disable the modem-on-hold feature. For example:

```
00-100 Sys Config
 AT Answer String
  [+AMH=0]
```

## Using V.44-related commands

The V.44 compression standard is an improvement over the previous V.42bis compression standard and will allow for faster data transfer speeds. The V.44 compression protocol allows V.44-capable modems to negotiate this more efficient protocol instead of the previous V.42bis protocol. While not part of the V.92 specification, the V.44 compression specification has been approved as a standard by the International Telecommunication Union (ITU-T), and is expected to be incorporated as a feature into the vast majority of V.92 capable modems.

By default, the V.44 compression standard is disabled on the unit and the module. Issue the `+v44=1` command string to enable V.44 compression for the MultiDSP module. For example:

```
00-100 Sys Config
  AT Answer String
   [+v44=1]
```

To disable the feature, issue the `+v44=0` command string.

## Combining V.92- and V.44-related commands

You can combine valid commands to enable one feature, disable another, and specify a value for a third feature at one time. For example, the following combination of commands enables quick-connect, sets modem-on-hold to two minutes, and disables V.44 compression:

```
00-100 Sys Config
 AT Answer String
  [+AQC=1+AMH=6+V44=0]
```

You can also disable V.92- and V.44-related features by omitting a feature from the AT command you specify. For example, the following combination of commands also enables quick-connect, sets modem-on-hold to two minutes, and disables V.44 compression:

```
00-100 Sys Config
 AT Answer String
  [+AQC=1+AMH=6]
```

## RADIUS support for V.92

A new V.92 RADIUS attribute has been added to the RADIUS dictionary file to support setting the modem-on-hold-timeout value for an individual connection:

```
ATTRIBUTE      Ascend-MOH-Timeout                  261          integer
```

The following attribute values have been added to the dictionary file:

```
VALUE TS_MOH_DISABLED 0
VALUE TS_MOH_TIMEOUT_10_SEC    1
VALUE TS_MOH_TIMEOUT_20_SEC   2
VALUE TS_MOH_TIMEOUT_30_SEC    3
VALUE TS_MOH_TIMEOUT_40_SEC    4
VALUE TS_MOH_TIMEOUT_1_MIN     5
VALUE TS_MOH_TIMEOUT_2_MIN     6
VALUE TS_MOH_TIMEOUT_3_MIN     7
VALUE TS_MOH_TIMEOUT_4_MIN     8
VALUE TS_MOH_TIMEOUT_6_MIN     9
VALUE TS_MOH_TIMEOUT_8_MIN     10
VALUE TS_MOH_TIMEOUT_12_MIN    11
VALUE TS_MOH_TIMEOUT_16_MIN    12
VALUE TS_MOH_TIMEOUT_NO_LIMIT  13
VALUE TS_MOH_CONN_DEFAULT      14
```

Following is an example RADIUS profile, named Lucent. The last two lines show how you would specify the use of the modem-on-hold timeout marking and set the modem-on-hold timeout value to 16 minutes.

```
   Test     Password              =          "test"
            Service-Type          =          Framed-User,
            Ascend-MOH-Timeout    =          TS_MOH_TIMEOUT_16_MIN
```

## Changed parameters

The AT Answer String parameter is modified by this release.

## AT answer string

**Description:** Enables, disables, or specifies values for V.92 and V.44 features for installed MultiDSP modules.

**Usage:** Issue one or a combination of the following commands, to which the unit adds an AT prefix.

- `+AQC=1`—Enables quick-connect.
- `+AQC=0`—Disables quick-connect.
- `+AMH=`*`n`*—Enables modem-on-hold and specifies the time the unit waits until a modem-on-hold times out where *`n`* is a numeric value `1` to `13`, as follows:
  - `1`—Ten seconds
  - `2`—Twenty seconds
  - `3`—Thirty seconds
  - `4`—Forty seconds
  - `5`—One minute
  - `6`—Two minutes
  - `7`—Three minutes
  - `8`—Four minutes
  - `9`—Six minutes
  - `10`—Eight minutes
  - `11`—Twelve minutes
  - `12`—Sixteen minutes
  - `13`—No limit
- `+AMH=0`—Disables modem-on-hold.
- `+v44=1`—Enables V.44 data compression.
- `+v44=0`—Disables V.44 data compression.

**Example:**

```
00-100 Sys Config
 AT Answer String
  [+AQC=1+AMH=6+V44=0]
```

**Dependencies:** Only the MultiDSP module supports V.92 and V.44. Before you issue AT Answer String commands, disable all other types of modem modules installed in the MAX unit. If you do not disable all other types of modem modules, the modem modules will fail to process calls.

**Location:** System > Sys Config

# RADIUS features

## *Maximum accounting checkpoint interval increased*

*Units affected: MAX 6000, MAX 3000*

In this release, you can specify 24 hours (1440 minutes) as the maximum interval at which a TAOS unit sends checkpoint packets to the RADIUS accounting server. Previously, the maximum interval was 60 minutes.

### VT100 interface changes

You can now specify a value from 0 through 1440 for the Acct Checkpoint parameter in the Ethernet > Mod Config > Accounting profile.

#### *Acct Checkpoint*

**Description:** Specifies the maximum interval, in minutes, at which a TAOS unit sends checkpoint packets to the RADIUS accounting server.

**Usage:** Specify an integer from 0 through 1440. The default is 0 (zero).

**Example:** `Acct Checkpoint = 120`

**Location:** Ethernet > Mod Config > Accounting

**See Also:** Acct Host

## *RADIUS Ascend-NAS-Port-Format (13) value included in Access-Request packets*

*Units affected: MAX 6000*

In this release, the RADIUS Ascend-NAS-Port-Format attribute is included in Access-Request packets. In previous releases, this attribute was included in accounting packets only. Now that the attribute is also included in Access-Request packets, NavisRadius 3.*x* can match Access-Request packets with Accounting-Request packets.

## *RADIUS session-based checkpoint accounting*

*Units affected: MAX 6000, MAX 3000*

You can now configure RADIUS checkpoint accounting on a per-session basis. Instead of sending all checkpoint records at one time, the TAOS unit sends individual checkpoint records for each individual session at the interval you specify.

## VT100 interface changes

You can specify per-session checkpoint accounting by setting a new parameter, ChkPt Timer, in the Ethernet > Mod Config > Accounting profile.

### *ChkPt Timer*

**Description:** Specifies whether to send RADIUS checkpoint accounting packets on a per-session basis.

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

- Per Session specifies that checkpoint packets are sent on a per-session basis at the interval specified by the Acct Checkpoint parameter.
- All Sessions (the default) specifies that checkpoint packets are all sent at the same time.

