Lucent Technologies
Bell Labs Innovations



TAOS 10.1.0 Release Note

for APX®and MAX TNT® Universal Gateways

For software version 10.1.0
March 25, 2003

Copyright © 2003 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.

For latest information, refer to online product documentation at www.lucent.com/support.

European Community (EC) RTTE compliance

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

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

Safety, compliance, and warranty information

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

Security statement

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

Trademarks

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

Ordering information

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

Feedback

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

Lucent Technologies

Customer Service

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

Finding information and software

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

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

Obtaining technical assistance

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Contents

Customer Service iii

Section 1 Upgrading and Downgrading 1-1

Boot-loader and tar files in TAOS 10.1.0 1-1
Before you begin upgrading 1-2
Upgrading an APX 8000 unit 1-3
Upgrading an APX 1000 or MAX TNT unit 1-3
Special upgrade situations in TAOS 10.1.0 1-4
Downgrading to a previous software release 1-5

Section 2 Welcome to TAOS 10.1.0 2-1

TAOS 10.1.0 software license requirements 2-1
How to use this release note 2-2
Feature request numbers 2-2
Firmware in TAOS 10.1.0 2-3

Section 3 Features in TAOS 10.1.0 3-1

MultiDSP features 3-1
V.92 PCM upstream 3-1
SDTN on MultiDSP cards 3-3
Basic and extended use of AT commands 3-4

Call processing features 3-10
Control of initial carriage return (CR) in terminal sessions 3-10
Support for PPP Extensible Authentication Protocol (EAP) calls 3-11
Disabling end-point discrimination for PPP sessions 3-12
Magic number negotiation during Link Control Protocol (LCP) setup 3-12
Configuring LCP/NCP timeout 3-13
Configurable egress packet flow 3-14
Configurable idle pattern for all channels of T1 3-15

Call routing features 3-16
Supported call-route types 3-16
Overview of the call routing algorithm 3-18
Deactivating a call route 3-19
Sort methods to distribute calls efficiently 3-20
Best-match requirement in selecting devices 3-20
New cost allocations for priority-based call routing 3-22
New call routing administrative capabilities 3-24

APX 8000 redundancy features 3-30
Redundancy support for various call types 3-30
Redundancy health monitoring 3-31
BITS interface support for APX 8000 platforms 3-33

Routing and traffic management features 3-39
ATM virtual path shaping 3-39
Virtual routers now able to route multicast traffic 3-44
Support for IGMPv3 3-47
Modifications to BGP rules for BGP summarization policies 3-52
New range for RIP triggered update delay 3-57

Tunneling features 3-57
Session idle timer enhancements for layer 2 tunneling 3-57
Configurable L2TP hello packet policy 3-61
New L2TP diagnostic commands 3-62
New L2TP attribute-value pairs 3-63
V.92 MOH signaling over L2TP 3-64
Configurable sending of LCP Configure Request message 3-64
Disabling IP-in-IP decapsulation 3-65

System administration features 3-65
Secure shell (**ssh**) for administrative access 3-65
Group permissions 3-68
New options to the `userstat` command 3-73
Displaying T1 or E1 performance monitoring statistics 3-73
Support for the `who` command 3-74
Administering Primary Rate Interface (PRI) layer 2 timers 3-76
Specifying whether to log L2TP `syslog` messages 3-76
Fatal index 388 introduced and fatal index 66 discontinued 3-77
Modifications to the `slrt` and `netstat` commands 3-77
New `boot-version` profile 3-78
Time zone information without using SNTP 3-79
Disabling the proprietary `afind` protocol 3-80
The `-t` option of `arptable` command removed 3-81
Permission-level change for **`device`** command 3-82
New command to display system information 3-82

RADIUS features 3-83
RADIUS and call logging support for V.92 3-83
RADIUS support for configurable AT answer string 3-85
Dynamic banner and login prompt 3-85
Configurable resending of the Accounting Event packet 3-86

SNMP features 3-87
SNMP support for V.92 3-87
Support for alarm MIBs 3-88
SNMP MIB load order 3-92
Enhancements to the `snmpMgrStats` command 3-95
New `SNMP admin-state-modem-if` profile for modem cards 3-96
Destructive `snmpset` commands disabled on the secondary controller 3-98

Signaling System 7 (SS7) features 3-100
Conversion of **`ss7-gateway`** to **`media-gateway`** settings 3-100

Support for multiple media gateway controllers 3-102
CLID Presentation Indicator support for IPDC 3-111

MultiVoice® features 3-115
Simultaneous single-stage dialing VoIP and modem calls 3-115
ISDN cause code verification 3-116
New features for G.723.1 and G.728 codecs 3-116
Special trunk group for hairpin calls 3-120
Enhanced speech transmission for VoIP G.711 codec 3-120
Configuring frames per packet for each codec 3-121
MultiVoice® control of trunk gain and loss 3-122
Echo cancellation support for all audio codecs 3-124
Enhanced MultiDSP support for G.723 3-124
Silence suppression and adaptive jitter buffer 3-125
E1 R2 cause codes enhancement 3-125
Silence suppression for G.728 codec 3-127
Calling Line Identification (CLID) indicator enhancement 3-128
IP Device Control support for Voice over IP tones 3-130
Including the NSF information element in Q.931 setup messages 3-136
Handling of rogue RTP streams 3-138
DTMF events RTP payload set dynamically via IPDC 3-140
Configuring two-stage dialing in SS7 networks 3-141
New IPDC feature support 3-142

Section 4 Change Requests in TAOS 10.1.0 4-1

Section 5 Notices, Known Issues, and Limitations 5-1

Notice in TAOS 10.1.0 5-1
Known issues and limitations in TAOS 10.1.0 5-2

Upgrading and Downgrading 1

Boot-loader and tar files in TAOS 10.1.0 1-1
Before you begin upgrading 1-2
Upgrading an APX 8000 unit 1-3
Upgrading an APX 1000 or MAX TNT unit 1-3
Special upgrade situations in TAOS 10.1.0. 1-4
Downgrading to a previous software release 1-5

Read the following instructions carefully before upgrading your system to True Access™ Operating System (TAOS) 10.1.0, or downgrading to a previous release.

Be aware of notices and known issues described in "Notices, Known Issues, and Limitations" on page 5-1.

If you need assistance with obtaining the TAOS 10.1.0 software, see "Customer Service" on page iii.

Boot-loader and tar files in TAOS 10.1.0

Table 1-1 lists the boot-loader files and tar files that you use to upgrade your unit to TAOS 10.1.0.

Table 1-1. Boot-loader and tar files in TAOS 10.1.0

APX 8000 files	APX1000 files	MAX TNT files	Description
`apxsrb.bin`	`apx1ksrb.bin`	`tntsrb.bin`	The boot loader. Both T1 and E1 loads use the same boot loader software.
`apxrel.tar` and `apxrel2.tar`	`apx1krel.tar`	`tntrel.tar` and `tntrel2.tar`	Tar files (T1 load). Contain images for the shelf controller and all T1-compatible slot cards.
`apxrele.tar` and `apxrele2.tar`	`apx1krele.tar`	`tntrele.tar` and `tntrele2.tar`	Tar files (E1 load). Contain images for the shelf controller and all E1-compatible slot cards.

Before you begin upgrading

The following recommended tasks help ensure a smooth upgrade process.

Verify that you have local access to the unit

Whenever you install system software, Lucent recommends that you access the unit through the shelf controller serial or LAN port rather than a slot card port.

Save the system configuration

As a general practice, save the system configuration before upgrading or downgrading system software. If you use TFTP to save the system configuration, the target file must exist on the TFTP server and you must have permission to write it. For example, the following commands executed on a TFTP server create a target file and set its permissions:

```
$ touch /tftpboot/config/testcfg.1
$ chmod a=rw /tftpboot/config/testcfg.1
```

Before you save the system configuration, you must enable the `allow-password` permission in the `user` profile to save the configured passwords. If you do not have `allow-password` permission enabled, you will be prompted to confirm that you wish to save the configuration without passwords. If you do so and then restore the saved configuration, all passwords in the configuration are wiped out. The following commands executed on the APX 8000 unit save the system's configuration to the target file on the TFTP server and then restore the saved configuration:

```
admin> save network 10.10.10.10 config/testcfg.1
admin> load config network 10.10.10.10 config/testcfg.1
```

For additional information about the `save` command and its options, see the *APX/MAX TNT Reference*.

Verify that the `load-select` profile is properly configured

TAOS includes a `load-select` profile that prevents the system from loading the entire set of slot card images. The `load-select` profile causes the system to determine which card types are present, load only those images, and delete all images in the flash card that were not selected in the `load-select` profile.

Verify that the `load-select` profile is configured to either automatically load only required or selected binaries. For more information about using the `load-select` profile, see the *APX/MAX TNT Administration Guide*.

Format the flash card(s)

Loading the new tar file during the upgrade procedure should delete any unnecessary images in the flash card(s). In cases of some unexpected error, however, the flash card(s) sometimes retain unwanted images from the previous release. You can optionally format the flash card(s) before the upgrading system software to ensure that any unwanted image has been removed.

The system flash card(s) might contain voice announcement files and slot card coredump files. Save those files to another location before formatting the unit's flash card(s).

Upgrading an APX 8000 unit

On a dual-controller system, if you are logged into the primary controller, the `load` and `reset` commands in the following procedure affect both controllers.

To upgrade a single-controller or dual-controller APX 8000 unit, proceed as follows:

1 Log into the hard IP address of the primary shelf controller. Do not use the soft IP address. To obtain IP address of the primary shelf controller, use the `dir ip-interface` command.

2 Load the boot loader. For example:

```
admin> load boot-sr network 10.10.10.10 apxsrb.binaries/apxsrb.bin
```

3 Load the tar file(s).

```
admin> load tar network 10.10.10.10 apxrel.tar apxrel2.tar
```

If the `load tar` command recognizes no slot cards and loads only the shelf controller image, reset system and load the tar files again. Entering the `load tar` command for a second time should load the appropriate slot card images for the system. To verify that images for all installed slot cards are present on the flash card(s), enter the `ls` command on both the primary and secondary controllers.

4 Restore system configuration. (Optional.)

5 Reset the system.

For example:

```
admin> reset
```

The `reset` command on the primary controller resets both controllers, dropping all calls.

Upgrading an APX 1000 or MAX TNT unit

Use the following instructions to upgrade to TAOS 10.1.0 from TAOS 9.0.*x* and later releases. To upgrade an APX 1000 or MAX TNT unit, proceed as follows:

1 Format the flash card (optional).

For example:

```
admin> format flash-card-1
```

2 Load the boot loader.

For example:

```
admin> load boot-sr network 10.10.10.10 tntsrb.bin
```

3 Load the tar file(s).

```
admin> load tar network 10.10.10.10 tntrel.tar tntrel2.tar
```

4 Reset the system. This step is required to set the name of the TAOS unit.

```
admin> reset
```

Special upgrade situations in TAOS 10.1.0

Be aware of the following situations that might exist for your system after upgrading the system software to TAOS 10.1.0.

Migration for the `ss7-gateway` profile in TAOS 10.1.0

When you upgrade to TAOS 10.1.0, all Internet Protocol Device Control (IPDC), Access SS7 Gateway Control Protocol (ASGCP), and Q.931+ configuration information contained in an `ss7-gateway` profile is converted and migrated to the new `media-gateway` profile. (See "Conversion of ss7-gateway to media-gateway settings" on page 3-100 for more information.)

If you load saved configuration that includes settings from an `ss7-gateway` profile onto a TAOS unit running TAOS 10.1.0, the `ss7-gateway` parameters are also converted and placed into the new `media-gateway` profile.

The index of a converted `media-gateway` profile is `default`. With this default index, T1 and E1 lines can to continue to provide service after an upgrade.

After upgrade, any existing `ss7-gateway` profile found in NVRAM upon startup is converted into a `media-gateway` profile and the following message is logged with the log-level warning upon the system startup:

```
LOG warning, Shelf 1, Controller, Time: 16:30:08--
  Profile conversion: SS7-GATEWAY is now MEDIA-GATEWAY ""
```

Enabling the system to recognize cost assignments from an earlier release

If you are upgrading from software version TAOS 10.0.0 and later releases and you have assigned non-default `cost` values in your `call-route` profiles, your `cost` assignments are not be taken into account following the upgrade unless you switch to `manual-enabled` mode, as shown in the following set of commands:

```
admin> read system
SYSTEM read

admin> set least-cost-call-routing = manual-enabled

admin> write -f
SYSTEM written
```

If you have not customized `cost` values in your `call-route` profiles, the default `auto-enabled` mode allows the call routing algorithm to automatically select the least cost destination for processing a call.

Recommendations for restoring call-routing configurations

After a reset or clear of NVRAM, the system automatically repairs the call-routing configuration, ensures that it handles all supported call-route types, and assigns priorities for efficient use of resources. For this reason, if you have not customized your `call-route` profiles, it is best not to save and restore older system-generated default profiles. To save the system configuration without saving the `call-route` profiles, use the `-x` option of the `save` command. For example:

```
admin> save network 10.10.10.10 file.cfg -x call-route
```

If you have customized your `call-route` profiles and you wish to restore them, consider the following:

- If you restore from an earlier software version, the restored profiles will not take into account additional software licenses or new supported call-route types.
- If you restore following a `reset`, you could create duplicate `call-route` profiles for the same `call-route-type` to the same slot card. Duplicate profiles can be confusing, but they do not cause a problem to the call routing algorithms.

You can repair `call-route` profiles by using one of the new administrative capabilities for repairing the call routing configuration (see "New call routing administrative capabilities"), or by resetting the system.

Downgrading to a previous software release

Releases are not necessarily backward compatible. Lucent recommends that you restore a backup configuration made under the previous version. The following procedures restore a previous software version (TAOS 9.0.*x*, 9.1.*x*, 10.0.*x*) to your unit. To downgrade, you must have serial access to the TAOS unit.

Downgrading an APX 8000 unit

To restore a previous software version on your APX 8000 unit, proceed as follows.

1 Load the previous version of the boot loader.

For example:

```
admin> load boot-sr network 10.10.10.10 apxsrb.bin
```

2 Format the flash cards of both the primary and the secondary controller.

For example:

```
admin> format flash-card-1
```

3 Load the previous version of the tar file (via TFTP from a local host).

– If you are downgrading to a TAOS version prior to version TAOS 10.0.*x*, enter the following command:

```
admin> load tar network 10.10.10.10 apxrel.tar
```

– If you are downgrading to TAOS version TAOS 10.0.*x*, enter the following command:

```
admin> load tar network 10.10.10.10 apxrel.tar apxrel2.tar
```

4 Clear all profiles by entering the `nvram` command, for example:

```
admin> nvram
```

5 Set the primary shelf controller IP address.

Log into the primary shelf controller via the serial connection. Open the `ip-interface` profile for the shelf controller and set the IP address. For example:

```
admin> read ip-interface {{1 right-controller 1} 0}
IP-INTERFACE/{{shelf-1 right-controller 1} 0} read

admin> set ip-address = 10.10.10.2/24

admin> write
IP-INTERFACE/{{shelf-1 right-controller 1} 0} written
```

6 Load a backup configuration made under the restored software version or one of its predecessors.

For example:

```
admin> load config network 10.10.10.10 config/backup-config
```

7 Reset the system as follows:

For example:

```
admin> reset
```

Downgrading an APX 1000 or MAX TNT unit

To restore a previous software version (TAOS 9.0.x, TAOS 9.1.x, or TAOS 10.0.x) on your APX 1000 or MAX TNT unit, proceed as follows:

1 Format the flash card.

For example:

```
admin> format flash-card-1
```

2 Load the previous version of the boot loader.

For example:

```
admin> load boot-sr network 10.10.10.10 tntsrb.bin
```

3 Load the previous version of the tar file.

– If you are downgrading to a TAOS version prior to TAOS 9.0, enter the following command:

```
admin> load tar network 10.10.10.10 tntrel.tar
```

– If you are downgrading to a TAOS 9.0 and later releases, enter the following command:

```
admin> load tar network tntrel.tar tntrel2.tar
```

4 Clear all profiles by entering the `nvram` command.

For example:

```
admin> nvram
```

5 Log into the system via the serial connection. Open the `ip-interface` profile for the shelf controller and set the address.

For example:

```
admin> read ip-interface {{1 controller 1} 0}
IP-INTERFACE/{{shelf-1 controller 1} 0} read

admin> set ip-address = 10.10.10.2/24

admin> write
IP-INTERFACE/{{shelf-1 controller 1} 0} written
```

6 Load a backup configuration made under the restored software version or one of its predecessors.

For example:

```
admin> load config network 10.10.10.10 config/801-config
```

7 Reset the system. This step is required.

For example:

```
admin> reset
```

Welcome to TAOS 10.1.0

2

TAOS 10.1.0 software license requirements 2-1

How to use this release note 2-2

Feature request numbers 2-2

Firmware in TAOS 10.1.0. 2-3

The True Access™ Operating System (TAOS) 10.1.0 introduces new features and software enhancements for the following units:

- APX 8000
- APX 1000
- MAX TNT
- MAX 6000

This release note describes new features and software enhancements introduced in TAOS 10.1.0 for APX 8000, APX 1000, and MAX TNT units.

For information about MAX 6000 units, the TAOS 10.1.0 release note for the MAX 6000 at `http://www.lucent.com/support`.

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

Caution Before installing or operating your TAOS unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see the "Safety-Related Electrical, Physical, and Environmental Information" appendix in your unit's *Getting Started Guide*.

TAOS 10.1.0 software license requirements

TAOS 10.1.0 includes built-in software features for WAN access environments, as well as optional extensions that require separate licensing or qualifying contracts to support a wide variety of WAN access environments.

In addition, certain major features in TAOS 10.1.0 are available only with the purchase of the TAOS 10.1 Premium Feature Set software license enabled.

Contact your Lucent sales representative if you have any questions about feature licensing for your system.

The TAOS 10.1 Premium Feature Set is enabled for your unit if the `feature-10-1-enabled` parameter is set to `yes` in the `base` profile, as in the following example:

```
admin> get base feature-10-1-enabled
[in BASE:feature-10-1-enabled ]
feature-10-1-enabled = yes
```

The following features require the 10.1 Premium Feature Set software license:

- "V.92 PCM upstream" on page 3-1
- "V.92 MOH signaling over L2TP" on page 3-64
- "Support for PPP Extensible Authentication Protocol (EAP) calls" on page 3-11
- "Secure shell (ssh) for administrative access" on page 3-65
- "Group permissions" on page 3-68
- "RADIUS support for configurable AT answer string" on page 3-85

How to use this release note

The table of contents on page v lists the features in this release. If you are reading this release note in PDF format, you can click the feature name to go directly to the description.

You can also search for a feature by feature ID number using Table 2-1 "TAOS 10.1.0 features with feature request numbers" on page 2-2.

Feature request numbers

Table 2-1 lists the features in TAOS 10.1.0 that are identified by a feature request number.

Table 2-1. TAOS 10.1.0 features with feature request numbers

Feature request ID	Description
260803	Support for multiple media gateway controllers
261211	Administering Primary Rate Interface (PRI) layer 2 timers
261218	MultiVoice® control of trunk gain and loss
261208	Silence suppression for G.728 codec
261209	Echo cancellation support for all audio codecs
261240	Displaying T1 or E1 performance monitoring statistics
261451	Redundancy support for various call types
261515	Handling of rogue RTP streams

Table 2-1. TAOS 10.1.0 features with feature request numbers

Feature request ID	Description
261547	Support for the `who` command
261547	Group permissions
261602	DTMF events RTP payload set dynamically via IPDC
261615	Special trunk group for hairpin calls
510175	Virtual routers now able to route multicast traffic
510274	Disabling end-point discrimination for PPP sessions
510538	Calling Line Identification (CLID) indicator enhancement
510590	SDTN on MultiDSP cards
510653	Configuring frames per packet for each codec
510708 510710	New L2TP attribute-value pairs
510728	Configuring LCP/NCP timeout
510791	Magic number negotiation during Link Control Protocol (LCP) setup
510794	CLID Presentation Indicator support for IPDC
510814 261805 261806 261807	Dynamic banner and login prompt
510816	Configurable L2TP hello packet policy
510820	Session idle timer enhancements for layer 2 tunneling

Firmware in TAOS 10.1.0

Following are the firmware versions for TAOS devices in this release.

Firmware versions for digital modem cards

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

- Series56 II Digital Modem (CSM/3, TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C)—V5.817
- Series56 III Digital Modem (CSMV/3, TNT-SL-48MODV3-S-C)—V5.8175

Firmware versions for MultiDSP slot cards

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

- Controller—V0.2.21
- PHS—V2.1.1
- Modem—V0.2011.0
- VoIP—V4.0.35
- V.110—V0.0.3
- WORM—V0.0.3

Features in TAOS 10.1.0

3

MultiDSP features 3-1
Call processing features 3-10
Call routing features. 3-16
APX 8000 redundancy features 3-30
Routing and traffic management features 3-39
Tunneling features 3-57
System administration features 3-65
RADIUS features 3-83
SNMP features 3-87
Signaling System 7 (SS7) features 3-100
MultiVoice® features 3-115

MultiDSP features

With this software version, MultiDSP cards support additional call features that include V.92 Pulse Code Modulation (PCM) upstream and support for Short Duration Transaction Network (SDTN). In addition, they support a more flexible way of specifying modulation selection in a modem AT string.

This software version also provides RADIUS, Navis® call logging, and SNMP support for V.92 modulation. For details, see the sections on RADIUS and SNMP features later in this release note.

V.92 PCM upstream

The ITU Recommendation for V.92 specifies the following features:

- An increase in the data rate towards the network to a theoretical maximum of 48Kbps (PCM upstream)
- Significantly quicker start-up times on recognized connections (quick-connect)

- The ability to put the modem on hold when the network indicates that an incoming call is waiting (modem-on-hold)

V.92 modem-on-hold (MoH) and quick-connect features were introduced in earlier TAOS versions, and are described in the MultiDSP chapter of the *Physical Interface Guide* for your platform. This release introduces support for the V.92 PCM upstream (PCMU) feature, as well as SNMP and RADIUS support for configuration of all V.92 modem features.