**Example:** `ChkPt Timer = Per Session`

**Dependencies:** For the ChkPt Timer parameter to apply, RADIUS accounting must be enabled.

**Location:** Ethernet > Mod Config > Accounting

**See Also:** Acct Checkpoint

# *RFC 2867 RADIUS tunnel accounting support for L2F*

*Units affected: MAX 6000, MAX 3000*

This release introduces RADIUS tunnel accounting support for Layer 2 Forwarding (L2F) in accordance with RFC 2867.

## RADIUS changes

In this release, new values have been added for the following attributes:

- Acct-Status-Type
- Ascend-Disconnect-Cause
- Ascend-Connect-Progress

### *New Acct-Status-Type values*

Following are new values for the Acct-Status-Type attribute:

| Value | Indicates that |
|---|---|
| Tunnel-Start (9) | A tunnel has been established.<br>The value specified by the User-Name attribute indicates the name of the dial-in user that initiated the tunnel, if the name is available. The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. |

| Value | Indicates that |
|---|---|
| Tunnel-Stop (10) | A tunnel has been deactivated.<br>The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Reject (11) | A tunnel could not be established.<br>The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. The Ascend-Disconnect-Cause and Ascend-Connect-Progress values indicate the reason for the failure. |
| Tunnel-Link-Start (12) | A client connection using the tunnel has been established.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Link-Stop (13) | A client connection using the tunnel has been deactivated.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Link-Reject (14) | A client connection using the tunnel could not be established.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. The Ascend-Disconnect-Cause and Ascend-Connect-Progress values indicate the reason for the failure. |

## *Sample accounting records for an L2F connection*

Following is an example of a set of accounting records generated by an L2F connection:

```
Tue Aug 29 11:42:32 2000
        User-Name = "PIPELINE"
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        NAS-Port = 30
        Ascend-NAS-Port-Format = 2
        NAS-Port-Type = Sync
        Service-Type = Framed
        Acct-Status-Type = Start
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985246"
        Acct-Authentic = RADIUS
        Vendor-Specific = vAscend-1c060000000a
        Ascend-Modem-PortNo = 19
        Ascend-Modem-SlotNo = 8
        Ascend-Modem-ShelfNo = 1
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
```

```
Tue Aug 29 11:42:32 2000
        User-Name = "PIPELINE"
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        Acct-Status-Type = Tunnel-Start
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985247"
        Acct-Authentic = Local
        Vendor-Specific = vAscend-1c0600000000
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
        Tunnel-ID = "1406ba5f" : 0
Tue Aug 29 11:42:33 2000
        User-Name = "PIPELINE"
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        NAS-Port = 30
        Ascend-NAS-Port-Format = 2
        NAS-Port-Type = Sync
        Service-Type = Framed
        Acct-Status-Type = Tunnel-Link-Start
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985246"
        Acct-Authentic = RADIUS
        Vendor-Specific = vAscend-1c060000000a
        Ascend-Modem-PortNo = 19
        Ascend-Modem-SlotNo = 8
        Ascend-Modem-ShelfNo = 1
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
        Tunnel-ID = "1406ba5f" : 0

Tue Aug 29 11:44:33 2000
        User-Name = "PIPELINE"
```

```
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        Acct-Status-Type = Tunnel-Stop
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985247"
        Acct-Authentic = Local
        Vendor-Specific = vAscend-1c0600000000
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
        Tunnel-ID = "1406ba5f" : 0
        Ascend-Disconnect-Cause = 736
        Ascend-Connect-Progress = 244

Tue Aug 29 11:44:33 2000
        User-Name = "PIPELINE"
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        NAS-Port = 30
        Ascend-NAS-Port-Format = 2
        NAS-Port-Type = Sync
        Service-Type = Framed
        Acct-Status-Type = Stop
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985246"
        Acct-Authentic = RADIUS
        Vendor-Specific = vAscend-1c060000000a
        Acct-Session-Time = 121
        Acct-Input-Octets = 203
        Acct-Output-Octets = 176
        Acct-Input-Packets = 5
        Acct-Output-Packets = 6
        Ascend-Disconnect-Cause = 100
        Ascend-Connect-Progress = 244
        Ascend-Xmit-Rate = 64000
        Ascend-Data-Rate = 64000
        Ascend-PreSession-Time = 1
        Ascend-Pre-Input-Octets = 100
```

```
        Ascend-Pre-Output-Octets = 122
        Ascend-Pre-Input-Packets = 4
        Ascend-Pre-Output-Packets = 4
        Ascend-Modem-PortNo = 19
        Ascend-Modem-SlotNo = 8
        Ascend-Modem-ShelfNo = 1
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
        Tunnel-ID = "1406ba5f" : 0
Tue Aug 29 11:44:33 2000
        User-Name = "PIPELINE"
        NAS-IP-Address = 10.6.0.3
        Ascend-Owner-IP-Addr = 0.0.0.0
        NAS-Port = 30
        Ascend-NAS-Port-Format = 2
        NAS-Port-Type = Sync
        Service-Type = Framed
        Acct-Status-Type = Tunnel-Link-Stop
        Acct-Delay-Time = 0
        Acct-Session-Id = "335985246"
        Acct-Authentic = RADIUS
        Vendor-Specific = vAscend-1c060000000a
        Ascend-Modem-PortNo = 19
        Ascend-Modem-SlotNo = 8
        Ascend-Modem-ShelfNo = 1
        Tunnel-Type = L2F : 0
        Tunnel-Server-Endpoint = "10.1.1.2" : 0
        Tunnel-Client-Auth-ID = "NAS_NAME" : 0
        Tunnel-Server-Auth-ID = "HGW_NAME" : 0
        Tunnel-ID = "1406ba5f" : 0
        Ascend-Disconnect-Cause = 736
        Ascend-Connect-Progress = 244
```

## Command-line changes

The L2F debug command now accepts an additional qualifier to enable accounting-related debugging. The following command toggles accounting debugging for L2F:

```
admin> l2f accounting
```

# RFC 2867 RADIUS tunnel accounting support for L2TP

*Units affected: MAX 6000, MAX 3000*

This release introduces RADIUS tunnel accounting support for Layer 2 Tunneling Protocol (L2TP) in accordance with RFC 2867.

## VT100 interface changes

The new ATC Encoding parameter has been added to the Ethernet > Mod Config > L2 Tunneling Options > L2TP Config profile.