Licensing for V.92 PCMU

V.92 modulation and the modem-on-hold and quick-connect features are supported in earlier TAOS software versions. To enable PCMU, introduced in TAOS 10.1, the system also requires the Premium Feature Set 10.1 software license. The following command verifies that the Premium Feature Set 10.1 license has been enabled in the system:

```
admin> get base feature
[in BASE:feature-10-1-enabled]
feature-10-1-enabled = yes
```

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

Enabling V.92 PCMU

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

```
[in TERMINAL-SERVER:modem-configuration]
modem-mod = v90-modulation
max-v92-receive-baud-rate = 48000-max-v92-baud
```

The `modem-mod` parameter sets the modulation protocol to be attempted by the modems during connection negotiation. When this is set to `v92-modulation`, the `max-v92-receive-baud-rate` parameter determines the maximum upstream (receive) baud rate to be negotiated by the modems. By default, it is set to 48000, which is the fastest rate specified in the ITU standard.

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

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set modem modem-mod = v92-modulation

admin> write -f
TERMINAL-SERVER written
```

The next commands limit the systemwide maximum negotiable upstream speed to 44Kbps:

```
admin> set modem max-v92-receive-baud-rate = 44000-max-v92-baud

admin> write -f
TERMINAL-SERVER written
```

Using an AT string to specify a connection's maximum upstream rate

You can use the AT+MS command to specify a maximum upstream (receive) rate in the individual connection or RADIUS profile for a modem call. For details about using this command, see "Extended AT+MS modulation settings" on page 3-7.

For example, the following AT+MS command in a connection profile limits the receive rate to a maximum of 36.0Kbps, and specifies a maximum transmit rate of 52Kbps:

```
admin> read connection client-modem-1
CONNECTION/client-modem-1 read

admin> set at-string = +MS=13,1,24000,36000,0,0,52000

admin> write -f
CONNECTION/client-modem-1 written
```

SDTN on MultiDSP cards

TAOS supports interaction with transaction servers to conduct short-duration transactions over IP-based networks. In previous versions, short duration transaction network (SDTN) was supported on Series II/III digital modem cards. With the current software version, SDTN is also supported on the following MultiDSP cards:

- 48-port model (TNTV-SL-ADI-C)
- 96-port model (APX8-SL-96DSP)
- 240-port model (APX-SL-DSP-3-L)
- 288-port model (APX-SL-DSP-3)

Licensing for SDTN on MultiDSP

SDTN is a feature protected by a special software license. The related parameters might be visible in the command-line interface but are not enabled unless the appropriate software license has been purchased from Lucent Technologies. You can verify that the SDTN license is enabled in your base profile by entering the following command:

```
admin> get base sdtn-enabled
[in BASE:sdtn-enabled]
sdtn-enabled = enabled
```

Configuring SDTN

You configure SDTN for calls terminated on MultiDSP cards by using the same settings described in earlier releases for SDTN calls on modem cards.

For details about configuring SDTN, see the *APX/MAX TNT WAN, Routing, and Tunneling Guide*.

Using AT strings to minimize connect times

The MultiDSP digital-signal processing (DSP) technology provides high performance and supports modulation schemes to achieve fast modem training time, which makes the MultiDSP card ideal for terminating SDTN transactions.

To enable dial-in terminals for transaction processing to connect quickly with as little modem training as possible, you can specify an AT string that sets the required modem timings, modulation types, speed, and other modem parameters. This customization reduces the modem training time prior to establishing the session. For details about settings that enable the cards to fine-tune modulation schemes to minimize training time, see "Extended AT+MS modulation settings" on page 3-7.

To support SDTN, MultiDSP cards now support V.22 and V.22bis data rates in both synchronous and asynchronous modes, with special variants of V.25 auto-answering aimed at minimizing connection times on delay-sensitive transaction services. For details about specifying an AT string to use these variants, see "Special variants of V.22 and V.22bis" on page 3-8.

Basic and extended use of AT commands

When a modem initiates a call to the system, the MultiDSP card is initialized with AT commands that are used to program data rate, compression, and other possible settings while the connection is being established. The two systems negotiate, based on these AT command settings, until the parameters of the call have been established, and then the session can begin.

How to specify an AT string

You can specify the AT commands sent by the MultiDSP card in a systemwide setting, which is used as the default AT string for modem calls, or in the individual `connection` or RADIUS profile for the remote unit. Settings in a `connection` or RADIUS profile always override the general systemwide AT commands.



Note Be very careful when entering AT commands. The system does not prevent you from entering incorrect strings.

Setting a systemwide AT answer string

Following is the systemwide parameter, shown with default setting, for specifying AT commands:

```
[in TERMINAL-SERVER:modem-configuration]
at-answer-string = ""
```

The value of this parameter can be set to valid AT commands of up to 36 characters. Do not begin the string with `AT`. The system adds `AT` to the beginning of the string automatically before sending it to the modem. Also, do not include an `A` (answer) or a `D` (dial) command anywhere in the string.

The following example enters the AT command `S37=11`, which causes the following string to be sent to the modem:

```
ATS37=11A
```

When the modem receives this string, it negotiates a V.32bis 14400 baud connection.

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set modem at-answer-string = S37=11

admin> write -f
TERMINAL-SERVER written
```

Setting a connection-specific AT string

Following is the connection-specific parameter, shown with default setting, for specifying AT commands:

```
[in CONNECTION/""]
at-string = ""
```

The value of this parameter can be set to valid AT commands of up to 58 characters. Do not begin the string with AT. The system adds AT to the beginning of the string automatically before sending it to the modem. Also, do not include an A (answer) or a D (dial) command anywhere in the string.



Note With this software version, you can also specify an AT string in a RADIUS user profile. For details, see the section "RADIUS support for configurable AT answer string" later in this release note.

The following example enters the \N5%C1 command, which causes the system to send the following AT string to the initiating modem for this connection:

```
AT\N5%C1A
```

This command specifies Microcom Network Protocol Class 5 (MNP5) data compression and error correction only. If the client modem is unable to negotiate the desired rate mode, the modem disconnects and responds with a No Carrier message.

```
admin> read connection M1
CONNECTION/M1 read

admin> set at-string = \N5%C1

admin> write -f
CONNECTION/M1 written
```

Table of commonly used AT commands

Table 3-1 shows the commonly used AT commands for MultiDSP calls:

Table 3-1. commonly used AT commands for MultiDSP calls

Command	Definition
AT	(Attention modem.) Command mode prefix.
S*n*=*v*	(Set the value (*v*) of the specified S-register.) For example, the following command sets the value of S47 to 20: ATS47=20
&G	(Generate guard tone.) See "Special variants of V.22 and V.22bis" on page 3-8.
&T	Test and diagnostics. See "Special variants of V.22 and V.22bis" on page 3-8.

Table 3-1. commonly used AT commands for MultiDSP calls

Command	Definition	
%C*n*	(Compression) Specifies the data compression the MultiDSP card negotiates on an error-corrected link. The value of *n* can be one of the following:	
	0	Do not negotiate data compression.
	1	Negotiate MNP5 data compression.
	2	Negotiate V.42bis data compression.
	3	Negotiate both V.42bis and MNP5 data compression.
\N*n*	(Operating mode.) Specifies the error correction mode to negotiate.	
	0	Negotiate normal speed buffered mode. (Do not attempt error-correction mode.)
	2	Negotiate reliable error-correction mode. The modem first attempts a Link Access Protocol for Modems (LAPM) connection and then an MNP connection. Failure to establish a reliable connection results in a hang-up.
	3	Negotiate auto reliable mode. The modem first attempts a LAPM connection and then an MNP connection. Failure to establish a reliable connection results in the modem falling back to the speed buffered normal mode.
	4	Negotiate LAPM error-correction mode. Failure to make an LAPM error-correction connection results in a hang-up.
	5	Negotiate MNP error-correction mode. Failure to make an MNP error-correction connection results in a hang-up.
+A8E=0,0,00,*n*,0,0	Enable or disable K56flex operation by enabling or disabling V.8bis negotiation. The value of *n* (0 or 1) must be positioned in the string as shown. For example, the following command disables K56flex: +A8E=0,0,00,0,0,0 and the following command enables K56flex: +A8E=0,0,00,1,0,0	
	0	Disable V.8bis (K56flex) negotiation.
	1	Enable V.8bis (K56flex) negotiation. (This is the default behavior.)
+MS	Select modulation settings. The MultiDSP card supports an extended format of this command that can specify modulation, enable or disable automode, and the lowest and highest connection rates. See "Extended AT+MS modulation settings" on page 3-7.	

Extended AT+MS modulation settings

When a modem initiates a call, the system must train the modem to a specific data rate before establishing the connection. For short-duration transactions, which must be established as quickly as possible, you can reduce the modem training time by specifying an AT string that sets the required modem parameters.

The MultiDSP cards support an extended format of the +MS (select modulation) generic AT command that can specify a supported modulation, enable or disable automode, and specify the lowest and highest connection rates. The extended format for most modulations uses the following syntax:

+MS=*mod*[,*automode*][,*min_rx_rate*][,*max_rx_rate*][,*x_law*] [,0][,*max_tx_rate*]

In this syntax,

- *mod* specifies a number that represents a supported modulation (see Table 3-2).
- *automode* disables (0)or enables (1) automode. When enabled, automode allows modulations lower than the one specified in the +MS string. When automode is disabled, the server modem will try to connect only in the particular modulation specified.
- *min_rx_rate* specifies a minimum receive (upstream) data rate (see Table 3-2).
- *max_rx_rate* specifies a maximum receive (upstream) data rate (see Table 3-2).
- *x_law* disables (0) or enables (1) A-law compression and expansion encoding.
- *max_tx_rate* specifies a maximum transmit (downstream) data rate (see Table 3-2).

For example, the following commands specify V.90 modulation with automode enabled, receive rates from 300bps to 21,600bps, and a maximum transmit rate of 49,333bps.

```
admin> read connection client-1
CONNECTION/client-1 read

admin> set at-string = +MS=12,1,300,21600,0,0,49333

admin> write -f
CONNECTION/client-1 written
```

The following commands specify V.92 modulation with automode enabled, and limit data rates by setting receive rates from 24,000 to 48,000bps, and a maximum transmit rate of 52,000bps.

```
admin> read connection client-2
CONNECTION/client-2 read

admin> set at-string = +MS=13,1,24000,48000,0,0,52000

admin> write -f
CONNECTION/client-2 written
```

Table 3-2 shows the possible rates for the various modulations.

Table 3-2. Data rates for modulations in the extended +MS command (page 1 of 2)

mod	Modulation	Possible Rates (bps)	Notes
0	V.21	300	None

Table 3-2. Data rates for modulations in the extended +MS command (page 2 of 2)

mod	Modulation	Possible Rates (bps)	Notes
1	V.22	1200	When V.22 or V.22bis is in use, you can specify values for S-registers to use variants for fast training. (See Table 3-3.)
2	V.22bis	2400 or 1200	
3	V.23	1200	V.23 originating mode transmits at 75 bps and receives at 1200bps and the answering mode transmits at 1200bps and receives at 75bps.
9	V.32	9600 or 4800	None
10	V.32bis	14400, 12000, 9600, 7200, or 4800	None
11	V.34	33600, 31200, 28800, 26400, 24000, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, or 2400	The possible upstream data rates are the same as the downstream data rates of V.34.
12	V.90	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 44000, 42667, 41333, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000	These rates are the possible downstream data rates. V.90 upstream rates are the same as the downstream data rates of V.34.
13	V.92	48000, 46667, 45333, 44000, 42667, 41333, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000, 26667, 25333, 24000	These rates are the possible upstream data rates. V.92 downstream rates are the same as the downstream data rates of V.90.
56	K56Flex (2,3)	56000, 54000, 52000, 50000, 48000, 46000, 44000, 42000, 40000, 38000, 36000, 34000, 32000.	None

Special variants of V.22 and V.22bis

To support SDTN, MultiDSP cards now support V.22 and V.22bis data rates in both synchronous and asynchronous modes, with special variants of V.25 auto-answering aimed at minimizing connection times on delay-sensitive transaction services. The modem operates in accordance with ITU-T V.22/V.22bis and is also able to operate with variations from the normal CCITT figures.

To enable digital loopback acknowledgement for remote request, you can specify the `&T4` command and a timeout in the `S18` register in the AT string (see Table 3-3).

Note If &T4 is specified in the syntax of the AT string, it must occur at the beginning of the string. This is a requirement for SDTN.

The syntax is as follows:

`[&T4[S18=n]]`

You can also use the extended format of the +MS command to set values of specific S-registers to fine-tune these variations, shown in Table 3-3. These values apply only when V.22 or V.22bis modulation is specified, and use the following syntax:

`+MS=mod[&GN][S221=n][S220=n][S10=n]`

In this syntax,

- *mod* must be set to 1 or 2 (see Table 3-2).
- &G*n* enables or disables an 1800Hz guard tone (see Table 3-3).
- S221=*n* specifies a silent period (see Table 3-3).
- S220=*n* specifies the answer tone duration (see Table 3-3).
- S10=*n* specifies a carrier loss detection timer (see Table 3-3).

Table 3-3. Variations from CCITT parameters (page 1 of 2)

Register	MultiDSP range	Function	Description
&T4	If specified, a remote digital loopback (RDL) request from a remote modem is allowed.	Test and diagnostics	If &T4 is included in the value of at-answer-string, the remote access services (RAS) modem will support V.54 RDL 2 (as specified in Section 7.1: Test Loops, in ITU spec V.22), originated from the client (terminal) modem and looped at the RAS modem. If S18 is non-zero, a test will terminate automatically after the time specified by S18 and display OK.
S18	1–255 in1-second increments	Test timer	Maximum duration for which the RAS modem performs loopback, if not terminated by the client.
&G	0–2, default 2 selects 1800Hz tone, 0 and 1 disable guard tone	1800Hz guard tone	Modem should be able to generate guard tone after the silence period and answer-tone.
S221	1–255 in 10ms increments (Default value: 25)	Silent period	Silence duration before the answering modem transmits the answering tone. Normal: 2.150 sec(+/- 0.35 sec) Reduced: 1.8sec(-0,+0.1sec) Short: <0.1sec

Table 3-3. Variations from CCITT parameters (page 2 of 2)

Register	MultiDSP range	Function	Description	
S220	1–255 in 450ms increments (Default value: 14)	Answer tone	Duration of ANS/ANSam modem-specific tones.	
			Normal:	3.3sec +/-0.7sec
			Reduced:	2.6sec(-0,+0.1sec)
			Short:	1.0sec(-0,+0.1sec)
			Nil:	0.0sec
S10	1–255 in100ms increments (Default value: 3)	Carrier loss disconnect timer	Time the modem waits before hanging up after carrier loss has been detected.	

For example, the following commands set the `at-string` to V.22 modulation, enable the loopback test with a timeout of 15 seconds, and set the S-registers to generate a 1800Hz guard tone, an answer tone duration of 4,950ms, a silence duration of 500ms, and a carrier loss disconnect waiting period of 300ms.

```
admin> read client-3
CONNECTION/client-3 read
admin> set at-string =&t4s18=15+MS=1&g2S220=11S221=50S10=3
admin> write
CONNECTION/client-3 written
```

Call processing features

TAOS 10.1.0 includes the following new call processing features.

Control of initial carriage return (CR) in terminal sessions

A new parameter, `drop-initial-cr`, has been added to the `terminal-server:terminal-mode-configuration` subprofile. This parameter enables the system administrator to choose whether the terminal server should drop the initial character received from the user if it is a carriage return (CR).

The change to the `terminal-mode-configuration` subprofile is as follows:

```
[in TERMINAL-SERVER:terminal-mode-configuration]
silent-mode = no
drop-initial-cr = yes
clear-screen = yes
...
```

Parameter	Setting
`drop-initial-cr`	Enables or disables the dropping of the initial character received from the user if it is a CR. Select one of the following values: ■ `yes` (the default)—Drop the initial character if it is a CR. ■ `no`—Do not drop any initial characters.

Support for PPP Extensible Authentication Protocol (EAP) calls

TAOS 10.1.0 introduces support for the PPP Extensible Authentication Protocol (EAP). EAP is defined in RFC 2284 *PPP Extensible Authentication Protocol (EAP)*.

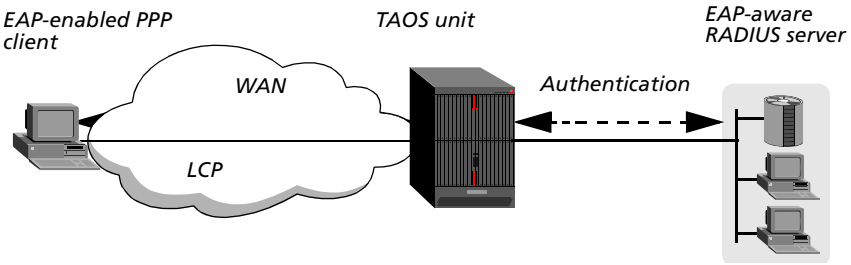
This feature requires the TAOS 10.1 Premium Feature Set software license (see "TAOS 10.1.0 software license requirements" on page 2-1).

TAOS implementation of EAP allows an EAP-enabled PPP client to successfully authenticate on a TAOS unit that uses an EAP-aware RADIUS server for authentication.

Note This initial implementation of EAP requires the use of a RADIUS server for authentication. The TAOS software does not provide EAP authentication within TAOS units, but instead uses RADIUS for authentication.

If a PPP client and a TAOS unit negotiates EAP during Link Control Protocol (LCP) negotiation, and the TAOS unit is not configured with a RADIUS authentication server, the authentication fails and the PPP client is denied access.

Figure 3-1. EAP negotiation on TAOS units



For more information about EAP, see RFC 2284.

To enable the TAOS unit to negotiate EAP during LCP, set the `receive-auth-mode` parameter in the `answer-defaults:ppp-answer` subprofile to one of the following values:

- `eap-ppp-auth`
- `any-ppp-auth`
- `pap-preferred`.

The following sample commands enable a TAOS unit to negotiate authentication for an EAP-enabled PPP client:

```
admin> read answer-defaults
ANSWER-DEFAULTS read
```

```
admin> set ppp-answer receive-auth-mode = eap-ppp-auth
admin> write
ANSWER-DEFAULTS written
```

Disabling end-point discrimination for PPP sessions

For Point-to-Point Protocol (PPP) connections, negotiating an end point discriminator is unnecessary and increases the time it takes to connect. You can disable end point discriminators for a PPP session, which allows negotiations to finish more quickly.

You can now set values for the following parameters so that the unit does not negotiate the Link Control Protocol (LCP) end point discriminator:

`ANSWER-DEFAULTS:mp-answer:enabled = no` and `ANSWER-DEFAULTS:mpp-answer:enabled` = no

or

`ANSWER-DEFAULTS:clid-auth-mode = clid-require or dnis-require` and `CONNECTION/profileName:encapsulation-protocol = ppp`.



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

Magic number negotiation during Link Control Protocol (LCP) setup

During Link Control Protocol (LCP) setup, each end of the connection generates a random number called a magic number. If the magic numbers are the same, then the connection is likely to be looped back.

A new parameter, `use-magic-number` has been added to the `answer:ppp-answer` subprofile. This parameter enables or disables negotiation of a magic number during LCP set up to ensure compatibility with certain types of third-party equipment used as dial-in clients.

When there is no magic number negotiation between some third-party clients acting as home gateways and a TAOS unit acting as a network access server (NAS), the gateway sends an echo request with 0 (zero) as the magic number. Receiving 0 in the request causes the TAOS unit to drop the connection. You can avoid dropped connections by forcing magic number negotiation with the `use-magic-number` parameter.

```
[in ANSWER-DEFAULTS:ppp-answer]
use-magic-number = no
```

Parameter	Specifies
use-magic-number	Enables/disables magic number negotiation during LCP setup. Select one of the following values: ■ yes—Enable magic number negotiation. ■ no (the default)—Disable magic number negotiation. If the lqm parameter in the same subprofile is set to yes, then magic number negotiation is enabled whether use-magic-number is set to yes or no.

Configuring LCP/NCP timeout

To limit retransmits that can prolong Point-to-Point Protocol (PPP) convergence, you can now set retry and timer values for Link Control Protocol (LCP) and Network Control Protocol (NCP). In TAOS 10.1.0, the answer-defaults:ppp-answer profile now includes the new max-ppp-configure-retry, ppp-restart-timer, and max-ppp-restart-timer parameters for configuring retry and timer values.

The connection:ppp-options subprofile also show the settings for these parameters, but only as read-only values.

When the TAOS unit sends a request, it waits for the amount of time specified (in hundredths of a second) by the ppp-restart-timer parameter to receive an acknowledgment. If the TAOS unit receives no response, it sends another request and waits twice the time it waited after the first attempt or the time indicated in the max-ppp-restart parameter, whichever is less. It retries the number of times specified in the max-ppp-configure-retry parameter.

Parameter	Setting
max-ppp-configure-retry	Number of attempts allowed if LCP or NCP fails. Specify a number from 0 to 100.
ppp-restart-timer	Elapsed time, in hundredths of a second, that the TAOS unit waits for a response after sending the first LCP or NCP request. Specify a number from 10 to 6000.
max-ppp-restart-timer	Maximum LCP/NCP restart timer in 1/100th of a second. Specify a number from 10 to 6000.

For example, with the following configuration in the answer profile's ppp-answer subprofile, the TAOS unit responds as follows:

```
[in ANSWER-DEFAULTS:ppp-answer}
max-ppp-configure-retry=10
ppp-restart-timer=200
max-ppp-restart-timer=300
```

The TAOS unit sends a request and waits for the time specified in the `ppp-restart-timer` parameter—200 x .01 second, or 2 second. If there is no acknowledgement, the unit sends another request. The unit then waits for 3 seconds (twice the value of `ppp-restart-timer` is 4 seconds, but the value of `max-ppp-restart-timer` is 3 seconds, which is less). If there is no acknowledgment after the second attempt, the TAOS unit sends another request. The unit continues to attempt to send the request for the number of times specified by the `max-ppp-configure-retry` parameter. In the example, it continues to try to connect up to 8 more times for a maximum of 10 attempts.

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

Configurable egress packet flow

The packet-flow control feature limits the packets sent from the egress card to the shelf controller. In this release, a `slot-pfctrl` profile is created for each egress slot card that uses the packet-flow control mechanism.

Supported cards

The packet-flow control feature is implemented for the following egress cards:

- Ethernet-2
- Ethernet-3
- Ethernet-3ND
- OC3-ATM
- APX Ethernet



Note Virtually all traffic arriving on an egress interface, and departing from an egress or WAN interface, should be sent slot-to-slot and not by means of the shelf controller.

Setting values in the `slot-pfctrl` profile

Following is a listing of the new `slot-pfctrl` profile:

```
[in SLOT-PFCTRL/{ shelf-1 slot-5 0 }]
slot-address* = { shelf-1 slot-5 0 }
threshold = 900
window-size = 1000
```

You can set the following parameters:

Parameter	Setting
slot-address	Shelf, slot, and item number.

Parameter	Setting
`threshold`	Packet-flow control threshold. Specify an integer from 300 through 20000. The default is 900 for a MAX TNT unit and 1000 for an APX unit.
`window-size`	Packet-flow control window size in milliseconds. Specify an integer from 500 through 2000. The default is 1000.

Changes are effective immediately.



Caution Unless a specific issue has been identified, changing the settings in the `slot-pfctrl` profile from their defaults is not recommended.

Configurable idle pattern for all channels of T1

The idle pattern of a DS0 channel is the bit pattern the system transmits when the channel is in the idle state. The pattern is specified by `255` for all ones, 0 or all zeros, or any value in between.

Previously, you could specify the idle pattern for each DS0 in the `channel-config` configuration. Now, you also have the choice to configure a single idle pattern to be applied to all DS0s of a T1 line. Following are the new parameters, shown with default settings:

```
[in T1/{ any-shelf any-slot 0 }
use-ds1-idle-pattern = no
idle-pattern = 255
```

Parameter	Setting
`use-ds1-idle-pattern`	Enables or disables use of the DS1-based idle pattern for all of the line's component DS0s. With the default `no` setting, the system transmits the idle pattern for each DS0 based on the settings in the DS0's `channel-config` subprofile. When set to `yes`, the system transmits the idle pattern specified in the T1 profile for all the line's component DS0s.
`idle-pattern`	The DS1-based idle pattern. For this pattern to be transmitted when any one of the DS0 channels of this line are idle, the `use-ds1-idle-pattern` parameter must be set to `yes`.

For example, the following commands configure a single idle pattern for all DS0s of a T1 line in slot 3:

```
admin> read t1 { 1 3 1 }
T1/{ shelf-1 slot-3 1 } read
admin> set line use-ds1-idle-pattern = yes
admin> set line idle-pattern = 200
admin> write -f
```

```
T1/{ shelf-1 slot-3 1 } written
```

Call routing features

With this software version, several call routing changes have been introduced to make the allocation of resources for calls easier and more efficient, and to make information about slot-card usage and status accessible to administrators.

Supported call-route types

When the system first detects the presence of a slot card, it generates a default `call-route` profile for each call-route type supported by the card. The number of supported types depends partly on software licensing and the kind of network interface (T1 or E1) in the system. Table 3-4 provides a general list of supported call-route types with licensing and interface requirements.

Table 3-4. General list of call-route types supported by slot cards

Type of slot card	`call-route-type` **value**	**Requirements**
All channelized line cards	`trunk-call-type`	None
Digital modem	`voice-call-type`	None
	`digital-call-type`	None
Hybrid Access	`digital-call-type`	None

Table 3-4. General list of call-route types supported by slot cards

Type of slot card	`call-route-type` **value**	**Requirements**
48-port MultiDSP	`voice-call-type`	None
	`digital-call-type`	None
	`wormarq-call-type`	Window-control Operation based on Reception Memory-Automatic Retransmission Request (WORM-ARQ) software license and T1
	`phs-call-type`	Personal Handyphone System (PHS) software licenses and T1
	`v110-call-type`	V.110 software license
	`voip-call-type`	Voice over IP (VoIP) software license
	`g729-call-type`	VoIP software license
	`g723-call-type`	VoIP software license
	`g728-call-type`	VoIP software license
96-port MultiDSP	`voice-call-type`	None
	`digital-call-type`	None
	`phs-call-type`	PHS software licenses and T1
	`v110-call-type`	V.110 software license
	`voip-call-type`	VoIP software license
	`g729-call-type`	VoIP software license

Table 3-4. General list of call-route types supported by slot cards

Type of slot card	`call-route-type` value	Requirements
288-port/240-port MultiDSP	`voice-call-type`	None
	`digital-call-type`	None
	`phs-call-type`	PHS software licenses and T1
	`v110-call-type`	V.110 software license
	`voip-call-type`	VoIP software license
	`g729-call-type`	VoIP software license
	`g723-call-type`	VoIP software license

Overview of the call routing algorithm

The algorithm for selecting a device to handle a call is affected by several things, including the `call-route` profiles used to generate the call route database, the nature of the platform and its cards, and the two sorting methods specified in the `system` profile.

1 Matching `call-route` parameters for a given `call-route-type`

When the system receives or places a call, it uses the following criteria (shown in order of precedence) to group cards depending on how well their `call-route` profiles for the given `call-route-type` match the parameters of the call.

- Trunk group
- Subaddress
- Phone number
- Preferred source

This results in groupings of cards whose profiles match the parameters of the call equally well (although not necessarily exactly). The first group contains best-matching cards, the next group of cards contains less specific matches, and so forth. All non-matching cards are discarded from further consideration. See "Best-match requirement in selecting devices" on page 3-20 for related information.

2 Precedence rules based on the nature of the platform and its cards

The system then evaluates the following criteria, shown in order of precedence:

- Reserved/suspect status of its resources
- Preferred destination quadrant when applicable (for the APX 8000)
- Preferred destination slot when applicable (L2TP dialout, MP+™ dialout)
- Cost (if priority-based call routing is enabled)

Cost has the lowest precedence because the other criteria are considered more important. For example, the system prefers not to use a reserved or suspect

resource, even at a higher cost. See "New cost allocations for priority-based call routing" on page 3-22 for related information.

3 Sort method specified in the `system` profile

At this point in the selection process, groups of matching cards have been divided into ordered subgroups based on the precedence rules. The resources within each subgroup are considered equally acceptable devices for the call. To choose among them, the system uses the call routing sort methods described in "Sort methods to distribute calls efficiently" on page 3-20.

Deactivating a call route

For each installed slot card, the system creates one default `call-route` profile for each `call-route-type` the card supports. These default `call-route` profiles ensure that the system can route the call types internally to the card. You can now control which cards process certain types of calls by deactivating the route to a card for a specific supported `call-route-type`.

To prevent a slot card from taking a supported `call-route-type`, you must set the following parameter (shown with its default value) in the system-generated default `call-route` profile for that `call-route-type`.

```
[in CALL-ROUTE/{ { { shelf-1 any-slot 0 } 0 } 0 }]
active = yes
```

Parameter	Setting
`active`	Activates or deactivates the `call-route` profile. Deactivating a profile causes the system not to route the `call-route-type` specified in the profile to the slot card specified in the profile's `index` field.

Note Simply deleting `call-route` profiles for the unwanted call type is not a reliable way of preventing a card from processing that type of call. At the next system reset, if the system detects that a card has no `call-route` profiles for a supported `call-route-type`, it recreates the default profile for that `call-route-type`.

For example, the following commands deactivate the `call-route` profile for digital calls to a MultiDSP card in slot 4:

```
admin> read call-route { { { 1 4 0 } 0 } 1 }
CALL-ROUTE/{ { { shelf-1 slot-4 0 } 0 } 1 } read

admin> set active = no

admin> list
[in CALL-ROUTE/{ { { shelf-1 slot-4 0 } 0 } 1 }]
index* = { { { shelf-1 slot-4 0 } 0 } 1 }
active = no
trunk-group = 0
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = digital-call-type
cost = 50
```

```
admin> write -f
CALL-ROUTE/{ { { shelf-1 slot-4 0 } 0 } 1 } written
```

Sort methods to distribute calls efficiently

In previous software versions, the `digital-call-routing-sort-method` setting was not operational. Because digital calls are often Multilink Protocol (MP) calls that span multiple channels, the system now supports this setting as a way to increase the likelihood that the channels of an MP call will be grouped efficiently on one slot card. Following are the parameters that affect these usage patterns, shown with default values:

```
[in SYSTEM]
call-routing-sort-method = item-first
digital-call-routing-sort-method = slot-first
```

These parameters are similar, but they have a different scope (one applies only to analog calls and the other to digital calls) and different default values. Both parameters can be set to one of the following values:

Setting	Description
`slot-first`	The `slot-first` setting causes device entries in the call route database to be sorted by this method: *`slot item logical-item`* This sort order weights the system toward using all resources of a card in one slot before moving on to use the resources of a card in the next slot. This results in improved performance for multichannel calls. The system chooses cards from the lowest slot number to the highest slot number. For example, a card in slot 3 is used until it has no remaining resources, at which point the system chooses a card in slot 4 or higher.
`item-first`	The `item-first` setting causes device entries in the call route database to be sorted by usage. This sort order weights the system toward interspersing the resources of different cards, resulting in a more even load balancing across all cards. The system evaluates a card's percentage of use and selects the card that is least busy.

Best-match requirement in selecting devices

As the system matches the parameters of a call to entries in its call route database, it creates groupings of cards whose profiles match the call parameters equally well (although not necessarily exactly). The first group contains best-matching cards, the next group of cards contains less specific matches, and so forth.

You can now set the following parameter, shown with its default value, to prevent the system from selecting a resource in another group if it does not find an available device in the best-matching group of destination resources:

```
[in SYSTEM]
best-match-only = no
```

Parameter	Specifies
`best-match-only`	With the default `no` setting, if the system cannot route the call to devices that match the call most specifically, for example, because those devices are all in use, the system looks for a less specific match. If set to `yes`, the system considers only the most specific match when selecting devices. This forces the system to route only to a specific resource or if that resource is not available, to drop the call.

In the following example, the system supports four line cards (such as T3, T1, or E1). In the `system` profile, the use of trunk groups is enabled and `num-digits-trunk-groups` is set to 1.

For the purposes of this example, an outbound call is being placed with the dial number 71234. Outbound calls have a `call-route-type` of `trunk-call-type`. Table 3-5 shows the system's relevant `call-route` profile settings. (The slot order of the line cards is unimportant, so they are simply designated as A through D.)

Table 3-5. Example trunk-call-type settings

Line card	Relevant `call-route` profile settings

Slot A	`trunk-group = 7`
	`phone-number = ""`
	`preferred-source = { { any-shelf any-slot 0 } 0 }`
	`call-route-type = trunk-call-type`

Slot B	`trunk-group = 7`
	`phone-number = "1234"`
	`preferred-source = { { any-shelf any-slot 0 } 0 }`
	`call-route-type = trunk-call-type`

Slot C	`trunk-group = 0`
	`phone-number = ""`
	`preferred-source = { { any-shelf any-slot 0 } 0 }`
	`call-route-type = trunk-call-type`

Slot D	`trunk-group = 7`
	`phone-number = ""`
	`preferred-source = { { any-shelf any-slot 0 } 0 }`
	`call-route-type = trunk-call-type`

With these call-route profiles, the selection algorithm for the outbound call results in the following groups of line cards, starting with the best-matching group:

- Group 1: Slot B

- Group 2: Slots A, D
- Group 3: Slot C

The system will first look for a resource in Group 1. If no resource is found, it falls back to Group 2, and so on to Group 3.

For example, the following commands force the system to route only to a specific resource that matches the call's parameters, or to drop the call if that resource is not found:

```
admin> read system
SYSTEM read
admin> set best-match-only = yes
admin> write -f
SYSTEM written
```

New cost allocations for priority-based call routing

Priority-based call routing is a way to direct the system to use its more specialized resources first for inbound or outbound calls. In the initial priority-based call routing implementation, introduced in TAOS 10.0, the system assigned hard-coded, customizable `cost` values to each `call-route-type` supported by a slot card. However, with this method, certain administrative events, such as a system upgrade or bouncing a slot card, could result in an uneven distribution of calls across slot card of the same type.

With this software version, the system uses a more generalized approach to cost assignments for call routing purposes.

The following parameters, shown with default settings, affect how the system uses `call-route` cost assignments:

```
[in CALL-ROUTE/{ { any-shelf any-slot 0 } 0 } 0 }]
call-route-type = any-call-type
cost = 0
[in SYSTEM]
least-cost-call-routing = auto-enabled
```

Parameter	Setting
`call-route-type`	Type of call supported by the destination slot card.
`cost`	Numeric value from 0 through 65,535, used by the system as a priority setting for routing the `call-route-type` to the destination slot card. When the system creates a default `call-route` profile, the `cost` value is always set to zero. This is a "magic" value that the system replaces with the card's standard cost. The standard cost for a card is equal to 10 times the number of `call-route-type` values supported by the slot card. Changing the default value of this parameter has no effect unless `least-cost-call-routing` is set to `manual-enabled`.

Parameter	Setting	
`least-cost-call-routing`	How to interpret the `cost` value in `call-route` profiles when selecting a device.	
	`auto-enabled`	Ignore the `cost` value in `call-route` profiles and use the standard cost (10 times the number of `call-route-type` values supported by the slot card) for all cards. The more types supported by a card, the more expensive the card is to use.
	`manual-enabled`	Use the `cost` value in a `call-route` profile. With the default `cost` value of zero in a `call-route` profile, the system automatically uses the standard cost for the slot card, which is the same behavior as `auto-enabled` mode. In this mode, you can also set specific `cost` values in `call-route` profiles to fine-tune call routing for specific call-route types.
	`disabled`	Do not consider costs in selecting the destination slot card for a call.

When you change the `least-cost-call-routing` setting, the system rebuilds the call routing tree on the fly to reflect the new setting immediately. Because the cost associated with a route is not always visible in the setting of the `cost` parameter, you must use the `callroute` command to see the actual costs being used. For example, the `callroute -ih` command shows costs for host cards:

```
admin> callroute -ih
   slot      cost  source          type             tg sa phone
 1:04:00/0     60 0:00:00/0   voice-call-type       0  0
 1:16:00/0     70 0:00:00/0   voice-call-type       0  0
 1:05:00/0    100 0:00:00/0   voice-call-type       0  0
 1:09:00/0     10 0:00:00/0   digital-call-type     0  0
 1:32:00/0     10 0:00:00/0   digital-call-type     0  0
 1:04:00/0     60 0:00:00/0   digital-call-type     0  0
 1:16:00/0     70 0:00:00/0   digital-call-type     0  0
 1:05:00/0    100 0:00:00/0   digital-call-type     0  0
 1:04:00/0     60 0:00:00/0   phs-call-type         0  0
 1:16:00/0     70 0:00:00/0   phs-call-type         0  0
 1:05:00/0    100 0:00:00/0   phs-call-type         0  0
 1:04:00/0     60 0:00:00/0   voip-call-type        0  0
 1:16:00/0     70 0:00:00/0   voip-call-type        0  0
 1:05:00/0    100 0:00:00/0   voip-call-type        0  0
 1:04:00/0     60 0:00:00/0   v110-call-type        0  0
 1:16:00/0     70 0:00:00/0   v110-call-type        0  0
 1:05:00/0    100 0:00:00/0   v110-call-type        0  0
 1:05:00/0    100 0:00:00/0   wormarq-call-type     0  0
 1:04:00/0     60 0:00:00/0   g729-call-type        0  0
```

```
 1:16:00/0     70 0:00:00/0   g729-call-type       0  0
 1:05:00/0    100 0:00:00/0   g729-call-type       0  0
 1:05:00/0    100 0:00:00/0   g728-call-type       0  0
 1:16:00/0     70 0:00:00/0   g723-call-type       0  0
 1:05:00/0    100 0:00:00/0   g723-call-type       0  0
```

If the `least-cost-call-routing` parameter to disabled, cost information is no longer displayed in the output of call-routing commands.

New call routing administrative capabilities

To provide more control over call routing and more related information, the `callroute`, `slot`, and `routecall` system commands have been modified.

Changes to the `callroute` command

The `callroute` command has been modified to support new `-t` and `-s` options to display information about device usage, and the `-r` option to repair a call routing configuration. All other options report a more static view of the call route database, without reflecting usage or status in their output. Following is the new `callroute` usage statement:

```
admin> ? callroute
callroute usage: callroute -option [ params ]
       -d  list call routing tables by (d)evice
       -ih list (i)nput (h)ost-side call routing entries
           ie, destination slot routing for host side
       -in list (i)nput (n)etwork-side call routing entries
           ie, destination slot routing for network side
       -t  detailed call routing tree for the given call-route-(t)ype
       -s  list call routing entries (devices) status for the given
           destination (s)lot
       -r  (r)epair CALL-ROUTE profiles for the given slot: will remove
           invalid profiles and add missing ones if applicable.
           Monitor SysLog (Info, Warning) for detailed report.
       -?  display this summary
```

Using `callroute -t` to view call distribution

The output of the `callroute -t` command gives a clear view of how calls of a particular `call-route-type` are distributed systemwide. Specify a call-route type as an argument to the command. You can enter the full type (a value of the `call-route-type` parameter), the `call-route-type` number, or a unique string identifying the type.

For host resources such as MultiDSP cards, it shows the percentage of use for each card (the number of assigned ports divided by the number of operational ports), and the percentage of suspect modems (the number of suspect ports divided by the number of available operational ports). A modem becomes suspect if it has too many consecutive failures.

For example, the following output was produced on a system with the default sort method (`slot-first`) for digital calls. The command was entered during traffic ramp-up, when traffic had just started and no call has disconnected yet. Because the calls

are sorted `slot-first`, the MultiDSP cards with the lowest slot numbers are used first.

```
admin> callroute -t digital
Call Routing Tree for: digital-call-type
=======================
Trunk Group 0, SubAddr 0, Phone Number "", pref. src. {{0 0 0} 0}
Cost: 50
Destination: {{1 4 0} 0} x1, usage 100% (suspect 0%), madd3-card
Destination: {{1 5 0} 0} x1, usage 100% (suspect 0%), madd3-card
Destination: {{1 7 0} 0} x1, usage 100% (suspect 0%), madd3-card
Destination: {{1 8 0} 0} x1, usage 100% (suspect 0%), madd3-card
Destination: {{1 9 0} 0} x1, usage 30% (suspect 0%), madd3-card
Destination: {{1 10 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 11 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 12 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 13 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 14 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 16 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 18 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 23 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 24 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 25 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 26 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 27 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 28 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 29 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 30 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 32 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 33 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 34 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 35 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 36 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 37 0} 0} x1, usage 0% (suspect 0%), madd3-card
Destination: {{1 38 0} 0} x1, usage 0% (suspect 0%), madd3-card
IDLE ports for digital-call-type: 6535
```



Note If you change the sort method for digital calls to `item-first`, the output would show an even distribution across MultiDSP cards.

For line cards such as T1, the output shows the percentage of reserved channels (the number of reserved ports divided by the number of available operational ports). MP calls normally reserve channels for additional calls. A reserved channel is available, meaning it can be used for incoming or outgoing calls, but the system prefers to use non-reserved channels first. Once a channel is reserved, it cannot be put on another reservation list. The following output for the T1 card shows one assigned channel, with one channel reserved:

```
admin> callroute -t trunk
Call Routing Tree for: trunk-call-type
=======================

Trunk Group 0, SubAddr 0, Phone Number "", pref. src. {{0 0 0} 0}
    Cost: 10
```

```
        Destination: {{1 3 0} 0} x1, usage 4% (reserved 4%), 8t1-card

IDLE ports for trunk-call-type: 22
```

Using `callroute -s` to display device maps

The `callroute -s` command displays DSP status for a given slot card, in the same sort order in which they occur in the call route database. Specify a slot number as an argument to the command. The output uses a single-character symbol for each device. The following symbols are used in the bitmap:

- An asterisk (`*`) means the channel is assigned.
- A hyphen (`-`) means the channel is idle.
- A lowercase O (`o`) means the channel is not operational.
- A lowercase R (`r`) means the channel is reserved.

Following is sample output for a Hybrid Access card in slot 11:

```
admin> callroute -s 11
    DSP      device Map
{1 11 3}  : *------- -------- -------- -------o
{1 11 5}  : *------- -------- -------- -------o
{1 11 6}  : ***----- -------- -------- -------o
{1 11 2}  : ****---- -------- -------- -------o
{1 11 1}  : ******** ******** ******** *------o
{1 11 4}  : **------ -------- -------- -------o
```

MultiDSP cards do not support multiple channels, so their devices are simply reported as `idle`, `active`, or `suspect`. For example, following is sample output for a MultiDSP card in slot 4:

```
admin> callroute -s 4
===== slot 4, madd2-card =====
    DSP      device Map
{1 4 1}   : idle
{1 4 2}   : idle
...
{1 4 95}  : idle
{1 4 96}  : idle
{1 4 46}  : idle suspect
```

Following is a sample output for a T1 line in which channel 12 is reserved:

```
admin> callroute -s 3
===== slot 3, 8t1-card =====
    DSP      device Map
{1 3 1}   : -------- ---r---- -------o ooooooo
```

Using `callroute -r` to repair `call-route` profiles

Whenever a card or the unit itself is reset, the system analyzes the `call-route` profiles for the card (or all cards) and performs repairs as needed. Specifically, it deletes invalid profiles, and if at least one `call-route` profile (whether active or inactive) did not exist for each `call-route-type` supported for a card, it creates a default profile for that type of call.