### *ATC Encoding*

**Description:** Specifies the encoding method used for the RADIUS Acct-Tunnel-Connection attribute.

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

| Value | Specifies that |
|---|---|
| Normal (the default) | The value specified by the Acct-Tunnel-Connection attribute consists of the source and destination IP addresses, tunnel IDs, and connection IDs. This value is for use with NavisRadius. |
| CSN-Dec | The value specified by the Acct-Tunnel-Connection attribute represents the 32-bit L2TP Call Serial Number (CSN) as present in the Incoming-Call-Request (ICRQ) or Outgoing-Call-Request (OCRQ) L2TP message, encoded as a decimal string. For the tunnel itself, no CSN exists, and the 32-bit value that is encoded represents the initiator Tunnel ID in the low 16 bits and the server Tunnel ID in the high 16 bits. |
| CSN-Hex | The value specified by the Acct-Tunnel-Connection attribute represents the L2TP CSN as present in the ICRQ or OCRQ L2TP message, encoded as a hexadecimal string. |

**Example:** `ATC Encoding = CSN-Dec`

**Dependencies:** There is no guarantee that the CSN is unique at all times. Even in a single tunnel, identical CSN values can occur if tunnel links are initiated from both the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS) side. Therefore, use caution when specifying the CSN with the Acct-Tunnel-Connection attribute.

**Location:** Ethernet > Mod Config > L2 Tunneling Options > L2TP Config

## RADIUS changes

Following are new values for the Acct-Status-Type attribute:

| Value | Indicates that |
|---|---|
| Tunnel-Start (9) | A tunnel has been established.<br>The value specified by the User-Name attribute indicates the name of the dial-in user that initiated the tunnel, if the name is available. The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Stop (10) | A tunnel has been deactivated.<br>The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Reject (11) | A tunnel could not be established.<br>The value specified by the Acct-Tunnel-Connection attribute is identical in all link and session accounting records for the tunnel. The Ascend-Disconnect-Cause and Ascend-Connect-Progress values indicate the reason for the failure. |
| Tunnel-Link-Start (12) | A client connection using the tunnel has been established.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Link-Stop (13) | A client connection using the tunnel has been deactivated.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Link-Reject (14) | A client connection using the tunnel could not be established.<br>The value specified by the Acct-Session-Id attribute is identical in all link and session accounting records for the tunnel. The Ascend-Disconnect-Cause and Ascend-Connect-Progress values indicate the reason for the failure. |

# MultiVoice features

## *Sequential dialing (H.323 caller originated disconnect)*

*Units affected: MAX 6000, MAX 3000*

In this release, new calls can be initiated by a user while a current call is in progress and is in any one of these stages: call proceeding, call alerting, call connected, or call busy.

A new call can be initiated by dialing a string (for example, `**9`) as specified in the new Next Call parameter in the Voip profile. Once the dialing string has been entered, the user hears a dial tone and can then proceed to enter the entire 7- or 10-digit (if the call is a long-distance call) number.

**Note:** While dialing, the digits must be entered within the time limit specified in the Inter Digit Timer parameter. If the digits are not entered within the time limit, the user must reenter the entire sequence of digits again. By default, callers have up to 6 seconds to enter each digit of a telephone number. However, the amount of time given to enter each digit can be changed.

## New Next Call parameter

This enhancement adds the Next Call parameter in the Voip profile, as described below.

A new call can be initiated while a current call is in progress when a user dials a string that matches the pattern as specified in the Next Call parameter.

The default value for the Next Call parameter is `**9`. However, the default can be changed to any string with a length between 1 and 5 digits or characters (for example, `**1`, `**999`). Each digit or character can be a number between 0 and 9 or *. Specifying # in the string is not allowed.

## Enabling next calls

The following procedure illustrates how to enable the Next Call feature with a value other than the default using the command line editor.

**1** From the MAX administration menu, select the Ethernet > Mod Config profile.

**2** Scroll down to the VOIP Options. . ., then press the Enter key to open this profile.

**3** Disable single-dialing. Scroll down to the Single Dial Enable parameter, then press the Enter key to open a command line with the cursor positioned, as shown below. Use the right arrow key to position the cursor over the selection you want to change. You must set this to `no`.

**Single Dial Enable:**
**[no]**

**4** Scroll up to the DTMF Tone Passing parameter, then press the Enter key to open a command line with the cursor positioned as shown below. Use the right arrow key to position the cursor over the selection you want to change. You must set this to `dtmf tone passed outofband`.

**DTMF Tone Passing:**
**[dtmf tone passed outofband]**

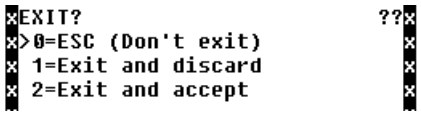
**5** Enable sequential calling. Scroll down to the Sequential Call Enable parameter, then press the Enter key to open a command line with the cursor positioned as shown below. Use the right arrow key to position the cursor over the selection you want to change. You must set this to `yes`.

**Sequential Call Enable:**
**[yes]**

**6** Scroll down to the Next Call parameter, then press the Enter key to open a command line with the cursor positioned as shown below. Use the right arrow key to position the cursor over the value you want to change. This example sets it to `**10`.

**Next Call:**
**[**10]**

**7** Press the Esc key to exit the set up and press it again to exit the options list. **Exit** and **accept** your changes as prompted by the screen below:




## Contingencies

New calls can be initiated only when the following parameters are configured in the Voip profile:

- The Single Dial Enable parameter

  Must be set to `no` because the MultiVoice Gateway must use two-stage dialing. The Single Dial Enable parameter enables or disables single-stage dialing of VoIP calls when MultiVoice is configured to perform H.323 call processing. In two-stage dialing, callers must dial the MAX, before being prompted to dial the called telephone number.

- The DTMF Tone Passing parameter

  Must be set to `Dtmf Tone Passed Outofband`. The parameter filters the tone from the voice path and passes the corresponding digits to the far-end gateway using a non-RTP path. Once received at the far end, the digits are played out. This out-of-band processing works even with both gateways operating in opposite modes. For example, when an inband gateway is talking to an out-of-band gateway, the inband gateway accepts the out-of-band DTMF play-out commands.

- The Sequential Call Enable parameter

  Must be set to `yes`. When this parameter is set to yes and a PIN is required to authenticate MultiVoice calls, reentering the PIN is not required to dial the next VoIP call, as long as the connection between the PSTN and near-end MultiVoice Gateway has not been terminated.

# *H.323 (v2) fastStart support*

*Units affected: MAX 6000, MAX 3000*

The H.323 (v2) fast connect procedure allows for faster call completion. Fast connect provides faster call setup and with fewer round-trip connections needed to establish a call between end points.

H.323 (v2) defines a fast connect procedure, which is also known as *fastStart.* This fast connect procedure streamlines the connection establishment of calls when

- Capabilities exchange is not necessary
- End point compatibility is assumed

H.245 capabilities exchange is performed *after* the fast connect procedure is completed, because the logical channel set-up exchange is embedded in the H.225 message exchange. However, open logical channel exchange is not performed.

With fast connect, messaging can be collapsed into a single handshake consisting of a setup message and a connect message.

The fast connect procedure results in much faster call setup in the network than that provided by the standard H.245 procedure. In situations in which fast connect is unsuccessful, the call is automatically set up using standard H.245 procedures instead.