With this software version, the `callroute -r` command enables administrators to perform these actions more simply, without resetting anything. The usage for the new option is as follows:

```
admin> callroute -r
usage: callroute -r <slot> | all
```

To repair routes to a single slot card, specify its slot number. To repair the `call-route` profiles of all cards currently in the UP state, specify the `all` argument on the command line. For example, the following command analyzes and repairs call routes for a MultiDSP card in slot 3:

```
admin> callroute -r 3
```

The changes occur silently. To view the addition or deletion of `call-route` profiles caused by this command, you must monitor log messages.

Using the `slot` command to force a new call routing configuration

Following is the new usage statement for the `slot` command:

```
admin> ? slot
slot usage: slot -u|d|r|b|m|? [ -all [ host | line ] | [ <shelf> ] <slot> ]
        -u  (u)p a slot card
        -d  (d)own a slot card
        -r  (r)emove a slot card
        -b  (b)ounce a slot card
        -m  put a slot card in (m)aintenance state
        -?  display this summary
```

With this software version, two suboptions are provided to the `-all` option, allowing administrators to affect all `host` cards or all `line` cards, respectively.



Caution Be very careful if you intend to use the **`slot -r -all line`** command to remove profiles for line cards! This command removes not only the `call-route` profiles, but also the T1 or E1 profiles from the system.

As an example of how to use the slot command to perform wide-reaching call routing changes, suppose you do not wish to use the customized settings in your `call-route` profiles for MultiDSP cards any longer. For a system with the following slot cards:

```
admin> show
Controller { right-controller } ( PRIMARY ):
                                Reqd  Oper   Slot Type
    { left-controller }         UP    UP     ( SECONDARY )
    { shelf-1 slot-1 0 }        UP    UP     8t1-card
    { shelf-1 slot-2 0 }        UP    UP     t3-card
    { shelf-1 slot-3 0 }        UP    UP     ether3-card
    { shelf-1 slot-4 0 }        UP    UP     madd2-card
    { shelf-1 slot-5 0 }        UP    UP     madd-card
    { shelf-1 slot-9 0 }        UP    UP     madd3-card
    { shelf-1 slot-16 0 }       UP    UP     madd3-card
    { shelf-1 slot-32 0 }       UP    UP     madd2-card
    { shelf-1 slot-33 0 }       UP    UP     ether3-card
```

The following set of commands creates a fresh call routing configuration for all host cards in the system. The first command brings down all host cards:

```
admin> slot -d -all host
Slot 1/4, state change forced
warning: new state will remain until next explicit management action.
Slot 1/5, state change forced
warning: new state will remain until next explicit management action.
Slot 1/9, state change forced
warning: new state will remain until next explicit management action.
Slot 1/16, state change forced
warning: new state will remain until next explicit management action.
Slot 1/32, state change forced
warning: new state will remain until next explicit management action.
```

The next command "removes" the cards, causing the system to delete their `call-route` profiles.

```
admin> slot -r -all host
Slot 1/4 removed
Slot 1/5 removed
Slot 1/9 removed
Slot 1/16 removed
Slot 1/32 removed
```

After the slot cards have been removed in this way, the system no longer recognizes that a host card is installed in the slot. The next command initiates an UP state for all slots that are not currently up, which forces the system to analyze the `call-route` profiles and create defaults for all supported call-route types.

```
admin> slot -u -all
Slot 1/1, state change forced.
Slot 1/2, state change forced.
Slot 1/3, state change forced.
Slot 1/4, state change forced.
Slot 1/5, state change forced.
Slot 1/9, state change forced.
Slot 1/16, state change forced.
Slot 1/32, state change forced.
Slot 1/33, state change forced.
```

Changes to the `routecall` command

The `routecall` command is used to simulate resource selection algorithm for call routing. With this software version, obsolete options have been removed and more specific call type selection has been added. Both incoming and outgoing calls can now be easily simulated, including support for the called phone number in both directions. A new option allows testing of the rerouting code.

Following is the command's new usage statement:

```
admin> routecall
usage: routecall -t call-route-type [ -o ] [ -n numChans ]
                 [ -p phoneNumber ] [ -s {{shelf slot item} li} ]
                 [ -d {{shelf slot item} li} ]
                 [ -r {{shelf slot item} li} ]
       -t  call-route-type
```

```
-o  this is for an (o)utgoing call (default is incoming),
    both HOST and LINE side will be selected
-n  (n)number of channels needed for the call (default is 1)
-p  called (p)hone number (DNIS)
-s  (s)ource device {{shelf slot item} logicalItem}
-d  preferred (d)estination {{shelf slot item} logicalItem}
-r  (r)erouting: validates device {{shelf slot item} logicalItem}
    for your parameters, and tries to find a better device
-?  display this summary
```

Command element	Description
`-t` *`call-route-type`*	Specifies the *`call-route-type`* to simulate. You can specify the *`call-route-type`* argument as a unique string or call type number. Valid *`call-route-type`* values are the same for this command as for the `call-route-type` parameter.
`-o`	Specifies that the simulated call is outgoing. Both the host and line sides are selected.
`-n` *`numChans`*	Specifies the number of channels needed for the call. The default is 1.
`-p` *`phoneNumber`*	Specifies the called telephone number. The default is null.
`-s {{`*`shelf slot item`*`}` *`logical-item`*`}`	Specifies source device. The default is {{0 0 0}0}.
`-d {{`*`shelf slot item`*`}` *`logical-item`*`}`	Specifies the preferred destination device. The default is {{0 0 0}0}.
`-r {{`*`shelf slot item`*`}` *`logical-item`*`}`	Validate the device {{*`shelf slot item`*} *`logical-item`* for your parameters and tries to find a better device if available.
`-s {{`*`shelf slot item`*`}` *`logical-item`*`}`	Specifies the source device. The default is {{0 0 0}0}.

Some sample outputs from the `routecall` command are as follows:

For an incoming digital call from the line card in slot 1:

```
admin> routecall -t dig -s { { 1 1 1 } 12 } -p 71234
HOST device selection...
        Incoming, digital-call-type, trkGrp 9, DNIS "71234"
        source {{1 1 1} 12}, pref destination {{0 0 0} 0}
        number of channels 1
Call will be routed to HOST device(s):
        {{1 5 1} 1}
```

For an outgoing analog call:

```
admin> routecall -o -t voice -p 71234
HOST device selection...
        Outgoing, voice-call-type, trkGrp 7, DNIS "71234"
        source {{0 0 0} 0}, pref destination {{0 0 0} 0}
        number of channels 1
```

```
Call will be routed to HOST device(s):
        {{1 10 7} 0}
LINE device selection...
        Outgoing, voice-call-type, trkGrp 7, DNIS "71234"
        source {{1 10 7} 0}, pref destination {{0 0 0} 0}
        number of channels 1
Call will be routed to DS0(s):
        {{1 2 1} 1}
```

APX 8000 redundancy features

This release provides enhanced controller redundancy functionality for APX 8000 systems with dual controllers. To support these features, the runtime synchronization (or *hot standby* redundancy) feature must be enabled by setting the `sync-enabled` parameter to `yes` in the `redundancy` profile. For example:

```
admin> read redundancy
REDUNDANCY read

admin> set sync-enabled = yes

admin> write -f
REDUNDANCY written
```



Note With this software version, you do not need a separate software license to enable this feature.

Redundancy support for various call types

With this software version, active calls of the following types are maintained across a shelf-controller switchover:

- PPP (including dialout and RADIUS dialout PPP calls)
- Multilink Protocol (MP), Bandwidth Allocation Control Protocol (BACP), and MP+™
- TCP-CLEAR
- Terminal-server `telnet` and `rlogin` connections
- IP Device Control (IPDC), including all call types except outgoing data calls
- Frame Relay permanent virtual circuits (PVCs, on Channelized T1, E1, and T3 modules)
- ATM PVCS (on DS3-ATM, E3-ATM and OC3-ATM modules)
- Layer 2 Tunneling Protocol (L2TP, excluding L2TP dialout)
- Callback protocols
- Ascend Tunnel Management Protocol (ATMP)
- Personal Handyphone System (PHS)
- V.110 and V.120

ATMP tunnels are maintained across a switchover on an APX 8000 system operating as ATMP home agent, foreign agent, or both.

For callback control protocols, if the system has completed the callback and established the connection, the connection is maintained across a switchover. Calls that have been initiated but not fully established are dropped when the switchover occurs.

Call types for which redundancy is not supported

Redundancy is *not* supported for the following call types in TAOS 10.1:

- Multilink Frame Relay
- IPDC outgoing data calls
- L2TP dialout
- Frame Relay switched virtual circuits (SVCs)
- ATM SVCs
- Access SS7 Gateway Control Protocol (ASGCP) and Q.931+
- Point-to-Point Tunneling Protocol (PPTP)
- X.25, X.75
- Serial Line IP (SLIP) and Compressed SLIP (CSLIP)
- H.323
- Short Duration Transaction Network (SDTN)

Redundancy health monitoring

For dual-controller APX 8000 systems with runtime-sync enabled in the `redundancy` profile, the redundancy function now supports controller health monitoring. Previously, failover from the primary to secondary controller occurred automatically only when a fatal error condition occurred on the primary controller. With health monitoring, a more preventive approach is possible in which failover occurs on the basis of warning conditions or available memory thresholds on the primary controller.

Health monitoring functions run on both controllers. Before the primary controller resets to initiate failover, it verifies the health of the secondary controller. If the secondary controller is not in prime condition or is unavailable, or if synchronization of data is incomplete, the primary controller does not reset.

When failover occurs due to health monitoring conditions, the system logs the following fatal error type:

```
67:FATAL_HEALTH_MONITORING
```

Configuring controller health indexes

You configure the parameters related to health monitoring in the new `redundancy-hm` profile. The contents of this profile is shown below with default values.



Note Default values for the secondary controller are more stringent than those for the primary, because the secondary must be at a level of health that ensures a smooth switchover. When changing default settings, you should maintain the more stringent requirements for the secondary controller.

```
[in REDUNDANCY-HM]
```

```
hm-enabled = no
max-warning-primary = 80
max-warning-secondary = 60
max-warning-per-minute-primary = 30
max-warning-per-minute-secondary = 20
memory-threshold-primary = 10
memory-threshold-secondary = 15
memory-alert-threshold-primary = 15
memory-alert-threshold-secondary = 20
memory-alert-timeout-primary = 90
memory-alert-timeout-secondary = 30
reset-stuck-primary-timeout = 5
```

Parameter	Setting
`hm-enabled`	Enables or disables the health monitoring function. If redundancy and runtime-sync are not enabled in the system, this setting has no effect.
`max-warning-primary`	Maximum total number of warnings (from 1 to 1024) such as "low Memory! reset" on the primary controller before initiating a reset. The default number is 80.
`max-warning-secondary`	Maximum total number of warnings (from 1 to 1024) such as "low Memory! reset" on the secondary controller before initiating a reset. The default number is 60.
`max-warning-per-minute-primary`	Maximum number of warnings per minute (from 1 to 1024) such as "low Memory! reset" on the primary controller before initiating a reset. The default number is 40.
`max-warning-per-minute-secondary`	Maximum number of warnings per minute (from 1 to 1024) such as "low Memory! reset" on the secondary controller before initiating a reset. The default number is 30.
`memory-threshold-primary`	Lowest percentage of available memory (from 0 to 70) allowed on the primary controller before initiating a reset. The default is 10%.
`memory-threshold-secondary`	Lowest percentage of available memory (from 0 to 70) allowed on the secondary controller before initiating a reset. The default is 15%.
`memory-alert-threshold-primary`	Lowest percentage of available memory (from 0 to 70) allowed on the primary controller before generating a log message. The default is 15%.
`memory-alert-threshold-secondary`	Lowest percentage of available memory (from 0 to 70) allowed on the secondary controller before generating a log message. The default is 20%.
`memory-alert-timeout-primary`	Maximum number of seconds (from 3 to 32,767) that the percentage of available memory level must stay below the level specified by `memory-alert-threshold-primary` before generating the log message. The default is 90 seconds.

Parameter	Setting
`memory-alert-timeout-secondary`	Maximum number of seconds (from 3 to 32,767) that the percentage of available memory level must stay below the level specified by `memory-alert-threshold-secondary` before generating the log message. The default is 30 seconds.
`reset-stuck-primary-timeout`	This setting does not apply to the APX 8000 platform.

For example, the following commands on the primary controller configure the system to reset the secondary controller if its available memory goes below 20%, and to reset the primary controller after three warnings about low memory.

```
admin> read redundancy-hm
REDUNDANCY-HM read

admin> set memory-threshold-secondary = 20

admin> set max-warning-primary = 3

admin> write -f
REDUNDANCY-HM written
```

Note that the primary controller will not reset itself due to health monitoring if the secondary controller is not ready to become primary.

BITS interface support for APX 8000 platforms

With this software version, the APX 8000 platform supports dual Building Integrated Timing Supply (BITS) interface modules. Each of the BITS interfaces obtains a reference clock from an attached T1 line and communicates with the system's controllers across the backplane.

Both controllers receive the same set of input signals, but only the primary shelf controller drives the master clock. The secondary controller locks to the same reference clock used by the primary controller, which makes it hot-standby in the event of a switchover. If a switchover occurs, the new primary controller continues to use the known good reference clock, and the new secondary controller locks to the same reference.



Note The BITS interface module supports T1 line interfaces only, so this feature is supported only on APX systems that use T1 and its aggregates for WAN interfaces.

Clock selection procedure

To the phased locked loop (PLL) of the controllers, a BITS clock source is the same as a clock source from a T1 slot card. If the primary controller cannot obtain a clock source from a BITS interface, it falls back to obtaining a reference clock from a T1 line on a slot card.

When you configure BITS interface modules, you assign a preference to either the BITS-A or BITS-B interface as clock source. The preferred interface is then the highest

priority clock source in the system, and the alternate BITS interface is the second highest priority clock source.

By default, all T1 lines are eligible for use as the master clock source, and are assigned the same priority in the clock-selection process. You can remove certain lines from consideration by configuring them as ineligible clock sources, or reduce the likelihood that they will be selected by lowering their priority. For details about T1 clock selection, see the chapter on T1 in the *Physical Interface Guide*. After the T1 lines have been enabled and configured, the clock selection process is as follows:

1 Select the preferred BITS interface clock if possible.

2 If the preferred BITS interface is unavailable, attempt to use the other BITS interface as master clock.

3 If both BITS interfaces are unavailable, select a T1 line on a slot card as clock source. If multiple T1 lines are available with the same priority, select one as clock source using the T1 clock selection algorithm, until a BITS interface becomes available.

4 If both BITS interfaces are unavailable and all T1 lines are either unavailable or configured as ineligible as clock source, use the internal clock generated from the oscillator on the primary shelf controller. Using the internal clock is generally not recommended.

The `clock-source` diagnostic command displays the current master clock source and all available clock sources. For example:

```
admin> clock
   Master: BITS-A
   Source List:
      Source: slot-1/9 Available      priority: 1
      Source: BITS-A Available        priority: 1
      Source: BITS-B Available        priority: 1
```

Enabling and configuring the BITS interfaces

Following are the default settings of the `bits-conf` profile:

```
[in BITS-CONF]
preferred-mode = disabled

bits-interface[1] = { a-bits-if yes esf b8zs csu 1-133 0-db }
bits-interface[2] = { b-bits-if yes esf b8zs csu 1-133 0-db }

[in BITS-CONF:bits-interface[N]]
bits-module = a-bits-if | b-bits-if
enabled = no
frame-type = esf
encoding = b8zs
front-end-type = csu
DSX-line-length = 1-133
CSU-build-out = 0-db
```

Parameter	Setting
`preferred-mode`	Enables BITS clocking and assigns a preference to either the BITS-A or BITS-B Interface. Following are valid values: `disabled` — Do not use BITS interfaces as clock sources. `a-preferred` — Assign BITS-A preference as the master clock source. If BITS-A is not available, examine BITS-B as a suitable source for the master clock. `b-preferred` — Assign BITS-B preference as the master clock source. If BITS-B is not available, examine BITS-A as a suitable source for the master clock.
`bits-interface[`*N*`]`	Two indexed subprofiles for configuring the two BITS interface modules.
`bits-interface[`*N*`]: bits-module`	Specifies a BITS interface (`a-bits-if` when *N* is 1, or `b-bits-if` when *N* is 2).
`bits-interface[`*N*`]: enabled`	Enables/disables the BITS interface.
`bits-interface[`*N*`]: frame-type`	Super-framing mode (`d4` or `esf`) to use on the BITS module's physical T1 link. Currently, this field is read-only and is set to `esf`.
`bits-interface[`*N*`]: encoding`	Layer 1 line encoding (`ami`, `b8zs`, or `none`) to use on the physical T1 link.
`bits-interface[`*N*`]: front-end-type`	Front end type (CSU/DSX) of the T1 transceiver. Use `csu` for long haul, or `dsx` for short haul.
`bits-interface[`*N*`]: DSX-line-length`	For short-haul T1 lines (`dsx`), this setting specifies a range of lengths for the physical line.
`bits-interface[`*N*`]: CSU-build-out`	For long-haul T1 lines (`csu`), this setting specifies the line buildout value.

For example, the following commands enable BITS clocking and specify BITS-A as the preferred interface:

```
admin> read bits-conf
BITS-CONF read

admin> list
[in BITS-CONF]
preferred-mode = disabled
bits-interface = [ { a-bits-if no esf b8zs csu 1-133 0-db } { b-bits-if +

admin> set preferred = a-preferred

admin> set bits-interface 1 enabled = yes

admin> write -f
BITS-CONF written
```

BITS interface states

When viewed from an external management entity, a BITS interface can be in one of the following states:

- not present
- loss of signal
- in sync, out of range
- in sync, in range

The `bits-if-state` profiles display read-only state information about each BITS interface module. This information is accessible in the command-line interface and by external management utilities. Following are the profile contents, shown with representative settings for an operational module:

```
[in BITS-IF-STATE/a-bits-if]
bits-module* = a-bits-if
present = yes
serial-number = 90904321
line-state = active
stratum-traceability = ssm-stratum-none
```

Parameter	Setting	
`bits-module`	Index of the BITS interface module (a–bits–if for BITS interface A or b–bits–if for BITS interface B).	
`present`	Indicates whether the controller detects the presence of the BITS interface module (`yes` or `no`).	
`serial-number`	The serial number of the BITS interface module.	
`line-state`	Line state of the BITS interface module. Following are valid values:	
	`does-not-exist`	Link is not present.
	`disabled`	Line disabled.
	`loss-of-sync`	Red-alarm state, plus or minus.
	`yellow-alarm`	Yellow-alarm state.
	`ais-receive`	Receiving keep-alive signal.
	`no-d-channel`	D-Channel failure.
	`active`	Multipoint established.
	`nt_active`	NT Multipoint established.
	`te_active`	TE Multipoint established.
`stratum-traceability`	Describes the last Synchronization Status Message (SSM) received on the interface, which indicates the Stratum traceability of the source feeding this interface's clocking. Following is the list of possible values:	
	`ssm-stratum1-traceable`	Stratum-1 traceable (Block of Packet (BOP) codeword 0x04).
	`ssm-stratum2-traceable`	Stratum-2 traceable (BOP codeword 0x0c).

Parameter	Setting
	`ssm-stratum3-traceable` Stratum-3 traceable (BOP codeword 0x10).
	`ssm-stratum3e-traceable` Stratum-3E traceable (BOP codeword 0x7c).
	`ssm-stratum-tnc-traceable` Stratum Transit Node Clock (TNC) traceable (BOP codeword 0x78).
	`ssm-stratum-smc-traceable` Stratum SONET minimum clock traceable (BOP codeword 0x22).
	`ssm-stratum4-traceable` Stratum-4(E) traceable (BOP codeword 0x28).
	`ssm-stratum-non-traceable` Unknown traceability (BOP codeword 0x08).
	`ssm-stratum-not-for-syn` Not usable for synchronization (BOP codeword 0x30).
	`ssm-stratum-provisioned` Provisioned by the network operator (BOP codeword 0x40).
	`ssm-stratum-none` The source feeding this interface's clocking has not sent any SSM since this interface last became operational, or is not configured to send SSM messages.

BITS interface statistics

When a BITS interface module becomes operational, the system creates a `bits-if-stats` profile for each of its interfaces. This is a volatile, read-only profile that provides alarm and performance monitoring statistics. The statistical information is viewable both in the command-line interface and by external management utilities.

Following are the profile contents, shown with representative values for an operational BITS interface module A:

```
[in BITS-IF-STATS/a-bits-if]
bits-interface* = a-bits-if
loss-of-frame = False
loss-of-signal = False
ais-receive = False
yellow-receive = False
framing-error-count = 0
lcv-error-count = 0
crc-error-count = 0
```

Parameter	Indicates
`bits-interface`	Index of the BITS interface module (a–bits–if for BITS interface A or b–bits–if for BITS interface B).
`loss-of-frame`	Loss of frame on the line (`False` or `True`).
`loss-of-signal`	Loss of signal on the line (`False` or `True`).

Parameter	Indicates
ais-receive	The far end is sending Alarm Indication Signal (False or True).
yellow-receive	The far end is sending loss of frame, also called Yellow Alarm (False or True).
framing-error-count	Framing bit error count (numeric).
lcv-error-count	Line code violation error count (numeric).
crc-error-count	Cyclic redundancy check error count (numeric).

Related log messages

The system generates a log message when there is a master clocking change. For example, if reference BITS A is chosen as master clock source, the following log message is displayed:

```
LOG notice, Shelf 1, Right-controller (P), Time: 01:49:56--
Master clock source changed to BITS Interface A
```

SNMP trap support

A trap for a BITS clocking status change is supported in Ascend Enterprise traps. If alarms are enabled, the system sends an alarm to an external management utility. The following parameters, shown with default settings, must be set to yes to enable the alarm:

```
[in TRAP/""]
alarm-enabled = yes
stratum3-status-trap-enabled = yes
```

Both these parameters must be set to yes for the Stratum 3 alarms to be sent to an external management utility. Following are the events related to BITS status that trigger an alarm:

- Change in the system clock source

```
systemClockChanged   NOTIFICATION-TYPE
STATUS           current
DESCRIPTION
"This trap indicates system clock source has changed.
This trap sent to managers when the alarm
and clock source have changed."
::= { ascendNotifications 55 }
```

- Change in the Stratum level of the BITS interface

```
stratumBitsClockLevel NOTIFICATION-TYPE
OBJECTS { bitsInterfaceState__ssm_state }
STATUS current
DESCRIPTION "This trap is sent to the SNMP-Manager to inform the
stratum3 clock sub-system stratum level."
::= { ascendNotifications 65}
```

Routing and traffic management features

TAOS 10.1.0 includes the following traffic management features.

ATM virtual path shaping

With previous TAOS versions, each ATM virtual circuit connected to a traffic shaper was allocated the full amount of bandwidth specified in the shaper definition. This is still the default traffic shaping behavior. If a traffic shaper specifies 1Mbps bandwidth and five virtual circuits are connected to the shaper, each connection is allocated 1Mpbs bandwidth for a total of 5Mbps managed by the shaper. The traffic shaper manages the cell streams as virtual channel connections (VCCs), and operates as a *virtual channel shaper.*

With this software version, you can configure a traffic shaper to operate as a *virtual path shaper*. In this mode, all ATM virtual circuits connected to the traffic shaper *share* the amount of bandwidth specified in the shaper definition. If the traffic shaper specifies 10Mbps bandwidth and five virtual circuits are connected to the shaper, each connection is allocated 2Mpbs bandwidth. The traffic shaper does not perform a virtual path identifier (VPI) check of the individual virtual circuits. In that way, it manages the cell streams as a virtual path connection (VPC), and operates as a virtual path shaper.

Virtual path shaping is supported on the following second-generation ATM slot cards:

Table 3-6. Second-generation ATM slot cards

Slot card	Product code
DS3-ATM2	APX8-SL-UDS3A2-C
E3-ATM	APX8-SL-UE3A-C
OC3-ATM2	TNT-SL-UOC3LF-C TNT-SL-UOC3SF-C TNT-SL-UOC3CP-C

As in previous releases, up to 15 configurable traffic shapers can be configured on each ATM interface. You configure traffic shapers to specify outgoing traffic characteristics such as peak rate and maximum burst size, and then apply a shaper to virtual circuits to affect those characteristics of their outgoing traffic. The new virtual path shaping behavior is enabled by setting the `aggregate` parameter in the traffic shaper to `yes`. A shaper with this setting is a virtual path shaper. When the `aggregate` parameter is set to `no` (the default), the shaper is a virtual channel shaper.



Note Details about defining traffic shapers are provided in the *APX /MAX TNT ATM Configuration Guide*. However, information presented in this release note supersedes similar information in the documentation. In addition to support for virtual path shaping, changes were also made to resource sharing and the minimum/maximum values in a shaper definition.

Changes in transmit resource sharing

With previous software versions, the transmit buffers of the second-generation ATM slot cards were separated into eight pools. The first seven pools were dedicated to traffic shapers 1 through 7, and the remaining pool was shared among the remaining traffic shapers (shapers 8 through 15). When multiple virtual circuits shared the same pool (shapers 8 through 15), the circuits competed for pool resources, which could cause congestion.

With the current TAOS version, each traffic shaper (1 through 15) has its own pool of transmit buffers, and the size of each pool is determined dynamically to provide sufficient resources for the bandwidth specified in a shaper.

In addition, a traffic shaper can now allocate transmit buffers fairly among the virtual circuits connected to the shaper. To ensure that a virtual circuit with low throughput is able to transmit when competing with a virtual circuit with very high throughput, each virtual circuit has a threshold that limits its transmission.

Constraints and limitations

As in previous TAOS versions, if you modify a traffic shaper after it has been applied to virtual circuits, all virtual circuits must be restarted to use the new values. You do not need to reset the system or bounce the slot card to use the new shaper values.

Each traffic shaper can be connected to a maximum of 32 virtual circuits. Because each ATM interface supports up to 15 shapers, each interface can shape a total of up to 480 (15*32) virtual circuits, distributed evenly among the shapers. If more than 32 virtual circuits are connected to a single shaper, the system displays the following warning-level log message:

```
ATM: Too many VCs on the shaper ID n
```

This message informs the administrator that a virtual circuit could not be connected because the number of virtual circuits connected to the shaper exceeded the limit of 32.

The maximum `bit-rate` or `peak-rate` value of a shaper is the effective line rate. TAOS checks that the `peak-rate` and `bit-rate` values of a specific shaper do not exceed the effective line rate. However, when virtual channel shaping is used, the aggregate rates of the virtual circuits connected to the shaper are not checked.

When virtual path shaping is in use, the minimum `bit-rate` or `peak-rate` value is the effective line rate * 32 divided by 65535. Table 3-7 shows the minimum values for each type of slot card:

Table 3-7. Minimum shaper values for second-generation ATM cards

Slot card	Minimum peak-rate or bit-rate value
DS3-ATM2	19Kbps
E3-ATM	15Kbps
OC3-ATM2	66Kbps

If the `peak-rate` or `bit-rate` parameters specifies a value that is less than the minimum shaper value, the system logs a warning message.

The worst case peak cell rate (PCR) is the effective line rate * 32 divided by 255. For example, for an OC3-ATM interface, which has a maximum cell rate of 353,207 cells per second, the worst case PCR is 17Mbps.

Virtual channel shapers are precise within 3%. Virtual path shapers are slightly less precise. Worst case precision is calculated as a percentage by using the following formula, where *n* is the number of virtual circuits connected to the shaper:

```
shaper-precision = 11.1/n
```

Overview of the aggregate parameter setting

Following is the `aggregate` parameter, shown with its default value. This is not a new parameter, but it can now be used to enable virtual path shaping.

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1]]
aggregate = no

[in E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1]]
aggregate = no

[in OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1]]
aggregate = no
```

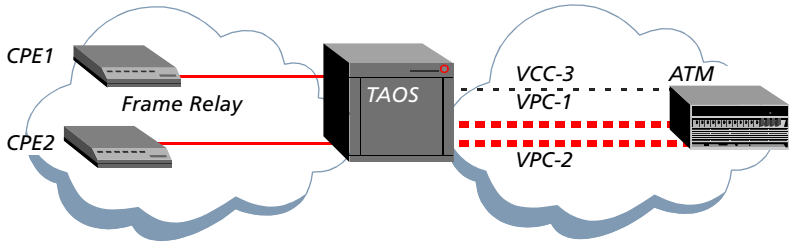
Parameter	Setting
`aggregate`	Enable/disable virtual path shaping mode. With the default `no` setting, each virtual circuit connected to the shaper can use the amount of bandwidth defined by the shaper. This mode is known as virtual channel shaping. In virtual channel shaping mode, TAOS does not verify that the aggregate rates of the multiple virtual circuits do not exceed the effective line rate. If this parameter is set to `yes`, all virtual circuits connected to the shaper share the amount of bandwidth defined by the shaper. This mode is known as virtual path shaping.

Defining and applying virtual path and virtual channel shapers

In the sample setup shown in Figure 3-2, the TAOS unit has an OC3-ATM interface to an ATM switch, and frame relay interfaces to customer premises equipment (CPE). It switches between frame relay encapsulated data from CPE1 and CPE2, and ATM permanent virtual circuits (PVCs) on the basis of ATM-frame relay circuit configurations, using traffic shapers on outbound ATM traffic.

For details about configuring ATM-frame relay circuits, see the *APX /MAX TNT ATM Configuration Guide*.

Figure 3-2. Sample setup to illustrate VP and VC shaping



In the sample setup, the ATM switch must have two virtual path connections to enable traffic switching for PVCs connected to traffic shapers 1 and 2 in the TAOS unit. The ATM switch must also have one virtual channel connection, to enable traffic switching for the PVCs connected to traffic shaper 3 configured in the TAOS unit.

Table 3-8 shows the TAOS traffic shaper values and corresponding QoS values in the ATM switch. Each shaper specifies a constant bit rate (CBR) level of service (`priority = 0`).

Table 3-8. Traffic shaper and QoS values for ATM virtual circuits

TAOS traffic shaper values		**Sample ATM switch VC values**	

`Shaper 1`	`enabled: yes`
	`bit-rate: 15000`
	`peak-rate: 15000`
	`max-burst-size: 2`
	`aggregate: yes`
	`priority: 0`
		VPC-1	QOS: CBR
			PCR: 39063

`Shaper 2`	`enabled: yes`
	`bit-rate: 14000`
	`peak-rate: 14000`
	`max-burst-size: 50`
	`aggregate: yes`
	`priority: 0`
		VPC-2	QOS:CBR
			PCR:36459

`Shaper 3`	`enabled: yes`
	`bit-rate: 1000`
	`peak-rate: 1000`
	`max-burst-size: 2`
	`aggregate: no`
	`priority: 0`
		VCC-3	QOS:CBR
			PCR:2605

The following set of commands configures the OC3-ATM interface and defines the virtual path shapers (1 and 2) and virtual channel shaper (shaper 3) in the TAOS unit:

```
admin> read oc3-atm {1 3 1}
OC3-ATM/{ shelf-1 slot-3 1 } read

admin> set name = atm-switch

admin> set enabled = yes
```

```
admin> set line-config nailed-group = 111
admin> set line-config traffic-shapers 1 enabled = yes
admin> set line-config traffic-shapers 1 bit-rate = 15000
admin> set line-config traffic-shapers 1 peak-rate = 15000
admin> set line-config traffic-shapers 1 aggregate = yes
admin> set line-config traffic-shapers 2 enabled = yes
admin> set line-config traffic-shapers 2 bit-rate = 14000
admin> set line-config traffic-shapers 2 peak-rate = 14000
admin> set line-config traffic-shapers 2 max-burst-size = 50
admin> set line-config traffic-shapers 2 aggregate = yes
admin> set line-config traffic-shapers 3 enabled = yes
admin> write
OC3-ATM/{ shelf-1 slot-3 1 } written
```

After configuring the traffic shapers, you can configure up to 32 virtual circuits connected to each shaper. PVCs connected to traffic shaper 1 will share 15Mbps bandwidth. If you connect two virtual circuits to traffic shaper 1, each connection will have approximately 7.5Mbps bandwidth.

The following set of commands configures the ATM virtual circuit sides of two ATM-frame relay circuits, and connects both virtual circuits to traffic shaper 1. The connection profiles for the frame relay sides of the ATM-frame relay circuits are not shown. See the *APX /MAX TNT ATM Configuration Guide* for details about those configurations.

```
admin> new connection vc-cpe1
CONNECTION/vc-cpe1 read
admin> set active = yes
admin> set encapsulation-protocol = atm-frame-relay-circuit
admin> set ip-options ip-routing-enabled = no
admin> set fr-options circuit-name = atmfr-1
admin> set telco-options call-type = ft1
admin> set telco-options nailed-groups = 111
admin> set session-options traffic-shaper = 1
admin> set atm-options vci = 101
admin> write
CONNECTION/vc-cpe1 written
admin> new connection vc-cpe2
CONNECTION/vc-cpe2 read
admin> set active = yes
admin> set encapsulation-protocol = atm-frame-relay-circuit
admin> set ip-options ip-routing-enabled = no
admin> set fr-options circuit-name = atmfr-2
admin> set telco-options call-type = ft1
admin> set telco-options nailed-groups = 111
```

```
admin> set session-options traffic-shaper = 1
admin> set atm-options vci = 102
admin> write
CONNECTION/vc-cpe2 written
```

Notice that when virtual circuits are connected to a virtual path shaper (traffic shaper 1 in this example), no VPI check is performed on the circuit's cell stream. Each PVC connected to a virtual path shaper has approximately the same throughput.

PVCs connected to traffic shaper 3 (a virtual channel shaper) will each be allocated 1Mpbs bandwidth. If you connect five virtual circuits to traffic shaper 3, for example, the connections will use a total of 5Mbps bandwidth.

Virtual routers now able to route multicast traffic

TAOS 10.1.0 extends multicast support from the main virtual router (Vrouter) to all Vrouters. Enabling Vrouters to route multicast traffic provides support for Web TV and other multimedia applications.

New `multicast-options` subprofile

New parameters for configuring multicast are located in the `vrouter` profile in a `multicast-options` subprofile. Existing parameters by the same names in the `ip-global` profile refer to the main Vrouter. The parameters are as follows (shown with their default values):

```
[in VROUTER/multicast-options]
multicast-forwarding = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
multicast-hbeat-addr = 0.0.0.0
multicast-hbeat-port = 0
multicast-hbeat-slot-time = 0
multicast-hbeat-Number-Slot = 0
multicast-hbeat-Alarm-threshold = 0
multicast-hbeat-src-addr = 0.0.0.0
multicast-hbeat-src-addr-mask = 0.0.0.0
multicast-member-timeout = 360
mbone-backup = [ { no "" { { any-shelf any-slot 0 } 0 } 0 } { no "" { { any+
mbone-timeout = 0
[in VROUTER/"":multicast-options:mbone-backup[1]]
enabled = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
mbone-timeout = 0
```

Parameter	Setting
multicast-forwarding	Enable or disable multicast forwarding. ■ yes enables multicast forwarding. ■ no (the default) disables multicast forwarding. Consider the following: ■ For multicast-forwarding to have any effect, you must set mbone-lan-interface or mbone-profile to specify the interface on which the MBONE router resides. ■ When the value of multicast-forwarding changes from no to yes, the multicast subsystem reads the values in the vrouter or ip-global profile and initiates the forwarding function. If you modify a multicast value in the vrouter or ip-global profile, you must set multicast-forwarding to no and then yes again to force a read of the new values.
mbone-profile	Name of a connection profile the TAOS unit uses to reach the MBONE router on a WAN interface. Default value is null. Do not set both this parameter and mbone-lan-profile; they are mutually exclusive.
mbone-lan-interface	Interface address to the MBONE router on a LAN interface. The default is null. Do not set both this parameter and mbone-profile; they are mutually exclusive.
multicast-hbeat-addr	Multicast address for heartbeat monitoring. The TAOS unit listens for packets to and from the associated group. Specify the address in dotted decimal notation. The default is 0.0.0.0.
multicast-hbeat-port	User Datagram Protocol (UDP) port number. The default is 0 (zero). If specified, heartbeat monitoring listens only for multicast packets received on that port. (All the multicast-hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.)
multicast-hbeat-slot-time	Interval (in seconds) in which the TAOS unit polls for multicast traffic. The default is 0 (zero).
multicast-hbeat-Number-Slot	How many times the TAOS unit polls before comparing the number of multicast packets it received to the multicast-hbeat-alarm-threshold value. The default is 0 (zero).

Parameter	Setting
multicast-hbeat-Alarm-threshold	Minimum number of packets the TAOS unit can receive without generating an alarm trap. The default is 0 (zero), which disables heartbeat monitoring.
multicast-hbeat-src-addr	An IP address. When the TAOS unit performs heartbeat monitoring, it ignores packets from the IP address you specify. Specify the IP address in dotted decimal notation. The default is 0.0.0.0.
multicast-hbeat-src-addr-mask	A subnet mask that the TAOS unit applies to the multicast-hbeat-src-addr value. Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.
multicast-member-timeout	Time-out (in seconds) for client responses to multicast polling messages. Specify an integer from 60 through 65535. The default is 360.
mbone-timeout	Number of seconds elapsed since the last receipt of an IGMP Host Membership Query packet. The router waits for this packet before considering the backup MBONE router to be dead and switching to another backup MBONE. Specify a number from 0 (the default) through 65535. A setting of 0 (zero) disables the mbone-timeout feature.
mbone-backup[1-3]: enabled	Enables or disables the backup MBONE router. In all profiles, specify yes or no. The default for the Ethernet profile is yes. The default for other profiles is no. ■ yes enables a feature, interface, or line. ■ no disables a feature, interface, or line. If enabled is set to no in the Ethernet profile, packets routed to and received by the interface are discarded.
mbone-backup[1-3]:mbone-profile	Name of a connection profile the TAOS unit uses to reach a backup MBONE router on a WAN interface. Default value is null. Do not set both this parameter and mbone-backup [1-3]:mbone-lan-profile; they are mutually exclusive.
mbone-backup[1-3]:mbone-lan-interface	Interface address to a backup MBONE router on a LAN interface. The default is null. Do not set both this parameter and mbone-backup[1-3]:mbone-profile; they are mutually exclusive.
mbone-backup[1-3]:mbone-timeout	Number of seconds elapsed since the last receipt of an IGMP Host Membership Query packet. The router waits for this packet before considering the backup MBONE router to be dead and switching to another backup MBONE. Specify a number from 0 (the default) through 65535. A setting of 0 (zero) disables the mbone-timeout feature.

Displaying Vrouter information

You can now use the `igmp` command to display information about Vrouters.

```
admin> igmp
    usage:  igmp < groups | clients | mbone > [vRouterName]
        command options:
              groups        display active multicast groups
              clients       display multicast clients
              mbone         display MBONE status
              vRouterName   virtual router name for display
```

Note If you do not specify, the command defaults to the main VRouterName.

You can now use the `netstat vrouter -rn` command to display the multicast address entries for the routing table. For example:

```
admin> netstat vrouter -rn
```

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

Support for IGMPv3

TAOS 10.1.0 introduces support for version 3 of the Internet Group Management Protocol (IGMPv3). For a description of TAOS support for IGMPv1 and v2 in previous versions, see the IP chapter of the *APX/MAX TNT Routing and Tunneling Configuration Guide*.

IGMPv3 supports source filtering, that is, the TAOS unit's ability to report interest in receiving packets *only* from specific source addresses or from *all but* specified source addresses, sent to a particular multicast address.

IGMPv3 receivers signal membership to a multicast host group in one of the following modes:

- Include mode—In this mode, the receiver announces membership to a group and provides a list of IP addresses, the *include* list, from which it wants to receive traffic.
- Exclude mode—In this mode, the receiver announces membership to a group and provides a list of IP addresses, the *exclude* list, from which it does not want to receive traffic. This mode indicates that the host wants to receive traffic only from sources other than the ones listed. To receive traffic from all sources, as in the case of the Internet Standard Multicast (ISM) service model, a host expresses *exclude* mode membership with an empty source list. This setting is equivalent to an IGMPv2 Join message.

For more information about IGMPv3, see the IETF draft *draft-ietf-idmr-igmp-v3-09.txt*.

New IGMP query-interval settings

TAOS now includes a new `igmp-options` subprofile in the `ip-interface` and `connection` profiles. You use the `igmp-options` subprofile to configure IGMPv3 settings on WAN and LAN interfaces. Following are listings of the `igmp-options` subprofile, shown with default settings:

```
[in CONNECTION/"":ip-options:igmp-options (new)]
robust-count = 2
query-interval = 125
query-response-interval = 100
last-member-query-interval = 1o
last-member-query-count = 2
igmp-version = v2
```

```
[in IP-INTERFACE/{ { shelf-1 controller 1 } 0 }:igmp-options]
robust-count = 2
query-interval = 125
query-response-interval = 100
last-member-query-interval = 10
last-member-query-count = 2
igmp-version = v2
```

Parameter	Setting
`robust-count`	Robustness of the interface. This parameter enables you to allow for expected packet loss on a subnet. Specify a number from 2 (the default) through 10. Set this parameter to a higher value if you expect a subnet to be lossy.
`query-interval`	Interval, in tenths of seconds, between general queries. Specify a number from 1 through 1024. The default setting is 125.
`query-response-interval`	Response time, in tenths of seconds, for queries sent. Specify a number from 1 through 1024. The default setting is 10.
`last-member-query-interval`	Last member query interval, in tenths of seconds. Specify a value from 1 through 1024. The default setting is 10. A higher value results in an increased time to detect the loss of the last member of a group.
`last-member-query-count`	Last member query count. Specify a number from 1 through 10. The default setting is 2.
`igmp-version`	IGMP version on this interface. Specify one of the following values: v1—IGMP v1 mode v2—IGMP v2 mode v3—IGMP v3 mode

Compatibility with IGMPv1 or IGMPv2

To ensure backward compatibility with IGMPv1 and IGMPv2, the `ip-global:multicast-member-timeout` and `ip-interface:multicast-group-leave-delay` parameters are valid only if the `igmp-querier-mode` parameter for an interface is set to `v2` or `v1`.

If the `igmp-querier-mode` parameter for an interface is set to `v3`, the `ip-interface:multicast-group-leave-delay` and `ip-global:multicast-member-timeout` parameters are not considered for the `GroupMemberTimers` and `LastMemberQueryTimer` values.

Enhancements to the `igmp` command

TAOS 10.1.0 includes the following enhancements to the `igmp` command.

Displaying IGMP settings for an interface

You can now use the new `cliinfo` keyword with the `igmp` command to display information about IGMP settings for an interface. For example, the following command displays the IGMP settings for an interface on the Ethernet-3 slot card:

```
ether3-1/5> igmp cliinfo 1
        Interface#: 1
        Robustness Variable: 2
        Query Interval: 60sec
        Query Response Interval: 10sec
        Last Member Query Count: 2
        Last Member Query Interval: 1sec
        Version: Version 3
        Querier on this i/f: 1.1.1.1
```

If the interface belongs to a virtual router (VRouter), append the name of the VRouter to the `igmp cliinfo` command.

```
ether3-1/5> igmp cliinfo 1 vrtr
        Interface#: 1
        Robustness Variable: 2
        Query Interval: 60
        Query Response Interval: 10
        Last Member Query Count: 2
        Last Member Query Interval: 1
        Version: Version 3
        Querier on this i/f: 1.1.1.1
```

If you enter an invalid interface or VRouter name, the system generates the following sample error message:

```
ether3-1/5> igmp cliinfo 2
No client with i/f# 2 in vrouter 0
```

Displaying source lists and source timers

The output of the `igmp groups` command now shows source lists and the source timers.

Output for a client in include mode

In the following example, a client is subscribed to the group at 224.1.1.1 in include mode and the client's source addresses are 7.7.7.1 and 7.7.7.2.

Following is the output of the igmp groups command from an Ethernet-3 slot card.