Upon completion of the fast connect procedure, to set up a voice call, the H.245 procedure is initiated and all mandatory H.245 procedures need to be completed using either H.245 tunneling or H.245 connection. This is especially important if you use a third-party gateway that does not support the fallback condition. In this case, the call will be released due to H.245 time-out.

## H.323 (v2) fast connect call flow

The following call flow occurs when H.323 (v2) fast connect is used.

The calling end point sends a setup message to the called end point. The setup message contains a fastStart element with the following audio mode information:

- Codec
- Rate
- RTP/RTCP addresses

If the called end point initiates the use of the fast connect procedure for the call, the called end point may return information in the call proceeding, call alerting, and call connect messages that contain a fastStart element.

If the called end point fails to initiate the use of the fast connect procedure, the called end point may respond with a call proceeding, call alert or call connect message that does not contain a fastStart element.

If the calling end point receives call proceeding, call alert, or call connect messages without a fastStart element, the calling end point terminates the fast connect procedure. The calling end point also completes the H.245 procedure, using one of the following two methods:

- H.245 tunneling, provided that H.323 tunneling is supported at both end points
- A separate H.245 channel

## Reverting to the H.245 connection

When fast connect is being used, either end point can initiate a separate H.245 connection at any time. Initiation of an H.245 connection is required under either of the following conditions:

- If either end point does not support the fastStart element and H.245 tunneling
- If a call uses the fastStart element and if H.245 tunneling is not supported for the call

When either end point initiates a separate H.245 connection, this supports:

- Fax transmission
- Invoking the call feature that require the use of H.245 procedures such as Out-of-Band (OOB) DTMF.

## H.245 call flow

All mandatory H.245 protocol elements that normally occur upon initiation of an H.245 connection are completed prior to initiation of any additional H.245 procedures. These include:

- Cap exchange
- Master/slave determination

**Note:** The media channels that are established as a result of the fast connect procedure are inherited as though they had been opened using normal H.245 OpenLogicalChannel and OpenLogicalChannelAck procedures. For such inheritance to succeed, media sessions opened during the fast connect procedure must use only well-known sessionID values, as defined in the H.245 standard.

## Using fastStart with H.245 tunneling

When a fastStart element is being used, either end point can initiate the use of H.245 tunneling. H.245 tunneling is required under either of the following circumstances to:

- Support the fax transition
- Invoke call features that require the use of H.245 procedures

A calling end point can also include both a fastStart element and can set the `h245Tunneling` field to TRUE within the same setup message. Similarly, a called end point can include a fastStart element and set the `h245Tunneling` field to TRUE within the same Q.931 response. In this instance, the fast connect procedures are followed, and the H.245 connection is not established until the actual transmission of the first tunneled H.245 message has occurred, or until the separate H.245 connection has been opened.

**Note:** In the H.323 (v2) standard, the calling end point must include one but *not* both of the following in the same setup message:

- A fastStart element
- An encapsulated H.245 messages in H245Control

The presence of the encapsulated H.245 message in this instance overrides the Fast Connect procedure.

## Terminating the H.323 V2 Fast Connect procedure

The Fast Connect procedure is terminated when one of the following events has occurred:

- An encapsulated H.245 message is sent
- A separate H.245 connection by either end point prior to the sending of a Q.931 message containing fastStart by the called end point is initiated

## New Faststart Enable parameter

A new parameter has been added, which enables and disables the fastStart feature.

If the Faststart Enable parameter is enabled (set to `yes`), the fast connect procedure is initiated. Yes is the default value.

Values assigned to the Faststart Enable parameter cause fastStart to be enabled (`yes`) or disabled (`no`.)

### *Enabling fastStart*

The following procedure illustrates how to enable fastStart:

1. From the MAX administration menu, select the Ethernet > Mod Config profile.
2. Scroll down to the VOIP Options. . ., then press the Enter key to open this profile.
3. Scroll down to the Faststart Enable parameter, then press the Enter key to open a command line with the cursor positioned, as shown below:

```
Faststart Enable:
[yes]
```

   Use the right arrow key to position the cursor over the value you want to select. You can leave the setting as `yes`, the default, to enable fastStart.

4. Press the Esc key to exit the set up and press it again to exit the options list. Exit and Save your changes as prompted by the screen below:

```
EXIT?                          ??
>0=ESC (Don't exit)
 1=Exit and discard
 2=Exit and accept
```

### *External interface changes*

The fastStart element has been added to the H.225 setup, call proceeding, call alert, and call connect messages.

# *New MAX MultiDSP modules supported*

*Units affected: MAX 6000, MAX 3000*

In this release, support for these two new features has been added:

- Voice over IP (VoIP) traffic is now supported on the MAX 3000.
- The MAX 3000 and MAX 6000 support new MAX MultiDSP modules. The MAX MultiDSP module is a DSP resource module that supports either voice over IP (VoIP) or data traffic from a single circuit card.

## Voice over IP (VoIP) support on MAX 3000

When a MAX 3000 is configured with a new MAX MultiDSP module, VoIP services are supported. VoIP is a service that offers voice telephony across IP network infrastructures. The MAX MultiDSP module VoIP implementation relies on the MultiVoice™ gateway to connect calls to public and private packet networks. The card's VoIP implementation supports the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard for H.323 signaling and messaging.

VoIP features supported by the MAX MultiDSP module include the following:

- (ITU-T) H.323 signaling and messaging.
- Voice compression and packetization.
- Connection of each port to a single DS0 (voice calls).
- Cut-through of progress-tone signals from the distant Public Switched Telephone Network (PSTN).
- Encoding schemes G.711 A-law, G.711 μ-law, G.729, G.723, full rate GSM (FRGSM).
- Silence suppression and detection for G.729 configured through the VoIP profile. Silence suppression automatically enabled for G.723.
- Real-time fax (T.38 fax).
- Voice announcements.

**Note:** Since the MAX 3000 does not have an external flash card, voice announcements must be stored on a remote TFTP host. The MAX 3000 downloads the files upon startup or when the announcement profiles are changed.

A VoIP software license is required for DSP support of the VoIP service. An additional software license is required for support of Real-Time Fax functionality.

VoIP functionalities, including real-time fax, are configured through the VoIP profile.

For details about VoIP and MultiVoice configuration, refer to the *MultiVoice for the MAX Configuration Guide*.

## New MAX MultiDSP modules on MAX 6000, 3000

The MAX MultiDSP module, similar to the MultiDSP 48-port slot card (TNTV-SL-ADI-C) and MultiDSP 96-port slot card (APX8-SL-96DSP) currently available for the MAX TNT and the APX gateway products, can be used in the MAX 3000 and MAX 6000 gateways. The MAX MultiDSP module can be configured for either voice *or* data operation on a per-chassis basis. An Universal Port “any-service-any-port” configuration is *not* supported in this release. There are two different MAX MultiDSP modules available (see Table 9).