```
ether3-1/5> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       00:01:08   0 :: 0 S4INC   7.7.7.1         00:01:08
                                                  7.7.7.2         00:01:08
```

From the shelf controller, the output of the igmp groups command shows groups registered on the Ethernet-3 client card and their sources. Source timers are not needed in this case and are therefore not displayed.

```
admin> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       Slot 1:5                    INC   7.7.7.1
                                                  7.7.7.2
```

From an MBONE interface, the output of the igmp groups command shows the MBONE interface registrations. Source timers do not apply on the MBONE interface and are therefore not shown in the output.

```
ether3-1/12> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       (Mbone)    0 :: 0 S4INC   7.7.7.1
                                                  7.7.7.2
                Slot 1:5                    INC   7.7.7.1
                                                  7.7.7.2
```

Output for a client in exclude mode

In the following example, a client is subscribed to the group at 224.1.1.1 in exclude mode, with sources at 7.7.7.1 and 7.7.7.2.

Following is the output of the igmp groups command from the Ethernet-3 slot card. A source expiration time of 0 on the client card indicates that the sources are blocked.

```
ether3-1/5> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       00:01:08   0 :: 0 S4EXC   7.7.7.1         00:00:00
                                                  7.7.7.2         00:00:00
```

Following is the output of the igmp groups command on the shelf controller. Source timers are not needed in this case and are therefore not included in the output.

```
admin> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       Slot 1:5                    EXC   7.7.7.1
                                                  7.7.7.2
```

The output of the `igmp groups` command on the MBONE interface shows the MBONE interface registrations. The source timers are not valid for MBONE interface and are therefore not included in the output.

```
ether3-1/12> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       (Mbone)    0 :: 0 S4EXC   7.7.7.1
                                                  7.7.7.2
                Slot 1:5                     EXC   7.7.7.1
                                                  7.7.7.2
```

Output for a client with an empty source list

In the following example, a client is subscribed to the group at 224.1.1.1 in exclude mode. The client has an empty source list. An empty source list indicates that all sources are allowed.

From the Ethernet-3 slot card, the output of the `igmp groups` command shows the group registered on the client card.

```
ether3-1/5> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       00:01:08   0 :: 0   S4EXC
```

From the shelf controller, the output of the `igmp groups` command shows group 224.1.1.1 registered with slot 5, in exclude mode, and an empty source list.

```
admin> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       Slot 1:5                     EXC
```

From the MBONE interface, the output of `igmp groups` command shows the registrations on MBONE interface.

```
ether3-1/12> igmp groups
IGMP Group address Routing Table
Group Address   Members Exp-time   Counts   Mode  SrcAddr        SrcExpTime
224.1.1.1       1       (Mbone)    0 :: 0 S4EXC
                Slot 1:5                     EXC
```

Modifications to the `netstat` command

From the shelf controller, the output of the `netstat -s` and the `netstat -s igmp` commands now show the total number of IGMP reports and queries received. The individual totals for IGMPv1, IGMPv2, and IGMPv3 reports and queries are also shown in the output.

```
admin> netstat -s
...
...
        igmp:
                15 packets received
                15 reports received
                2 v1 reports received
                5 v2 reports received
```

```
                8 v3 reports received
                18 query packets received
                1 v1 queries received
                1 v2 queries received
                16 v3 queries received
...
...
admin> netstat -s igmp
        igmp:
                15 packets received
                15 reports received
                2 v1 reports received
                5 v2 reports received
                8 v3 reports received
                18 query packets received
                1 v1 queries received
                1 v2 queries received
                16 v3 queries received
                ...
                ...
```



Note The heartbeat functionality is currently not working with IGMPv3.

Modifications to BGP rules for BGP summarization policies

A Border Gateway Protocol (BGP) route summarization indicates how routing information from a connected or static route is forwarded to a TAOS unit for advertisement to other BGP peers.

You can now use the same policy for several summarizations. If you configure a `bgp-policy` profile with several rules, each rule can have an `if` setting that matches the route prefix in each of several `bgp-summarization` profiles.

Overview of BGP summarizations

You define a BGP summarization as follows:

1. Create a summarization policy for a particular route by means of the `bgp-policy` profile.
2. Apply the policy in the `summarization-policy` parameter of the `bgp-summarization` profile.

(For more information about configuring BGP, see the *APX/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.)

A BGP policy consists of one or more rules. The rules in a policy are actions (`permit`, `deny`, or `include`), followed by conditional statements with an *if* and *then* format. Earlier TAOS versions did not take into account the `if` portion of a rule in a summarization policy and used only the `then` part of the policy to extract the local preference (`lp`), multiexit discriminator (`MED`), and community attributes (`community`) settings.

If a rule in a summarization policy had `if` attributes to be compared, the system ignored that rule and proceeded to the next rule. The system checked the `then` part of a rule only if the rule had no `if` settings.

Using `if` keywords in a rule

In this release, TAOS applies policy rules with `if` settings that include the following keywords:

- `prefix`
- `prefix exactly`
- `prefix-longer-than`

These keywords enable you to create a single summarization policy that has multiple rules corresponding to multiple summarizations.

The system ignores other arguments in the `if` part of a rule, such as `as-path` or `community`, because the `bgp-summarization` profile has no matching parameters to compare them with.



Caution Do not use the `if as-path *` keywords when defining rules for BGP summarization policies. The system ignores a rule for a summarization policy defined with `if as-path` arguments, except when the `as-path` argument is set to an asterisk (`*`). If the `as-path` argument is set to match any series (`as-path *`), the system matches any entry in the autonomous system path sequence, including `none`. Such a check always succeeds and the rule is applied, ignoring any subsequent matching rules.

Upgrading from an earlier release

If an existing rule for a summarization policy has no `if` argument configured, the functionality of the policy remains valid in this release, and you need not make any changes to the summarization policy.

Suppose, however, that an existing summarization policy has a rule with an `if` argument and another rule follows it with no `if` argument. If the first rule matches the prefix of a particular summarization, then the system considers only the first rule for the summarization and ignores the subsequent rules for the summarization as in earlier releases.

Typical summarization policy for multiple summarizations

To use one summarization policy (defined in a single `bgp-policy` profile) for the summarizations defined in several `bgp-summarization` profiles, the summarization policy must include a rule that matches the prefix of each `bgp-summarization` profile.

Suppose you want to summarize routes for the following prefixes:

- 55.55.55.0/16
- 66.66.66.0/24
- 77.77.77.77/8

To do so, create p1, a single summarization policy with the following four rules, and apply it in a summarization for each prefix:

1 *For all summarizations,* deny summarization of all routes with the prefix 110.110.0.0/16.

2 *For the 55.55.55.0/16 summarization,* permit summarization of routes with a prefix of 55.54.0.0/15, and then add a local preference value of 22, an output multiexit discriminator of 222, and a community tag of 2222.

3 *For the 66.66.66.0/24 summarization,* permit summarization of routes that match 66.66.66.0/24 exactly, then add a local preference value of 33, an output multiexit discriminator of 333, and a community tag of 3333.

4 *For the 77.77.77.77/8 summarization,* permit summarization of all routes, then add a local preference value of 44, an output multiexit discriminator of 444, and a community tag of 4444.

Creating summarization policy p1

The following sample commands create bgp-policy profile p1, with rules that apply to each route summarization. A final command restarts BGP to make the system apply the policy.

```
admin> new bgp-policy p1
BGP-POLICY/p1 read
admin> set rule 1 = deny if prefix 110.110.0.0/16
admin> set rule 2 = permit if prefix 55.54.0.0/15 then lp 22 omed 222
community add 2222
admin> set rule 3 = permit if prefix exactly 66.66.66.0/24 then lp 33 omed
333 community add 3333
admin> set rule 4 = permit then lp 44 omed 444 community add 4444
admin> write
BGP-POLICY/p1 written
admin> bgp show policy p1
1 deny
  if prefix 110.110.0.0/16
2 permit
  if prefix 55.54.0.0/15
  then local-pref 22 output-multi-exit-disc 222 community add 0 2222
3 permit
  if prefix exactly 66.66.66.0/24
  then local-pref 33 output-multi-exit-disc 333 community add 0 3333
4 permit
  then local-pref 44 output-multi-exit-disc 444 community add 0 4444
admin> bgp restart
admin> BGP restart complete
```

Creating three summarizations

The following sample commands create a `bgp-summarization` profile for each of the three routes. Each profile applies the single summarization policy `p1`. A final command verifies the summarizations.

```
admin> new bgp-summarization {55.55.55.0/16}
BGP-SUMMARIZATION/{ 55.55.55.0/16 } read

admin> set enable = yes

admin> set summarization-policy = p1

admin> write
BGP-SUMMARIZATION/{ 55.55.55.0/16 } written

admin> new bgp-summarization {66.66.66.0/24}
BGP-SUMMARIZATION/{ 66.66.66.0/24 } read

admin> set enable = yes

admin> set summarization-policy = p1

admin> write
BGP-SUMMARIZATION/{ 66.66.66.0/24 } written

admin> new bgp-summarization {77.77.77.77/8}
BGP-SUMMARIZATION/{ 77.77.77.77/8 } read

admin> set enable = yes

admin> set summarization-policy = p1

admin> write
BGP-SUMMARIZATION/{ 77.77.77.77/8 } written

admin> bgp show summarizations
77.0.0.0/8/C              Init Count of supporting routes:       0
    LP :            44    MED:           444
    CAS: 0/4444/4444
66.66.66.0/24/C           Init Count of supporting routes:       0
    LP :            33    MED:           333
    CAS: 0/3333/3333
55.55.0.0/16/C            Init Count of supporting routes:       0
    LP :            22    MED:           222
    CAS: 0/2222/2222
```

Typical summarization policy with `prefix-longer-than`

You can also use the `prefix-longer-than` argument in the `if` part of the rule to configure different summarizations for similar prefixes of different lengths [?]. In the following example, two `bgp-summarization` profiles use the same summarization `bgp-policy` profile `p2`.

The following sample commands create the policy `p2`:

```
admin> new bgp-policy p2
BGP-POLICY/p2 read

admin> set rule 1 = permit if prefix-longer-than 23 then lp 33 omed 333
community add 3333

admin> set rule 2 = permit if prefix-longer-than 15 then lp 22 omed 222
community add 2222
```

```
admin> write
BGP-POLICY/p2 written
```

When you display the BGP policies, note that the rules address the varying prefix lengths.

```
admin> bgp show policy p2
1 permit
  if prefix-longer-than 23 prefix-length-longer-than 23
  then local-pref 33 output-multi-exit-disc 333 community add 0 3333
2 permit
  if prefix-longer-than 15 prefix-length-longer-than 15
  then local-pref 22 output-multi-exit-disc 222 community add 0 2222

admin> bgp restart
admin> BGP restart complete
```

The following commands create summarizations for the prefixes 55.55.55.0/16 and 55.55.55.0/24 and applies the p2 policy to both. A final command verifies the summarizations.

```
admin> new bgp-summarization {55.55.55.0/16}
BGP-SUMMARIZATION/{ 55.55.55.0/16 } read

admin> set enable = yes

admin> set summarization-policy = p2

admin> write
BGP-SUMMARIZATION/{ 55.55.55.0/16 } written

admin> new bgp-summization {55.55.55.0/24}
BGP-SUMMARIZATION/{ 55.55.55.0/24 } read

admin> set enable = yes

admin> set summarization-policy = p2

admin> write
BGP-SUMMARIZATION/{ 55.55.55.0/24 } written

admin> bgp show summary
55.55.55.0/24/C           Init Count of supporting routes:       0
    LP :            33    MED:           333
    CAS: 0/3333/3333
55.55.0.0/16/C            Init Count of supporting routes:       0
    LP :            22    MED:           222
    CAS: 0/2222/2222
```

Modification to the `bgp show summarization` command

Starting with this release, the output of the `bgp show summarization` command now displays only those summarizations that you have configured using the `bgp-summarization` profile.

Previously, the output also included static and connected route summaries that are automatically created by the system when you configure the parameters `static-route-redist-policy` and `conn-route-redist-policy` in the `bgp-global` profile.

To display summarizations that are automatically generated by the system, you now need to add the `automatic` keyword to the `bgp show summarizaton` command. For example:

```
admin> bgp show summarization automatic
4.4.4.0/24/A              The same Count of supporting routes:       0
    LP :           100    MED:              8
    CAS: not applicable
```

Without the `automatic` keyword, the output of the command displays only summarizations that are created using the `bgp-summarization` profile. For example:

```
admin> bgp show summarization
3.3.0.0/16/C              Bad Count of supporting routes:       0
    LP : none set         MED: none set
    CAS: not set
2.2.8.0/24/C              Bad Count of supporting routes:       0
    LP : none set         MED: none set
    CAS: not set
2.2.7.0/24/C              Bad Count of supporting routes:       0
    LP : none set         MED: none set
    CAS: not set
2.2.6.0/24/C              Bad Count of supporting routes:       0
    LP : none set         MED: none set
    CAS: not set
```

New range for RIP triggered update delay

The range for the parameters `min-rip-trigger-delay` and `max-rip-trigger-delay` in the `ip-global` profile has been increased. The range for both parameters is now 0 to 30 seconds. The value of `max-rip-trigger-delay` must be greater than or equal to the value of `min-rip-trigger-delay`. Lucent recommends choosing `1` (1 second) for the value of `min-rip-trigger-delay and 5` (5 seconds) for the `max-rip-trigger-delay`.

Tunneling features

TAOS 10.1.0 includes the following tunneling features.

Session idle timer enhancements for layer 2 tunneling

This enhancement enables generic call filters to be applied to PPP frames that are transported by Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP). Consequently, the unit ignores certain frames for session-idle-timer calculations.

Use generic call filters on the network access server side (L2F), L2TP access concentrator side, or PPTP access concentrator side of the tunnel. The unit applies the generic filter to the carried PPP frames, consequently ignoring certain frames for session-idle-timer calculations. When a frame matches a filter rule, the filter control "drop" prevents the frame from affecting the session idle timer.

The intent of this enhancement was to prevent LCP echo Request packets from keeping an L2TP, L2F, or PPTP session active even though no user data is being transferred. This enhancement uses generic call filters, however, so it can be applied to other packet types.



Note This enhancement applies only to the network access server side (L2F), L2TP access concentrator side, or PPTP access concentrator side of the tunnel.

The following example of a local filter profile shows how to set up the filters to ensure the session idle timer is unchanged by LCP Echo Request packets. The filter drops LCP ECHO REQUEST (C0 21 09) and LCP ECHO REPLY (C0 21 0A), so that the idle time does not reset.

```
admin> new filter lcp-echo
FILTER/lcp-echo read
admin> set input 1 valid = yes
admin> set input 1 forward = no
admin> set input 1 type = generic-filter
admin> set input 1 generic-filter offset = 0
admin> set input 1 generic-filter len = 5
admin> set input 1 generic-filter more = no
admin> set input 1 generic-filter comp-neq = no
admin> set input 1 generic-filter mask = ff:ff:ff:ff:ff:00:00:00:00:00:00:00
admin> set input 1 generic-filter value =
ff:03:c0:21:0a:00:00:00:00:00:00:00

admin> set input 2 valid = yes
admin> set input 2 forward = no
admin> set input 2 type = generic-filter
admin> set input 2 generic-filter offset = 0
admin> set input 2 generic-filter len = 3
admin> set input 2 generic-filter more = no
admin> set input 2 generic-filter comp-neq = no
admin> set input 2 generic-filter mask = ff:ff:ff:00:00:00:00:00:00:00:00:00
admin> set input 2 generic-filter value =
c0:21:09:00:00:00:00:00:00:00:00:00

admin> set input 3 valid = yes
admin> set input 3 forward = no
admin> set input 3 type = generic-filter
admin> set input 3 generic-filter offset = 0
admin> set input 3 generic-filter len = 3
admin> set input 3 generic-filter more = no
admin> set input 3 generic-filter comp-neq = no
admin> set input 3 generic-filter mask = ff:ff:ff:00:00:00:00:00:00:00:00:00
```

```
admin> set input 3 generic-filter value =
c0:21:0a:00:00:00:00:00:00:00:00

admin> set input 4 valid = yes
admin> set input 4 forward = yes
admin> set input 4 type = generic-filter
admin> set input 4 generic-filter offset = 0
admin> set input 4 generic-filter len = 0
admin> set input 4 generic-filter more = no
admin> set input 4 generic-filter comp-neq = no
admin> set input 4 generic-filter mask = 00:00:00:00:00:00:00:00:00:00:00:00
admin> set input 4 generic-filter value =
00:00:00:00:00:00:00:00:00:00:00:00

admin> set output 1 valid = yes
admin> set output 1 forward = no
admin> set output 1 type = generic-filter
admin> set output 1 generic-filter offset = 0
admin> set output 1 generic-filter len = 5
admin> set output 1 generic-filter more = no
admin> set output 1 generic-filter comp-neq = no
admin> set output 1 generic-filter mask =
ff:ff:ff:ff:ff:00:00:00:00:00:00:00
admin> set output 1 generic-filter value =
ff:03:c0:21:09:00:00:00:00:00:00:00

admin> set output 2 valid = yes
admin> set output 2 forward = no
admin> set output 2 type = generic-filter
admin> set output 2 generic-filter offset = 0
admin> set output 2 generic-filter len = 5
admin> set output 2 generic-filter more = no
admin> set output 2 generic-filter comp-neq = no
admin> set output 2 generic-filter mask =
ff:ff:ff:ff:ff:00:00:00:00:00:00:00
admin> set output 2 generic-filter value =
ff:03:c0:21:0a:00:00:00:00:00:00:00

admin> set output 3 valid = yes
admin> set output 3 forward = no
admin> set output 3 type = generic-filter
admin> set output 3 generic-filter offset = 0
```

```
admin> set output 3 generic-filter len = 3
admin> set output 3 generic-filter more = no
admin> set output 3 generic-filter comp-neq = no
admin> set output 3 generic-filter mask = ff:ff:ff:0:00:00:00:00:00:00:00:00
admin> set output 3 generic-filter value =
co:21:09:00:00:00:00:00:00:00:00:00

admin> set output 4 valid = yes
admin> set output 4 forward = no
admin> set output 4 type = generic-filter
admin> set output 4 generic-filter offset = 0
admin> set output 4 generic-filter len = 3
admin> set output 4 generic-filter more = no
admin> set output 4 generic-filter comp-neq = no
admin> set output 4 generic-filter mask = ff:ff:ff:0:00:00:00:00:00:00:00:00
admin> set output 4 generic-filter value =
co:21:0a:00:00:00:00:00:00:00:00:00

admin> set output 3 valid = yes
admin> set output 3 forward = yes
admin> set output 3 type = generic-filter
admin> set output 3 generic-filter offset = 0
admin> set output 3 generic-filter len = 0
admin> set output 3 generic-filter more = no
admin> set output 3 generic-filter comp-neq = no
admin> set output 3 generic-filter mask = 00:00:00:0:00:00:00:00:00:00:00:00
admin> set output 3 generic-filter value =
00:00:00:00:00:00:00:00:00:00:00:00
admin> write
FILTER/lcp-echo written
```

Following is the comparable RADIUS profile:

Note The filters "generic in forward 0 0 0" and "generic out forward 0 0 0" are mandatory because the default behavior (when filters exist and there is no match) is to drop the packets.