*Table 9. MAX MultiDSP module types for MultiVoice*

| Card type | Notes |
|---|---|
| MultiDSP-48 port (MX-SL-48M-DSP) | 48-port DSP module. Recommended for VoIP or modem use. Provides support for up to (48) sessions of VoIP or data communications.<br>Simple and complex codecs are supported (G.711, G.729(A), G.723.1, G.728, Full-Rate GSM). |
| MultiDSP-60 port (MX-SL-60M-DSP) | 60-port DSP module. Recommended for VoIP or modem use. Provides support for up to (60) sessions of VoIP or data communications.<br>G.711 and G.729(A) simple codecs supported only. |

## Data services

The MAX MultiDSP module supports calls made through analog modems that comply with standards such as V.90. Digital calls can come from an ISDN Primary Rate Interface (PRI) line or an E1 line with R2 signaling.

Although analog modem service is enabled by default, additional software licenses might be required to support digital calls that use particular signaling schemes or protocols. For example, a MAX software license is required to support the R2 call setup signaling protocol.

For information about configuring a MAX for specific types of calls, refer to the MAX *6000/3000 Network Configuration Guide*.

## Configuring and administering the basics

The VoIP configuration and call setup procedures on the MAX 3000 are the same as for the MAX 6000. The VoIP license must be enabled to make VoIP calls on the MAX MultiDSP module.

When a MAX detects the presence of a card in one of its slots, the MAX creates default profiles appropriate for that type of card. Some default profiles might need to be reconfigured when a new card is installed in a slot.

For the MAX MultiDSP module, minimal configuration is required to set up DSP services on the MAX. Depending on the type of MAX MultiDSP module installed, either 48 or 60 default call routes are created for each enabled service when the card is installed.

Configuration might be required for implementing VoIP MultiVoice functionality. MultiVoice configuration is described in the *MultiVoice for the MAX Configuration Guide* and the *MultiVoice Access Manager User's Guide.*

### Configuration tasks

MAX MultiDSP module configuration includes the following tasks:

- Confirm that the call routes are correct for the desired DSP services. The Mod Config profile controls call routing in the MAX. A MAX that is running TAOS 9.1.0 automatically generates call routes for modem calls or all licensed services, such as MultiVoice, when you install the slot card.
- Verify that all other configurations associated with DSP services have been performed. For example, for Voice-over-IP (VoIP) DSP support, all required configurations for VoIP, and other desired MultiVoice features must also be performed.
- Add support for an additional DSP service, if necessary.

### Main configuration screen

You can configure the MAX MultiDSP module from the main configuration screen. The MAX MultiDSP module appears as MultiDSP-*XX*, where *XX* indicates the number of DSP ports on the installed card. The following shows an example of the VT100 interface for an installed MultiDSP 48-port card.

```
========== MAX EDIT ========
 |Main Edit Menu               |
 | 00-000 System               |
 | 10-000 Net/T1               |
 | 20-000 Empty                |
 | 30-000 MultiDSP-48          |
 | 40-000 Ethernet             |
 | 50-000 Ether Data           |
 | 60-000 Not Avail            |
 | 70-000 Not Avail            |
 |                             |


   ========== MAX EDIT ========
   |30-000 MultiDSP-48 |
   | 30-100 Mod Config         |
   |                           |
   |                            |


 ========== MAX EDIT ========
 |30-100 Mod Config          |
 |>Module Name=              |
 | Call Numbers...           |
 | Default Call=VOIP         |
 | Support Complex Coders=NO |
 | MaddSlot=Enable Slot      |
 | DSP #1=Enable DSP         |
 | DSP #2=Enable DSP         |
 | DSP #3=Enable DSP         |
 | ...                       |
 | ...                       |
 | DSP #30=Enable DSP        |
```

### *Mod Config profile parameters*

The Mod Config profile parameters configure the following configuration tasks:

- Enables or disables a MAX MultiDSP module.
- Enables or disables an individual DSP on a MAX MultiDSP module.
- Specifies a default call type.
- Specifies up to four answer numbers per call type.

This release adds MAX MultiDSP module configuration to the Mod Config profile to support MAX as follows:

```
30-100 Mod Config
 >Module Name=
  Call Numbers...
  Default Call=voip
  Support Complex Coders=No
  MaddSlot=Enable Slot
  DSP #1=Enable DSP
  DSP #2=Enable DSP
  ...
  DSP #11=Enable DSP
  DSP #12=Enable DSP
```

Table 10 describes the parameters that configure the MAX MultiDSP module.

*Table 10. MAX MultiDSP module parameters*

| Parameter | Description |
|---|---|
| MaddSlot | Enable or disable the slot in which the MAX MultiDSP module is installed. If the slot card is disabled then all DSPs are also disabled and no calls are answered. The default is Enable Slot.<br>**Note:** The DSP #*x* parameters are shown as `N/A` when the MaddSlot parameter is set to `Disable Slot`. |
| Support Complex Coders | If set to Yes (the default), complex voice coders (such as G.723.1, G.728, and Full-Rate GSM) in addition to simple voice coders can be used. However, the additional processing needed by complex voice coders will reduce the capacity and the number of ports available will decrease to either 24 or 30 ports.<br>If set to No, only simple voice coders can be used (G.711 A-law, G.711 µ-law, or G.729(A)). |
| Module Name | Specifies a name for a MAX MultiDSP module slot card. Valid values are any alphanumeric characters. The default setting is a null setting. |
| Default Call | Specifies the call type a MAX MultiDSP module uses for an unmatched call. Valid values are Modem or VOIP. The default is VOIP. |
| DSP #*x* | Specifies whether an individual DSP (on a specified MAX MultiDSP module slot card) is enabled or disabled. If an individual DSP is disabled it does not accept any incoming calls. However, any other DSP that is enabled continues to accept incoming calls. Valid values are Enable DSP or Disable DSP. The default is Enable DSP. |

### *Call Number subprofile*

This release includes a Call Numbers subprofile in the Mod Config profile that specifies the answer numbers for each call type a MAX MultiDSP module can support.

```
30-100 Mod Config
 Call Numbers...
```

```
>Modem Ans 1#=
 Modem Ans 2#=
 Modem Ans 3#=
 Modem Ans 4#=
 VoIP Ans 1#=
 VoIP Ans 2#=
 VoIP Ans 3#=
 VoIP Ans 4#=
```

Modem *or* VoIP calls are supported on a MAX unit. Each entry is of the standard phone number type found in the MAX unit's modem configuration menu. The menu might expand in future releases to include answer numbers for other supported call types.

## *Displaying the status of ports for each DSP*

Use MADD Stat status window to display the status of the logical port hosted on each DSP of a MAX MultiDSP module. To specify that the MAX displays the information on the MAX unit's VT100 interface, use the `Status x Config` parameter in the MAX unit's Sys Config profile.

The following sample of the MADD Stat status window shows a MAX unit configured to support a MAX MultiDSP module:

```
+====================+
| x30-000 MADD Stat  |
| 123456789012345    |
| +**++++++++++++    |
| ++++a++++++****    |
+====================+
```

Table 11 describes the information provided in the Madd MAX *xx* status display.

*Table 11. Madd MAX status display*

| Character | Description |
|---|---|
| + | The DSP driver is currently processing two active calls. |
| - | The DSP port is unused. Available for use. |
| * | Carrier established. |
| . | DSP doesn't exist. Unavailable for use. |
| a | Outgoing connection pending. |
| A | Connected. No end-to-end data yet. |
| f | DSP failed POST. Unavailable for use. |
| o | DSP disabled. Unavailable for use. |
| p | VoIP carrier. |

*Table 11. Madd MAX status display (continued)*

| Character | Description |
|---|---|
| r | Release pending. |
| u | Assigned but not in use |
| v | Virtual connection is up. |

## *Using MAX diagnostics to administer a MAX MultiDSP module*

The Lanport Madd diagnostic command, in the MAX unit's Diagnostic Command-Line Interface (CLI), displays a report on the status of the availability of ports in the MAX MultiDSP module unit. Each time you enter `lanport madd`, you get a snapshot of current port states and the recent history for each modem. The command is particularly helpful for troubleshooting connection problems, for which you must focus on the ability of individual ports to successfully connect with users.

The status of each port can be placed in one of six lists the MAX generates when you enter the `lanport madd` diagnostic command:

- Available—The MAX unit places a port in its list of available ports whenever none of the other conditions apply.
- Suspect—A port moves to the suspect list if its first four calls are bad or if it experiences eight bad calls in a row. Ports on the suspect list can still be used if all available ports are in use. Any subsequent successful call to a suspect port places that port back on the available ports list.
- Disabled—The MAX unit's administrator removed the port from the unit's list of available ports. The port is not available until the MAX unit's administrator changes the status of the port to available.
- Dead—At the time of power-on self test (POST) or during the course of processing calls, the port failed.
- Busy—The port is currently processing an active call. This port becomes available when the active call is cleared and the port is added to the available ports list. The `dir` parameter indicates the direction of the last call into each modem. It can have the following settings:

  1 — Call direction unknown

  2 — Call was outgoing

  3 — Call was incoming
- Downed—Calls to this port failed and the port is not reliable for normal call processing. A port is moved to the downed list if it experiences twelve bad calls in a row.

A call is successful if modem handshaking (training) and authentication are successful. A call is bad if modem handshaking fails at any point in the initial call set-up, or if the dial-in user does not successfully log in.

**Note:** A call that is categorized as bad does not necessarily indicate a port problem with the MAX MultiDSP module. Poor line quality, software problems with the calling port, wrong numbers, and forgotten passwords can all generate calls that appear as bad calls but are not associated with ports on the MAX MultiDSP module.

```
> lanport madd
Dump of Available ports list
02:58    67       unused      89 calls,     0 bad, last 32:ffffffff
Dump of Suspect ports list
Dump of Disabled ports list
Dump of Dead ports list
Dump of Busy ports list
02:01    10      carrier      90 calls,     0 bad, last 32:fefbeffe inc
02:10    19      carrier      83 calls,     0 bad, last 32:ffffffff inc
02:16    25      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:02    11      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:25    34      carrier      88 calls,     0 bad, last 32:ffffffff inc
...
...
02:51    60      carrier      90 calls,     0 bad, last 32:ffffffff inc
02:54    63      carrier      89 calls,     0 bad, last 32:ffffffff inc
02:53    62      carrier      87 calls,     0 bad, last 32:ffffffff inc
Dump of Downed ports list>
```

Looking at port one in slot two (designated 2:01), the eight-digit hexadecimal number has to be converted to binary to indicate how many of the last 32 calls were successful:

```
fefbeffe = 11111110111110111110111111111110
```

The ones above show that port 2:01 has had 28 successful calls.

## *Using the Show Modem command*

The MAX unit's terminal-server command line interface (CLI) includes a Show Modem command, which can now display a MAX MultiDSP module unit's possible 48 or 60 ports. The Show Modem command issued on a MAX unit configured to support a MultiDSP 60-port slot card displays the following sample output:

```
ascend% show modem
slot:item   modem   status
3:1         1       idle
3:2         2       idle
3:3         3       idle
3:4         4       idle
...
...
3:51        51      idle
3:52        52      idle
3:53        53      idle
3:54        54      idle
...
...
```

## MAX MultiDSP module specifications

MAX MultiDSP module specifications appear in Table 12.

*Table 12. MAX MultiDSP module card specifications*

| Specification Type | Description or Operating Requirement |
|---|---|
| Physical interfaces | 48 ports of supported application per MultiDSP 48-port slot card, 60 ports of supported application per MultiDSP 60-port slot card. |
| Power requirements | 4.2 amps maximum at 5 volts |
| Module weight | Approximately 0.584 pounds (0.265kg) |
| Hot-swap capability | No |
| Operating altitude | 0 to 14,764 feet (0 to 4500 meters) |
| Operating humidity | up to 95%, noncondensing |
| Storage humidity | up to 95%, noncondensing |
| Operating temperature | 23 to 131° F (-5 to 55° C) |
| Storage temperature | -40 to 176° F (-40 to 80° C) |
| Short-term temperature | 23° to 131° F (-5 to 55° C) for a period of not more than 96 consecutive hours and a total of not more than 15 days in one year |
| Maximum rate of temperature change | 86° F per hour (30° C per hour) |

**Note:** The MAX MultiDSP module does not require additional cooling beyond that which is provided by its host MAX.

# Reporting call failures in cause codes

*Units affected: MAX 6000, MAX 3000*

In this release, the MultiVoice Gateway has been modified to report the call progress cause code into the billing disengage request (DRQ). The new cause code is recorded in call detail records (CDRs) and in debug information so that all necessary information can be examined to determine the precise point of failure.

## Background

Historically, many ISDN switches sent a release complete message instead of the call progress message that contained the call failure reason. The message oftentimes reported ambiguous and misleading call failure information. The real reason of failure was contained in the call progress message, but was ignored. The call progress message contained a CAUSE field that includes the type of call failure (for example, Invalid Number Format).

## Implementation details

To more accurately reflect the exact cause of call failure, the following were implemented:

- When a Call Progress message contains a Progress Indicator of 8 from the PSTN, the value of the Q.391 cause code is captured. The reason indicates why the call failed (for example, Invalid Number Format).
- A new field is added to the disengage request (DRQ) message. A progress cause code is a embedded in this DRQ message, which is recorded by the Gatekeeper (for example, MVAM).
- The Gatekeeper includes the new cause code information in a new field of the call detail record (CDR). Look at the release cause code of the CDR to determine if a problem occurred during the processing of the call.
- The new cause code information is displayed using `h323debug`.

# H.323 Annex D T.38 fax support

*Units affected: MAX 6000, MAX 3000*

## Feature definition

This release includes support for real-time facsimile (FAX) interoperability with other vendors H.323 gateways, through the implementation of the H.323 Annex D standard. This implementation, which also requires the use of recommendation T.38, allows FAX interoperability with gateways of other vendors that have implemented this standard. MultiVoice-to-MultiVoice communication for FAX uses a prestandard version of T.38, which includes improved feature performance.

## User interface

The MultiVoice gateway must be licensed to use real-time fax. To configure this gateway for Fax, Enable `Fax` mode and `Fast Start` for Annex D Fax.

To enable Fax mode:

1. Select `Ethernet` from `Main Edit` Menu.
2. Select `Mod Config.`
3. Select `RT Fax Options.`
4. Press Enter (toggle enables RT Fax, changing it to Yes.

*Figure 3. RT Fax Enabling on MAX: Main Edit, Ethernet, ModConfig Screens)*

```
Main Edit Menu
 00-000 System
 10-000 Net/T1
 20-000 Net/T1
 30-000 VOIP-16
 40-000 VOIP-16
 50-000 VOIP-16
 60-000 VOIP-16
 70-000 VOIP-16
 80-000 VOIP-16
>90-000 Ethernet
 A0-000 Ether Data
 B0-000 Serial WAN
 C0-000 Ether Data
 D0-000 Ether Data
```

```
90-000 Ethernet
 90-100 Connections
 90-200 Names / Passwords
 90-300 Bridge Adrs
 90-400 Static Rtes
 90-500 Filters
 90-600 Frame Relay
 90-700 Answer
 90-800 SNMP Traps
 90-900 SNMPv3 USM Users
 90-A00 SNMPv3 Notifications
 90-B00 SNMPv3 Target Params
 90-C00 Virtual Routers
>90-D00 Mod Config
```

```
90-D00 Mod Config
 Module Name=
 Ether options...
 WAN options...
 SNMP options...
 OSPF options...
 OSPF global options...
 Route Pref...
 VOIP Options...
>RT Fax Options...
 PSTN Options...
 TServ options...
 Bridging=N/A
 Shared Prof=No
 Telnet Security=Global
 Telnet PW=
 RIP Policy=Poison Rvrs
```

*Figure 4. RT Fax Enabling on MAX: RT Fax Screens*

```
90-D00 Mod Config          ??
 RT Fax Options...
 >T.38 Fax Enabled=No
  ECM Enabled=N/A
  Low Latency Mode=N/A
  Command Spoof=N/A
  Local Retransmit LSF=N/A
  Packet Redundancy=N/A
  Fixed Packets=No
  Max Rate=14400
```

```
90-D00 Mod Config          ??
 RT Fax Options...
 >T.38 Fax Enabled=Yes
  ECM Enabled=Yes
  Low Latency Mode=Yes
  Command Spoof=N/A
  Local Retransmit LSF=N/A
  Packet Redundancy=N/A
  Fixed Packets=No
  Max Rate=14400
```

To enable Fast Start for the Annex D FAX feature:

**1** Select `Ethernet` from `Main Edit` Menu.

**2** Select `Mod Config.`

**3** Select `VOIP Options...`

**4** Select `Faststart Enable` (ensure you have selected the default [yes]).

MultiVoice gateways automatically detect other gateways of a call that are not MultiVoice gateways. Subsequently, if Fax tones are detected, this system will use the H.323 Annex D standard for Fax. MultiVoice gateways identify themselves in the `vendorIdentifier` fields of H.225 call signaling messages.

This feature implements section D.5 entitled "Replacing an existing audio stream with a T.38 fax stream" of the H.323 Annex D standard, version 4 dated November, 2000. The implementation of this feature also uses `nonStandardParameter` fields to indicate T.38 support in H.245 messages requiring an indication for T.38.

# *Additional Navis support for RTP payload information*

*Units affected: MAX 6000, MAX 3000*

## Feature definition

The RTP QoS statistics generated are obtainable periodically, through a polling parameter. RTP QoS periodic statistics (such as end-of-call statistics) are sent to the protocol (this function is not dependent upon the enabling of either RTP QoS polling or Call Logging).

Supported codecs for this feature are limited to G.711 and G.729 on a MAX. RTP QoS information passed onto the Call Logging Server is enhanced in this feature to offer a good perspective of the QoS.

The RTP QoS feature can be observed in two factions: SNMP Polling and Call Logging.

- In SNMP polling, when you activate this parameter, statistics are periodically reported.
- In call logging, call statistics are reported to Navis after each call. However, each call must remain active for at least 60 seconds in order for the statistics to be recorded.

**Note:** This feature is available only on a MAX, configured with MultiDSP 48-port (MX-SL-48M-DSP) or MultiDSP 60-port (MX-SL-60M-DSP) cards.

## User interface changes

TAOS collects information periodically during the voice call; the general information content is described in Table 13.

**Note:** The RTP statistics set, sent to the STOP packet's call logging server, is enhanced through the addition of attributes into that packet. TAOS collects periodic information during voice calls. Table 13 is a description of this QoS information content.

*Table 13. Qos Information*

| **Direction** | **LocalGW - RemoteGW** | | | **RemoteGW - LocalGW** | | |
|---|---|---|---|---|---|---|
| Info (Units) | | | | | | |
| | Sent | Lost | Late | Sent | Lost | Late |
| Packets(N) | X | X | X | X | X | X |
| Bytes (N) | X | | | | | |
| * Jitter (ms) | | X | | | X | |
| * Round-Trip Delay | Applies to both | | | | | |
| (ms) | | | | | | |
| Silence Detect (% of Packets) | | X | | | X | |

**Note:** * Maximum observed value, minimum observed value, average and standard variance are provided in the STOP packet.

The implementation of the STOP packet information generates a new mib; ASCEND-RTP-QOS-STATS-MIB. You can use this mib to extract QoS statistics for an active VoIP (RTP) call.

*Table 14. Polling MAX VoIP Profile user interface*

| **Parameter/Field** | **Specifies** |
|---|---|
| admin> list VoIP | {0 0} |
| rtpqos-polling-enable | No |
| valid range of values | Yes / No |
| Data Type | Boolean |
| Size Limits | N/A |
| Default Value | No (polling disabled) |
| When the change is effective | Immediately |
| When the field is N/A | When packet-audio-mode is not G.711 or G.729 |

## External interface changes

The Call Logging STOP Packet will contain the attributes given in the tables below.

| Option | Specifies |
|---|---|
| Ascend-Rtp-Local-Jitter-Minimum | Minimum jitter measured at local RTP receiver |
| Ascend-Rtp-Local-Jitter-Maximum | Maximum jitter measured at local RTP receiver |
| Ascend-Rtp-Local-Jitter-Mean | Average jitter measured at local RTP receiver |
| Ascend-Rtp-Local-Jitter-Variance | Variation in jitter measured at local RTP receiver |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Local-Delay-Minimum | Minimum round trip delay measured at local RTP transmitter |
| Ascend-Rtp-Local-Delay-Maximum | Maximum round trip delay measured at local RTP transmitter |
| Ascend-Rtp-Local-Delay-Mean | Average round trip delay measured at local RTP transmitter |
| Ascend-Rtp-Local-Delay-Variance | Variation in round trip delay measured at local RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Local-Packets-Sent | Total number of packets transmitted by local RTP transmitter |
| Ascend-Rtp-Local-Packets-Lost | Total number of packets failed to arrive at local RTP transmitter |
| Ascend-Rtp-Local-Packets-Late | Total number of packets arrived late at local RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Local-Silence-Sent | Total number of bytes transmitted by local RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Local-Silence-Percent | Percentage silence measured at local RTP transmitter |

The following are statistics regarding Remote RTP Transmitter and Receiver

| Option | Specifies |
|---|---|
| Ascend-Rtp-Remote-Jitter-Minimum | Minimum jitter measured at Remote RTP receiver |
| Ascend-Rtp-Remote-Jitter-Maximum | Maximum jitter measured at Remote RTP receiver |
| Ascend-Rtp-Remote-Jitter-Mean | Average jitter measured at Remote RTP receiver |
| Ascend-Rtp-Remote-Jitter-Variance | Variation in jitter measured at Remote RTP receiver |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Remote-Delay-Minimum | Minimum round trip delay measured at Remote RTP transmitter |
| Ascend-Rtp-Remote-Delay-Maximum | Maximum round trip delay measured at Remote RTP transmitter |
| Ascend-Rtp-Remote-Delay-Mean | Average round trip delay measured at Remote RTP transmitter |
| Ascend-Rtp-Remote-Delay-Variance | Variation in round trip delay measured at Remote RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Remote-Packets-Sent | Total number of packets transmitted by Remote RTP transmitter |
| Ascend-Rtp-Remote-Packets-Lost | Total number of packets failed to arrive at Local RTP transmitter |
| Ascend-Rtp-Remote-Packets-Late | Total number of packets arrived late at Local RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Remote-Silence-Sent | Total number of bytes transmitted by Remote RTP transmitter |

| Option | Specifies |
|---|---|
| Ascend-Rtp-Remote-Silence-Percent | Percentage silence measured at Remote RTP transmitter |

# Known issues

## *MAX data issues*

Known issues you should be aware of before loading release 9.1.0 include the following:

- TAOS 9.1.0 for MAX does not support AppleTalk. Do not upgrade to TAOS 9.1.0 if your network requirements include support for AppleTalk.
- After you upgrade a MAX unit from the TAOS 8.0-110 Limited Availability Release to TAOS 9.1.0, you must re-enter 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.
- Change in Call-logging packet format

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

  Because of the proprietary nature of and potential modification to call-logging packets, you should not use call-logging packets with any application other than Lucent Technologies' NavisAccess.
- Some multimedia features are not supported in this release. Customers using the following features should not upgrade to 9.1.0:
  - 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 this release is loaded.
- In MAX units, data flows between T1/E1 WAN ports and host devices such as modems and HDLC ports using a limited group of internal data pathways. The capacity of these pathways is sufficient to accommodate the built-in WAN ports of the MAX. When BRI cards are installed in the system, pathways normally allocated for built-in T1/E1 ports are used to support the BRI WAN ports, and are not available for T1/E1 usage.

Table 15 summarizes how the addition of BRI cards affects the availability of built-in WAN ports in various MAX units. These limits apply regardless of the type of BRI card used (Net, Host, IDSL, etc.).

*Table 15.WAN ports available when BRI cards are in use*

| Model | Number of BRI cards | WAN ports available |
|---|---|---|
| MAX 6000 | 0 | 1, 2, 3, 4 |
| | 1 | 1, 2, 3 |
| | 2, 3 | 1, 2 |
| | 4, 5, 6 | Unsupported |

# MultiDSP module issues

Issues you should be aware of before installing the MultiDSP module include the following:

- In an E1 environment, the MultiDSP module can exhibit a lower-than-expected call connect 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.
- The MultiDSP module does not currently support any version of Personal Handyphone System (PHS), V.110, or High-Level Data Link Control (HDLC).

# MultiVoice issues for the MAX 3000

Known issues you should be aware of before loading release 9.1.0 include the following:

MultiVoice issues for the MAX 3000 you should be aware of before loading release 9.1.0 include the following:

- MultiDSP slot card

  For the 9.1.0 release, you must use a MultiDSP slot card (MX-SL-48M-DSP or MX-SL-60M-DSP) in the MAX 3000 chassis.

- CAS Signaling Not Supported

  Channel Associated Signaling (CAS), is not supported on the MAX 3000. Only ISDN-PRI signaling is supported.

- Audio codec support

  On the MAX 3000, when using the G.711 audio codec, only 1 T1 PRI or 1 E1 PRI interface can be used, and the Frames Per Packet parameter in the Voip profile must be set to 6 or higher. When using the G.729(A) audio codec, 2 T1 PRI or 2 E1 PRI interfaces can be used, and the Frames Per Packet parameter must be set to 2 or higher.

- Voice announcements

  A MAX 3000 can only support the standard set of voice announcement files that are downloadable from a TFTP server. Break-in announcements, arbitrary announcements, multiple languages, and the branding of voice announcements are not supported.

# MultiVoice issues for the MAX 6000

Known issues you should be aware of before loading release 9.1.0 include the following:

- VDSP cards

  For the 9.1.0 release, you must use a MultiDSP slot card (MX-SL-48M-DSP or MX-SL-60M-DSP) in the MAX 6000 chassis. Older VDSP cards (MXV-SL-DSP8, MXV-SL-DSP12, MXV-SL-DSP16) are not supported in this release. Support for the VDSP cards is planned for a subsequent 9.1.x release.

- Voice announcements

  The MAX 6000 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 MAX 6000.

- Maximum configuration

  The maximum supported configuration for the MAX 6000 is 2 T1 PRI or 2 E1 PRI interfaces, 48 or 60 calls respectively.

- MAX

  If you have MAX(s) in your MAX 6000 unit, and at least one card is configured to support MultiVoice using simple audio codecs (e.g., G.711), then all VoIP calls will be restricted to use simple audio codecs as well.

- Audio codec support

  On the MAX 6000, when using the G.729(A) audio codec, 2 T1 or 2 E1 PRI interfaces can be used, and the Frames Per Packet parameter in the Voip profile must be set to 2 or higher.When a MultiDSP card is used with the G.711 audio codec, you must set the Frames-Per-Packet parameter in the Voip profile to a value of 4 or more.