```
# LCP ECHO REQUEST/REPLY, Address-and-Control-Field-Compression (ACFC) disabled
Ascend-Call-Filter = "generic in drop 0 fffffffff ff03c02109"
Ascend-Call-Filter = "generic in drop 0 fffffffff ff03c0210a"
# LCP ECHO REQUEST/REPLY, Address-and-Control-Field-Compression (ACFC) enabled
Ascend-Call-Filter = "generic in drop 0 ffffff c02109"
Ascend-Call-Filter = "generic in drop 0 ffffff c0210a"
# Everything else is user data
Ascend-Call-Filter = "generic in forward 0 0 0"
# LCP ECHO REQUEST/REPLY, Address-and-Control-Field-Compression (ACFC) disabled
```

```
Ascend-Call-Filter = "generic out drop 0 ffffffffff ff03c02109"
Ascend-Call-Filter = "generic out drop 0 ffffffffff ff03c0210a"
# LCP ECHO REQUEST/REPLY, Address-and-Control-Field-Compression (ACFC) enabled
Ascend-Call-Filter = "generic out drop 0 ffffff c02109"
Ascend-Call-Filter = "generic out drop 0 ffffff c0210a"
# Everything else is user data
Ascend-Call-Filter = "generic out forward 0 0 0"
```

Configurable L2TP hello packet policy

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

In previous software releases, you could disable the system's sending of Hello messages or configure the unit to always send them after the period specified by the `hello-timer` parameter in the `l2-tunnel-global:l2tp-config` subprofile. However, because the receipt of an L2TP control or data packet from a remote peer indicates that the remote L2TP system is alive, the system need not send Hello messages if it is receiving control or data packets.

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

New `hello-packet-policy` parameter

A new parameter in the `l2-tunnel-global:l2tp-config` subprofile, `hello-packet-policy`, specifies whether a TAOS unit's sending of L2TP Hello messages to its peer is based on an inactive control channel or inactive control *and* data channels. You can set this parameter to one of the following values:

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

Changes to the `hello-packet-policy` parameter take effect after the period specified by the `hello-timer` parameter. The `hello-packet-policy` parameter is not applicable if L2TP is not active on the unit.

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

Sample configuration

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

```
admin> read l2-tunnel-global
L2-TUNNEL-GLOBAL read
```

```
admin> set l2tp-mode = lac
admin> set l2tp-config hello-packet-policy = no-activity
admin> set l2tp-config hello-timer = 15
admin> write -f
L2-TUNNEL-GLOBAL written
```

New L2TP diagnostic commands

With previous software versions, the `l2tpstart` and `l2tpstop` commands were protected in the debug environment. With this software version, these commands have been made accessible to administrators as diagnostic-level commands on all host slot cards.

To use these commands, you must first open a session with a host card. For example, the following command opens a session with a MultiDSP card in slot 2:

```
admin> open 1 2
madd-1/2>
```

When the session to a card is open, the prompt changes to reflect your current location. To quit the session and return to the main system prompt, use the `quit` command. For example:

```
madd-1/2> quit
admin>
```

`l2tpstart` command

The `l2tpstart` command starts an L2TP tunnel to a remote L2TP peer. It is typically used to verify basic tunnel configuration without having to place a call. In most cases, because the tunnel does not have any calls, the tunnel is deactivated automatically after a short amount of time. This command is available only on host slot cards.

The syntax for the command is as follows:

```
l2tpstart [-r vrouterName] server [password]
```

Syntax element	Description
`-r` *vrouterName*	Specifies the vrouter where the tunnel will be established. The default is the main vrouter.
`server`	The remote server's IP address. It can be either a dotted IP address (for example, 1.2.3.4) or a fully qualified domain name (for example, lns.example.com).
`password`	The tunnel password for L2TP authentication. The default is no password.

For example, the following command opens a tunnel to the specified LNS host address:

```
madd-1/2> l2tpstart 1.2.3.4 tnl-pwd
   L2TPCM: Connecting to host 1.2.3.4, VR='main' (0), password 'tnl-pwd'
```

To find out if the tunnel came up, use the `l2tp` command, or monitor `syslog` output for a message such as the following:

```
LOG info, Shelf 1, Controller, Time: 18:46:21--
   TUNNEL-1, L2TP Control Channel up with my-lns
```

`l2tpstop` command

The `l2tpstop` command deactivates an L2TP tunnel connected to a remote L2TP peer. All the calls that were using the tunnel are disconnected. The syntax for the command is as follows:

`l2tpstop` *`sessionID`*

Syntax element	Description
`sessionID`	The session ID of the tunnel. The number can be obtained using the `l2tp` command from the shelf controller or the `l2tpsessions` command on the host slot card.

For example, the following command on a MultiDSP card displays session information about an L2TP tunnel with session ID 2:

```
madd-1/2> l2tpsessions
   SessionID 2, peerTunnelID 4, peerAddress [1.2.3.4:1701]
   State: Up, Pending Calls? No, controlSlot: Yes[5]
   Peer name 'my-lns', Vendor 'Ascend', L2TP Protocol Ver 1.0
   Peers RX Win 4, FW Rev 0x0010, Bearer Cap 0x03, Framing Cap 0x03,    MOH-
capable
   Client name (local) 'apx', Server name (peer) 'my-lns'
   Server-Endpoint '1.2.3.4'
```

The following command closes the L2TP tunnel:

```
madd-1/2> l2tpstop 2
   L2TPCM-2: stopping, RC=6, EC=0, msg='Admin'
```

New L2TP attribute-value pairs

TAOS 10.1.0 includes support for the following new L2TP attribute-value pairs (AVPs):

- Physical channel ID (38)—The Physical channel ID attribute value contains the same value as the NAS-Port RADIUS attribute reported by the L2TP access concentrator (LAC).
- Q.931 Cause Code (12)

These AVPs are optional and encoded as defined in RFC 2661, *Layer Two Tunneling Protocol "L2TP"*.

V.92 MOH signaling over L2TP

In previous software versions, V.92 modem-on-hold (MOH) was supported across L2TP tunnels. However, the L2TP base protocol does not provide a way for the L2TP access concentrator (LAC), where the modem is connected, to inform the L2TP network server (LNS), where the PPP session is handled, that a modem link is on hold.

With this software version, a mechanism has been added to inform the LNS that the client modem has put a call on hold. The details of this mechanism are described in the Internet Engineering Task Force (IETF) draft entitled *Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP)*. For this mechanism to operate, the TAOS 10.1 Premium Feature Set license must be enabled in the system.

When the LNS is a MAX® 6000 unit, the LNS saves the current progress code when it receives an indication that the client modem went on hold. When the MAX® LNS receives an indication that the client modem returned online, it restores the progress code it saved previously. If the call disconnects while on hold, the MAX® LNS reports a progress code of `PR_MODEM_ONHOLD (34)`. No other action related to V.92 MOH is taken by the LNS.

Configurable sending of LCP Configure Request message

For incoming clients calls that are not authenticated with Point-to-Point Protocol (PPP) authentication, the L2TP access concentrator (LAC) must sometimes inject a dummy Link Control Protocol (LCP) Configure Request into the data stream destined for incoming client calls to restart PPP negotiations that otherwise would be stuck for a full LCP timeout. Proxy LCP makes this dummy LCP packet unnecessary.

You can now control whether the TAOS unit sends this dummy LCP Config Request packet for incoming calls that are not authenticated with a PPP authentication.

By default, the TAOS unit does not send this dummy LCP packet because the L2TP network server (LNS) should be able to restart the PPP negotiations with the proxy LCP information sent by the TAOS unit on the Incoming Call-Request (ICRQ) message. In previous software releases, the default behavior was to send a dummy LCP packet.

To configure the TAOS unit to inject a dummy LCP Configure Request message into the data stream destined for incoming client calls, set the new `inject-dummy-lcp-config-request` parameter in the `l2-tunnel-global:l2tp-config` to `yes`. For example:

```
admin> read l2-tunnel-config
L2-TUNNEL-CONFIG read

admin> set l2tp-config inject-dummy-lcp-config-request = yes

admin> write -f
L2-TUNNEL-CONFIG read
```

Disabling IP-in-IP decapsulation

With TAOS 10.1.0, you can now disable IP-in-IP decapsulation on TAOS units. In previous software releases, if the IP-in-IP software license was enabled for your unit, you could not disable IP-in-IP decapsulation, and any IP-in-IP packet received by your TAOS unit addressed to a local IP address was decapsulated.

New `decapsulation-enable` parameter

To disable IP-in-IP decapsulation, set the new `decapsulation-enable` parameter in the `ip-global:ipinip-options` subprofile to `yes`. By default, the `decapsulation-enable` parameter is set to `no`. The following sample commands enable IP-in-IP decapsulation on a TAOS unit:

```
admin> read ip-global
IP-GLOBAL read

admin> set ipinip-options decapsulation-enable = yes

admin> write
IP-GLOBAL written
```

The `decapsulation-enable` parameter is applicable only if the IP-in-IP software license is enabled for your unit. The software license is enabled for your unit if the `ipinip-enabled` parameter in the `base` profile is set to `enabled`, as in the following example:

```
admin> get base ipinip-enabled
[in BASE:ipinip-enabled]
ipinip-enabled = enabled
```

Upgrading issues

By default, IP-in-IP decapsulation is disabled in TAOS 10.1.0. If you are upgrading from an earlier software version, and IP-in-IP was enabled for your system, you must set the `decapsulation-enable` parameter to `yes`.

System administration features

TAOS 10.1 includes the following features for system administration.

Secure shell (`ssh`) for administrative access

The secure shell (`ssh`) is a software-based approach to network security. It is a de facto standard for protected remote logins. The `ssh` program enables you to log securely into another computer over a network, to enter commands on a remote machine, and to move files from one machine to another. It can replace `telnet`, `rlogin`, and `rsh` applications.

The `ssh` program provides strong authentication, encryption, and secure communications over unsecure channels, for secure administrative access to a TAOS unit from a UNIX system. Up to five simultaneous `ssh` connections can be established with any one server. Subsequent connection attempts are refused.



Note Lucent recommends that you use ssh only for administrative access to a TAOS unit.

The ssh program provides the following features:

- Data Encryption Standard (DES) and Triple Data Encryption Standard-cypher block chaining (3DES-CBC) encryption types.
- Authentication by means of the username and password in the TAOS user profile. (RADIUS authentication is not supported.)
- exec shell requests.



Note For the TAOS unit to use ssh, the gateway must be licensed with the 10.1 Premium Feature Set.

TAOS ssh implementation

You configure the ssh daemon using the new ssh-server-config profile.

When the ssh daemon is running, you can log into a TAOS unit from a UNIX system using the UNIX ssh command. For example, the following command entered on a UNIX system initiates an ssh login, using DES encryption and authenticating the admin user profile, to a TAOS unit at 1.1.1.1:

```
ssh -x -c des -l admin 1.1.1.1
```

You can verify that the TAOS ssh daemon is running by checking netstat command output.

Overview of the ssh-server-config profile

Following is a listing of the new ssh-server-config profile. Parameters are shown with their default values.

```
[in SSH-SERVER-CONFIG]
ssh-enabled = no
ssh-version = ssh-version-1
server-key-size = 768
server-key-regeneration-interval = 3600
login-grace-time = 300
authentication-type = password-authentication
allow-empty-passwords = no
```

You can set the following parameters:

Parameter	Setting
ssh-enabled	Enable/disable the ssh feature. To enable ssh, specify yes. The default is no. After changing the value of the ssh-enabled parameter, you need to reset the gateway.
ssh-version	Version of the protocol ssh uses. Currently, only ssh-version-1 is supported.

`server-key-size`	Size of the server key generated at the interval specified by `server-key-regeneration-interval`. Specify a number from `512` through `896`. The default is `768`. No special authorization is required to modify this parameter.
`server-key-regeneration-interval`	Interval (in seconds) in which the server key is regenerated. A change in this value is reflected the next time the server key is generated. Specify a number from `3600` through `7200`. The default is `3600`. No special authorization is required to modify this parameter.
`login-grace-time`	Time (in seconds) in which login must be complete once authentication starts. Specify a number from `0` through `600`. The default is `300`. No special authorization is required to modify this parameter.
`authentication-type`	Type of authentication for the `ssh` session. Currently, only `password-authentication` is supported.
`allow-empty-passwords`	Determines whether an empty password is allowed for `ssh` authentication. If you specify `yes`, be aware that the unit cannot ensure a safe connection. The default is `no`.

Secure shell considerations

Consider the following:

- When you change the value of the `ssh-enabled` parameter, you must restart the gateway for the new setting to take effect.
- If the Premium Feature Set license is disabled, the host key is cleared and the `ssh-enabled` parameter is reset to the default value of `no`. If the license is enabled again at a later date, a new host key is generated.



Note The host key is generated after the 10.1 Premium Feature Set license has been enabled. The `host-key` and `host-key-length` TAOS parameters are read-only and are visible in the `ssh-server-config profile` only when debug mode is on.

- When the Premium Feature Set license is enabled, `ssh` is also enabled. However, if the license is then disabled, the gateway restarts.
- The following `syslog` message is displayed the first time the gateway is rebooted after the TAOS 10.1 Premium Feature Set license is disabled, when `ssh` has been enabled, or when the host key is generated after the Premium Feature Set license has been enabled:

  ```
  SSHD: SSH disabled and Host Key cleared, as 10.1 Premium Feature Set is
  disabled.
  ```

Secure shell `syslog` messages

The following `ssh`-related `syslog` messages indicate an error condition:

`syslog` message	Event that generated `syslog` message
SSHD: Server Key Load info failed	Unit failed to load server-key information.
`SSHD: SSHD_HOST_KEY_IMPORT failed`	Unit failed to import a host key from NVRAM.
`SSHD: SSHD_HOST_KEY_GENERATE.. SSH abort`	Unit failed to generate a host key.
`SSHD: SSHD_HOST_KEY_EXPORT.. SSH abort`	Unit failed to export a host key to NVRAM.
`SSHD: SSHD_HOST_KEY_LOAD.. SSH abort`	Unit failed to load a host key.

Group permissions

In this release, you can create a centralized definition of the TAOS commands that a group of users can perform, and associate individual users with a command user group. To use this functionality, the 10.1 Premium Feature Set license must be enabled on your unit.

Configuring parameters in the new `user-group` profile

The new `user-group` profile enables you to define command access for all the users you specify. You can specify access settings and a list of up to 512 commands that users in the command user group have permission to use. To define a command user group, specify the following parameters in the `user-group` profile:

Parameter	Setting
`name`	Name of a command user group. You can specify up to 23 characters. The default is null.
`allow-termserv`	Enable/disable permission for the users in the group to use terminal-server commands. ■ `yes` specifies that users have terminal-server permission. ■ `no` (the default) specifies that users do not have terminal-server permission.
`allow-system`	Enable/disable permission for the users in the group to use system-level commands. ■ `yes` specifies that users have system-level permission. ■ `no` (the default) specifies that users do not have system-level permission.

Parameter	Setting
`allow-diagnostic`	Enable/disable permission for the users in the group to use diagnostic-level commands. ■ `yes` specifies that users have diagnostic-level permission. ■ `no` (the default) specifies that users do not have diagnostic-level permission.
`allow-update`	Enable/disable permission for the users in the group to use update-level commands. ■ `yes` specifies that users have update-level permission. ■ `no` (the default) specifies that users do not have update-level permission.
`allow-password`	Enable/disable permission for the users in the group to view passwords. ■ `yes` specifies that users can view passwords. ■ `no` (the default) specifies that users cannot view passwords.
`allow-code`	Enable/disable permission for the users in the group to use code-level commands. ■ `yes` specifies that users have code-level permission. ■ `no` (the default) specifies that users do not have code-level permission.
`exclude-listed-commands`	Enable/disable permission for the users in the group to use the commands designated by the `command` parameter. ■ `yes` specifies that the users do not have permission to use the designated commands. ■ `no` (the default) specifies that the users have permission to use the designated commands.
`command [`*n*`]`	Commands to allow or exclude.

When you change the `user-group` settings, the permissions of the associated users are automatically adjusted. If a `user-group` profile is deleted, the sessions of all the associated users are terminated.

Configuring new parameters in the user profile

Following are the new parameters you can set in the user profile:

Parameter	Setting
user-group	Name of a user-group profile. The default is null. If the user-group parameter refers to a valid user-group profile, the access settings of the user-group profile are applied to the user session, overriding those in the user profile. If the user-group profile cannot be found, the user cannot log on or perform any commands. If no user-group profile is specified in the user profile, the access settings in the user profile apply.
use-group-permissions	Enable/disable the user's access to all the allow-*xxx* settings in the user-group profile specified by the user-group parameter. ■ yes specifies that the user has access to all commands permitted by the allow-*xxx* setting in the user-group profile, and that the allow-*xxx* settings in the user profile are ignored. ■ no (the default) specifies that the user does not have access to the commands permitted by the allow-*xxx* settings in the user-group profile, and that only the commands permitted by the allow-*xxx* settings in the user profile apply.

Using the new userGroupCheck command

The unit does not prohibit you from entering a command user group or a user that does not exist, nor from entering an invalid list of commands. To verify that your specifications are valid, you can use the new userGroupCheck command. Following is the userGroupCheck syntax:

```
userGroupCheck [-u user|-g group] [-a]
```

Command element	Description
-u *user*	Verify the user-group profile specified by the user-group parameter in the user profile called *user*, and display the commands to which *user* has access.
-g *group*	Verify that the user-group profile specified by *group* specifies a valid list of commands. If the command user group contains commands that are valid on a slot card, this option displays the commands.
-a	Verify that all user-group profiles specify valid lists of commands, and that all user-group profiles specified by user profiles are valid.

For example, to verify the `user-group` profile specified in the `user` profile called `bill`:

```
admin> usergroupcheck -u bill
Group provisioning: Commands all valid.
Commands available to this user are:
     ?                              ( user )
     auth                           ( user )
     clear                          ( user )
     date                           ( user )
     delete                         ( update )
     dtunnel                        ( user )
     filtcache                      ( user )
     get                            ( system )
     gre                            ( user )
     grep                           ( user )
     help                           ( user )
     l2tp                           ( user )
     l2tpcards                      ( user )
     l2tpsessions                   ( user )
     l2tptunnels                    ( user )
     list                           ( system )
     netware                        ( user )
     new                            ( system )
     prtcache                       ( user )
     quit                           ( user )
     whoami                         ( user )
     write                          ( update )
```

To verify that the `newyork` command user group contains a valid list of commands:

```
admin> usergroupcheck -g newyork
Group provisioning commands all valid
```

To verify that all `user-group` profiles specify valid lists of commands, and that all `user-group` profiles specified by `user` profiles are valid:

```
admin> usergroupcheck -a
All groups and users verified
```

Sample command user group configuration

In this example, the user `bill` is given permission to use the six commands that he needs to provision new users. The user `ted` can use all the TAOS commands except `reset`, `slot`, and `read`:

```
admin> new user bill
admin> set password = neo
admin> set user-group = provisioning
admin> write -f
admin> new user-group provisioning
admin> set use-group-permissions = yes
admin> set command 1 = new
admin> set command 2 = list
```

```
admin> set command 3 = delete
admin> set command 4 = write
admin> set command 5 = get
admin> set command 6 = auth
admin> write -f

admin> new user ted
admin> set password = esq
admin> set allow-update = yes
admin> set allow-system = yes
admin> set allow-termserv = yes
admin> set allow-diagnostic = yes
admin> set allow-password = yes
admin> set allow-code = yes
admin> set user-group = maintenance
admin> write -f

admin> new user-group maintenance
admin> set exclude-listed-commands = yes
admin> set command 1 = reset
admin> set command 2 = slot
admin> set command 3 = read
admin> write -f
```

Extra levels of security

Certain command options have extra levels of security restricting access beyond that of standard commands, and these security levels cannot be bypassed by means of the `user-group` profile. For example, the standard `arptable` command displays the contents of the ARP cache, and is protected by the `system` level in both the `user` and `user-group` profiles. In addition, the option to add entries to the table is protected by the `diagnostic` or `update` level. As a result, allowing a command user group access to the `arptable` command by designating it with the `command` parameter does not allow members of the group to add entries to the ARP cache, unless the group or any of its users is granted access to system, diagnostic, and update commands.

Following are other commands and options that have additional levels of security:

- `arptable -a`—Protected by update or diagnostic permission.
- `arptable -d`—Protected by update or diagnostic permission.
- `arptable -f`—Protected by update or diagnostic permission.
- `loadmate`—Protected by debug and code permissions.
- `filtcache -f`—Protected by update or diagnostic permission.
- `prtcache -f`—Protected by update or diagnostic permission.

- `resrcmgr -t`—Protected by diagnostic permission.

When used to restore configurations, the `load` command also requires the use of the `new`, `set`, and `write` commands, because the device runs these commands in the process of loading the configuration.

New options to the `userstat` command

This release implements three new options that enable you to terminate one or more sessions by means of the `userstat` command. Following are the new options:

Command element	Description
`-k all`	Terminate all sessions.
`-k range` *`prefix begin end`*	Terminate sessions of all users within a specified range of usernames that begin with the same prefix.
`-k ip` *`ipaddr`*	Terminate an individual session specified by an IP address.

To terminate all user sessions, specify `userstat` with the `-k all` option. For example, if 35 user sessions are established and you want to terminate them all, specify the following:

```
admin> userstat -k all
35 Sessions cleared
```

To terminate sessions on the basis of usernames, specify `userstat` with the `-k range` option. For example, to terminate sessions for all users from `test100` through `test200`, specify the following:

```
admin> userstat -k range test 100 200
101 Sessions are cleared.
```

To terminate a session associated with a particular IP address, specify `userstat` with the `-k ip` option. For example, to terminate a session for the user at IP address 10.10.10.10, specify the following:

```
admin> userstat -k ip 10.10.10.10
Cleared Session with IP 10.10.10.10
```

If you specify an invalid session ID, the system generates the following message:

```
Session invalid-session-id does not exist
```

Displaying T1 or E1 performance monitoring statistics

In TAOS 10.1, the new command `fdlstat` displays the extended superframe format (ESF) performance statistics for the facility data link (FDL) for each T1 or E1 interface. The display can show data for all T1 or E1 interfaces in a TAOS unit, for a specific slot card only, or for a single specific channel.

The syntax for the fdlstat command is as follows:

```
fdlstat [ [ -all ] | [ shelf ] [ slot ] item ]
```

Command element	Description
-all	Show information about all T1 or E1 interfaces.
shelf	When used, always use a value of one (1).
slot	Optionally specify the slot number of the T1 or E1 interface.
item	Optionally specify the line (item) number of the T1 or E1 interface in a specified slot.

The following sample command shows ESF performance statistics for the card in slot 6:

```
admin> fdlstat 1 6
         Address    es   uas   ses   bes    lofc   css
         1/06/01     0     0     0     0       0     0
         1/06/02    19     0     0     0       0    19
         1/06/03    19     0     0     0       0    19
         1/06/04     0     0     0     0       0     0
         1/06/05     0     0     0     0       0     0
         1/06/06     0     0     0     0       0     0
         1/06/07     0     0     0     0       0     0
         1/06/08     0     0     0     0       0     0
```

Field	Description
es	Errored seconds.
uas	Unavailable seconds.
ses	Severely errored seconds.
bes	Bursty errored seconds.
lofc	Loss of frame count.
css	Controlled slip seconds.

Support for the who command

This release includes support for the who command. The who command displays information about or disconnects administrative users. The syntax of the command is as follows:

```
who [am i ]|[-k username IPaddress]
```

Displaying administrative users

Without any arguments, the output of the command displays names of administrative users, user profiles, and IP addresses of administrative users from Telnet sessions. An asterisk (*) denotes the current session. For example:

```
admin> who
      user       profile    from
                            console
   * admin       admin      198.4.92.5
     josh        admin      198.4.92.5
```

Displaying the current user

To display the current user and user profile for an administrative session, use the who am i command. The output of this command is similar to the existing whoami command. For example:

```
admin> who am i
User Name : admin       User Profile : admin
```

Disconnecting administrative sessions

To disconnect an administrative session, use the -k option with the who command. For example, the following command disconnects the user josh logged in from IP address 135.254.96.37:

```
admin> who -k josh 198.4.92.5
   LOG critical, Shelf 1, Controller, Time: 00:02:16--
     user admin from 198.4.92.5 disconnected user josh from 198.4.92.5
   1 administrative users killed
```

The preceding command disconnects all sessions with the user name josh logged in from IP address 135.254.96.7.

You cannot use the who -k command to disconnect the current session or a session from the console if for its serial port the user-profile parameter in the serial profile is set to a value other than null.

Fatal error logs, code load error messages, and terminal server diplays

Fatal error logs, code load error messages, and the terminal server user display now report the name the user used to log in, not the user profile of the administrative user.

In the following sample output, the externally authenticated user josh caused the following fatal error to be logged:

```
SLOT CARD BOUNCED:  Index: 220  Revision: 10.1b0e0  Slot 1/2
        Date: 08/16/2002.       Time: 00:22:51
        Card bounced by 198.4.92.5, user profile josh.
```

Administering Primary Rate Interface (PRI) layer 2 timers

Two timers are now available for fine-tuning the interface to match the local Primary Rate Interface (PRI) variants. These timers are defined for Layer 2 in Integrated Services Digital Network (ISDN):

- T200
- T203

New `t200-timer` and `t203-timer` parameters

To configure the PRI layer 2 timers, set the `t200-timer` and the `t203-timer` parameters, which are located in the `line-interface` sub-profile of a T1 or E1 profile:

```
admin> read e1 { 1 1 1 }
E1/{ shelf-1 slot-1 1 } read

admin> list line
[in E1/{ shelf-1 slot-1 1 }:line-interface]
enabled = yes
t-online-type=none
       .
       .
admin> set t200-timer = 3000

admin> write
E1/{ shelf-1 slot-1 1 } written
```

Parameter	Setting
`t200-timer`	Maximum number of milliseconds (from 100 through 10000) to wait between transmission and acknowledgement of a Link Access Procedure on D (LAPD) LAPD frame. Default is 1085 on an ETSI compliant E1 system; 1000 on a 1TR6/ETSI compliant T1 system; 2000 on any other system.
`t203-timer`	Maximum number of milliseconds (from 1000 through 300000) to wait without receiving an LAPD frame. Default is 10000 if the line's default switch type is as per the Q.921 ETSI or 1TR6 standards, or to 30000 if it is not. This value is as per the AT&T 5ESS standard and the 1998 NI PRI CPE Guidelines.

Specifying whether to log L2TP `syslog` messages

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

The `log` profile contains a new parameter called `log-tunnel-progress`, which enables and disables transmission of the messages to `syslog`. If you specify `yes` (the default),

L2TP `syslog` messages are sent to the `syslog` server. When an L2TP tunnel is established, messages in the following format are sent:

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

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

When the tunnel is deactivated, L2TP messages in the following format are sent:

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

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

Fatal index 388 introduced and fatal index 66 discontinued

This release introduces fatal index 388 and discontinues fatal index 66.

On APX units with dual controllers, the system now displays the following message to the console to report the resetting of a controller because it is yet not ready to takeover as primary:

```
Controller not ready to takeover, will reset.
        Please stand by. System reset in progress...
```

Following is the a sample of a fatal log recorded with fatal index 388:

```
S/W OVER NOT RDY:  Index: 388  Revision: 10.1.0 right-controller (apxsr)
        Date: 05/27/2002.       Time: 04:38:46
        Controller reset due to failover before it is ready to takeover as
primary.
```

Fatal index 66 is no longer reported in TAOS 10.1.0.

Modifications to the `slrt` and `netstat` commands

This release includes changes to the `slrt` and `netstat` commands.

New `-rp` option for the `slrt` command

This release introduces the `-rp` option to the `slrt` command. On slot cards that support routing tables, the `-rp` option display the slot's routing entries that match a particular IP prefix. This option works like the `-p` option of the `netstat` command.

Output of the -p option displays the total number of matched entries

The system now prints the total number of matched entries when you specify the `-p` option for with the `netstat` and `slrt` commands.

Following is a sample output from an Ethernet-3 slot card:

```
ether3-1/3> slrt -rp 110.110.110
Destination         Gateway         Sh:Sl  Flg   Use Cnt
110.110.110.0/24    -                1:3                0
110.110.110.2/32    -                1:17  L            0
Total matched entries = 2
```

```
ether3-1/3> slrt -rp 110.110.110.2
Destination         Gateway         Sh:Sl  Flg   Use Cnt
110.110.110.2/32    -                1:17  L            0

Total matched entries = 1
```

From the shelf controller, following is a sample output of the `netsat -rnp` command :

```
admin> nets -rnp 110.110.110
Destination       Gateway        IF         Flg   Pref Met     Use       Age
110.110.110.0/24   -             ie1-3-1     C        0   0       0      3836
110.110.110.2/32   -             local       CP       0   0       0      3836
Total matched entries = 2
```

Changes to the behavior of `netstat -rn` and `slrt -r` commands

In this release, if you issue the `netstat -rn` and `slrt -r` commands and the system has insufficient memory to print the entire routing table, it generates a notice about the insufficient memory. Also, the system now generates an accurate count of the total number of entries in the routing table. Previously, the count was inaccurate when the system ran out of memory. (The option to print a partial list of the routing table by specifying the `-p` option is still available in this release.)

Following is sample output of a `netstat -rn` command entered from the shelf controller when the system has insufficient memory:

```
admin> netsat -rn
Insufficient memory to display routing entries
Total Routes  = 61508   Hidden Routes = 0
```

Following is sample output of an `slrt -r` command entered from an Ethernet-3 slot card when the system has insufficient memory:

```
ether3-1/3> slrt -r
Insufficient memory to display routing entries

Total Routes = 32248
```

New `boot-version` profile

The parameters `boot-sr-version` and `jam-file-components` have been moved from the `system` profile to a new `boot-version` profile. Following is a sample listing of the read-only `boot-version` profile:

```
[in BOOT-VERSION]
boot-sr-version = 10.1b0c4
jam-file-components = { 6305_0005_003_12june2001c.sof 6305_0006_003_14may2+
```

Following is a sample listing of the read-only `jam-file-components` subprofile.

```
[in BOOT-VERSION:jam-file-components]
jam-file-1 = 6305_0005_003_12june2001c.sof
jam-file-2 = 6305_0006_003_14may2001.sof
jam-file-3 = 6305_0005_003_12june2001c.sof
jam-file-4 = -
jam-file-5 = -
```

```
jam-file-6 = -
```

Parameter	Setting
boot-sr-version	Read-only parameter containing the version number of the boot loader used by the shelf controller.
jam-file-components	A read-only subprofile containing 6 parameters, jam-file-1 through jam-file-6. This subprofile is valid for the APX 8100 only.
jam-file-N	There are three programmable logic devices (PLDs) in the APX 8100 shelf controller. The parameters jam-file-1 through jam-file-3 contain the firmware versions for each respective PLD. The parameters jam-file-4 through jam-file-6 are not used.

Time zone information without using SNTP

Correct time zone information is now available regardless of whether Simple Network Time Protocol (SNTP) is configured. TAOS 10.1 includes a new parameter time-zone in the system profile to report time zone information. Although you can still use the existing parameter, gmt-offset in the ip-global:sntp-info subprofile, Lucent recommends that users switch to the new time-zone parameter.

The parameter system:time-zone overrides the ip-global:sntp-info:gmt-offset parameter unless time-zone is set to the value utc-unused. The user must change the value of time-zone from its default value of utc-unused for the time-zone parameter to supply the Coordinated Universal Time (UTC) offset to the unit.

Using the time-zone parameter to change the time zone changes the system time of the unit automatically, without waiting for SNTP updates to be received or the timedate profile to be written.

When the TAOS unit's software is upgrade, time zone information is not lost. It is taken from the gmt-offset setting.



Note Do not modify the ip-global:sntp-info:gmt-offset and system:time-zone parameters and the timedate profile when there are active calls on the TAOS unit.

The new parameter system:time-zone is defined as follows:

Parameter	Setting
time-zone	Specifies the offset from Coordinated Universal Time (UTC) for the time zone of this unit. Set the value equal to utc+0000 to maintain time in UTC. Valid values include utc-unused (the default), utc+0000 (UTC), and values increasing and decreasing from UTC in increments of 30 minutes.

Parameter	Setting
	For example, San Francisco, which is 8 hours behind UTC, uses the value utc-0800, while Frankfurt, which is 1 hour ahead of UTC, uses the value utc+0100/ If time-zone is set to the default value of utc-unused, then the system uses the value of the gmt-offset parameter in the ip-global:sntp-info subprofile. Lucent strongly recommends that you use time-zone and not gmt-offset.

Disabling the proprietary afind protocol

A new parameter, afind-ipadrcfg has been added to the system profile. If the afind-ipadrcfg parameter is set to no, the afind protocol is disabled. This feature supplies additional security for afind access.

Security for afind access

TAOS implements a proprietary protocol informally named afind to provide an easy method to identify and query TAOS-based devices. It has also been made available as the *MAX/Pipeline Configurator*. It is currently used to identify, inventory, and configure new units using a special utility program. Typically this is done in mass staging facilities prior to final network deployment.

The afind protocol uses specially formatted User Datagram Protocol (UDP) packets that are broadcast or unicast to the UDP discard port. It has both a query and a set option.

In response to an afind query, the unit returns the following information: the unit name, serial number, software version number, load name, installed options list, IP address, and Ethernet MAC address.

You can change the unit's IP address and subnet mask by using the afind set option. The afind protocol is password protected using the read-write-community parameter in the snmp profile as the password. However, afind is not part of Simple Network Management Protocol (SNMP) and works even if SNMP is disabled.

If the read-write-community parameter in the snmp profile is set to its default value anyone is able to change the ip-address or system name of the TAOS unit. Such changes can occur even if the enabled or read-write-enabled parameter in the SNMP profile is set to no. Unauthorized individuals can also obtain information using Afind that can be used to attack the TAOS unit in some way.

To prevent such attacks, the parameter afind-ipadrcf has been added to the system profile. Lucent strongly recommends that after the snmp profile has been configured, the afind-ipadrcf parameter be set to no. This setting secures the TAOS unit from attacks using the afind protocol.

Addition to the system profile

The new afind-ipadrcfg parameter has been added to the system profile.

```
[in SYSTEM]
installation-complete = yes
name = tnt95f
...
...
support-dbcs = no
afind-ipadrcfg = yes
```

Parameter	Specifies
afind-ipadrcfg	Enables/disables the Afind protocol configure and query requests. Select one of the following values: ■ yes (the default)—Enable afind configure and query requests. The requests are accepted only if: – The ip-address for any shelf controller is 0.0.0.0. or – The ip-address for any shelf controller is not 0.0.0.0 and the parameter snmp:read-write-community is not set to the value write. ■ no—Disable all afind configure and query requests.

The -t option of arptable command removed

The -t option of the arptable command has been removed. Switching Address Resolution Protocol (ARP) debugging on and off is now done with the diag arp command.

The help menu for the arptable command is as follows:

```
usage: arptable [vRouter] [[-a hostname MAC_address] | [-d hostname] | [-f]]
       [vRouter]: VRouter to which this ARP command is applicable
       [-a hostname MAC_address]: Adds hostname entry to the ARP table with
      MAC_address
       [-c]: Displays count of arp entries
       [-d hostname]: Deletes hostname entry from ARP table
       [-f]: Clears an entire ARP cache
```

If ARP debugging is set to off, issuing the command again sets it to on. Following is an example:

```
admin> diag arp
 arp debug is ON

admin> diag arp
 arp debug is OFF
```

Permission-level change for `device` command

The `device` command is now available only in the `debug` environment. Previously, the command required only diagnostic permissions.

New command to display system information

TAOS now includes a command `info` for displaying information about the TAOS system, including hardware platform, system name, serial number, software version, boot firmware version, and controller role. The command can be used on all APX and MAX TNT models.



Note During booting, TAOS units running TAOS 10.1 or later display platform, system name, software version, and boot version to the console.

Use the `info` command as follows:

```
admin > info
Platform          : Lucent APX 8000
System Name       : my_apx8000
Serial Number     : 98981234
Software Version  : TAOS 10.1.0 (apxsr)
Boot Version      : TAOS 10.1.0
Controller Role   : Primary
```

The fields displayed by the command are defined as follows:

Field	Definition
`Platform`	Hardware platform type.
`System name`	Name of the system as configured in the `system` profile. If the `system` profile has not been configured, the command displays `no name`.
`Serial number`	Serial number of the system.
`Software version`	Current version of the operating system.
`Boot version`	Version of boot loader on the system.
`Controller role`	Current role of the APX controller, either primary or secondary. (This field applies only on APX 8000 and APX 8100 units.)

RADIUS features

TAOS 10.1.0 includes the following features for RADIUS.

RADIUS and call logging support for V.92

With this software version, RADIUS and Navis® call logging support the following new attribute values:

```
Ascend-Modulation = v92
```

```
Ascend-Recv-Symbol-Rate = sym8000
```

```
Ascend-Modem-Disconnect-Reason = mohDisconnect
```

```
Ascend-Modem-Disconnect-Reason = mohTimerExpired
```

For example, suppose a system has enabled V.92 modulation and set up their `call-logging` profile as shown below:

```
admin> get call-logging
[in CALL-LOGGING]
call-log-enable = yes
call-log-host-1 = 134.112.25.108
call-log-host-2 = 0.0.0.0
call-log-host-3 = 0.0.0.0
call-log-port = 1646
call-log-key = ascend
call-log-timeout = 1
call-log-id-base = acct-base-10
call-log-reset-time = 0
call-log-stop-only = yes
call-log-limit-retry = 0
call-log-server-index = host-1
call-log-evaluation-end-julian-time = 0
call-log-radius-compat = 16-bit-vendor-specific
call-log-multi-packet = no
call-log-stream-period = 15
call-log-connection-packets-enable = no
call-log-csm-modem-diag = yes
voip-call-logging = yes
call-log-switchover = no
```

If a V.92 client establishes a connection to this system and then the call is dropped, the call log will contain attributes showing modulation, symbol rate, and speeds populated with V.92 numbers. The relevant entries are shown in bold in the following sample records:

```
Start record:
Sun Jan 12 16:02:24 2003
Event-Timestamp = 1018624664
NAS-IP-Address = 134.112.25.26
NAS-Identifier = "noname"
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 22
Ascend-NAS-Port-Format = 2_4_5_5
NAS-Port-Type = Async
```

```
Ascend-Line-Type = DSO
Ascend-Dsl-Physical-Slot = 1
Ascend-Dsl-Physical-Line = 1
Ascend-Dsl-Physical-Channel = 23
Acct-Status-Type = Start
Acct-Delay-Time = 0
Acct-Session-Id = "387469263"
Acct-Authentic = Local
Ascend-Modem-PortNo = 23
Ascend-Modem-SlotNo = 12
Ascend-Modem-ShelfNo = 1
Client-Port-DNIS = "4735"
Ascend-Call-Direction = Ascend-Call-Direction-Incoming
Ascend-Service-Type = Ascend-Service-Type-PPP
Ascend-Error-Correction-Protocol = lap-m
Ascend-Compression-Protocol = v42bis
Ascend-Modulation = v92
Ascend-Recv-Symbol-Rate = sym8000
Ascend-Current-Xmit-Level = 10
Ascend-Current-Line-Quality = 18

Stop Record:
Sun Jan 16:03:32 2003
Event-Timestamp = 1018624732
NAS-IP-Address = 134.112.25.26
NAS-Identifier = "noname"
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 22
Ascend-NAS-Port-Format = 2_4_5_5
NAS-Port-Type = Async
Ascend-Line-Type = DSO
Ascend-Dsl-Physical-Slot = 1
Ascend-Dsl-Physical-Line = 1
Ascend-Dsl-Physical-Channel = 23
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "387469263"
Acct-Authentic = Local
Acct-Session-Time = 67
Acct-Input-Octets = 0
Acct-Output-Octets = 0
Acct-Input-Packets = 0
Acct-Output-Packets = 0
Ascend-Data-Rate = 30667
Ascend-Disconnect-Cause = 81
Ascend-Connect-Progress = 40
Ascend-PreSession-Time = 27
Ascend-Pre-Input-Octets = 0
Ascend-Pre-Output-Octets = 0
Ascend-Pre-Input-Packets = 0
Ascend-Pre-Output-Packets = 0
Ascend-Xmit-Rate = 49333
```

```
Ascend-Modem-PortNo = 23
Ascend-Modem-SlotNo = 12
Ascend-Modem-ShelfNo = 1
Client-Port-DNIS = "4735"
Ascend-Call-Direction = Ascend-Call-Direction-Incoming
Ascend-Service-Type = Ascend-Service-Type-PPP
Ascend-Error-Correction-Protocol = lap-m
Ascend-Compression-Protocol = v42bis
Ascend-Modulation = v92
Ascend-Recv-Symbol-Rate = sym8000
Ascend-Current-Xmit-Level = 10
Ascend-Current-Line-Quality = 18
Ascend-Min-Xmit-Rate = 49333
Ascend-Max-Xmit-Rate = 49333
Ascend-Min-Recv-Rate = 30667
Ascend-Max-Recv-Rate = 30667
Ascend-Local-Retrain-Requested = 0
Ascend-Remote-Retrain-Requested = 0
Ascend-Connection-Time = 73
Ascend-Modem-Disconnect-Reason = linkDisconnect
```

RADIUS support for configurable AT answer string

The new RADIUS vendor-specific attribute (VSA) `Ascend-AT-Answer-String` enables you to override the value of the `AT-answer-string` parameter in the `terminal-server:modem-configuration` profile. The new attribute must appear in a RADIUS user profile that specifies calling line ID (CLID) or Dialed Number Information Service (DNIS) authentication. Following is a sample RADIUS user profile:

```
5555551212 User-Password = "Ascend-CLID"
           Ascend-Require-Auth = Require-Auth,
           Ascend-AT-Answer-String = "+A8E=,,,0"
```

The sample `Ascend-AT-Answer-String` setting disables V.8bis signaling on MultiDSP slot cards for calls from CLID `5555551212`.

Dynamic banner and login prompt

In previous releases, the terminal-server banner and login prompt could be specified only by settings in the `terminal-server` profile, making a unique banner and login prompt impossible to specify for an individual user. In this release, you can use RADIUS to specify a unique banner and login prompt for an individual user on the basis of first-tier authentication.

Specifying a banner and login prompt

In this release, a 16-bit vendor-specific attribute (VSA) called `Ascend-TermSrv-Login-Prompt (273)` has been added to the RADIUS dictionary file. Using this attribute, you can specify a terminal-server login prompt of up to 32 characters. To specify a banner, use the existing `Reply-Message` attribute. Both attributes must appear in a

RADIUS user profile that specifies calling line ID (CLID) or Dialed Number Information Service (DNIS) authentication. Following is a sample RADIUS user profile:

```
5059    User-Password = "Ascend-DNIS"
        Service-Type = Framed-User,
        Ascend-Require-Auth = Require-Auth,
        Ascend-TermSrv-Login-Prompt = "MyPrompt:",
        Reply-Message = "Welcome to the terminal server! "
```

In this profile, `Ascend-TermSrv-Login-Prompt` specifies the terminal-server login prompt, and `Reply-Message` specifies the terminal-server banner, for dial-in clients with DNIS number 5059. Dial-in clients who fit this profile receive the following terminal-server window:

```
Welcome to the terminal server!
System Password:
MyPrompt:
Password:
```

The terminal-server banner and login prompt specified in a RADIUS user profile take precedence over the banner and login prompt defined in a TAOS `terminal-server` profile.

Configurable resending of the Accounting Event packet

When a TAOS unit powers up, it sends an Accounting Event packet (code 33) to the external accounting server, if it is configured with one. The Accounting event packet includes a ColdStart packet and an Accounting On packet, with the attribute Ascend-Event-Type set to Ascend-ColdStart. The ability to resend the Accounting Event packet is useful for certain situations, such as when the connection from the TAOS unit to the RADIUS server is over a frame relay link.

But RADIUS versions such NavisRadius 1.3A8 and NavisRadius 3.0 and 4.0 do not support Accounting Event packet and do not reply with an acknowledgement. In previous software releases, after several retries, the system's default behavior was to add the request to the back-off queue indefinitely.

In this release, the system's default behavior is now to quietly discard the request if an Accounting Event packet if it has been not acknowledged by the RADIUS server after three retries.

To enable the system to retry sending the Accounting Event packet to the RADIUS server indefinitely, set the new `resend-coldstart` in the of the `external-auth:rad-acct-client` subprofile to `yes`. From example:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set rad-acct-client resend-coldstart = yes

admin> write
EXTERNAL-AUTH written
```

SNMP features

TAOS 10.1.0 includes the following new SNMP features.

SNMP support for V.92

The `lmodem.mib` associated with this release supports new values for V.92 connections. These values are used to populate SNMP modem tables with the correct values from a V.92 call. Following are relevant attribute-value pairs:

```
csmLanMdmDiagModulation.1.0 = v92(18)

csmLanMdmDiagSymbolRate.1.0 = sym8000(7)

csmLanMdmDiagDisconnectReason.1.0 = mohDisconnect(24)

csmLanMdmDiagDisconnectReason.1.0 = mohTimerExpired(25)
```

For example, if a V.92 client establishes a connection and then the call is dropped, the following command from an authorized SNMP workstation:

```
swalk csmLanMdmDiagTable
```

will show the proper modulation, symbol rate, and speeds for V.92. For example, the relevant entries are shown in bold in the following sample output:

```
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagIndexNumber.1.0 = 1

enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagCurrentXmitRate.1.0 = baud49333(42)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagMinXmitRate.1.0 = baud49333(42)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagMaxXmitRate.1.0 = baud49333(42)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagCurrentRecvRate.1.0 = baud30667(33)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagMinRcvRate.1.0 = baud30667(33)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagMaxRcvRate.1.0 = baud30667(33)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagProtocol.1.0 = lap-m(2)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagCompression.1.0 = v42bis(3)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagModulation.1.0 = v92(18)
enterprises.ascend.lanModemGroup.csmLanMdmDiagTable.csmLanMdmDiagEntry.
csmLanMdmDiagSymbolRate.1.0 = sym8000(7)
```

Support for alarm MIBs

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

Supported alarm MIBs

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

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

The MIBs provides information about the following:

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

Use of the alarm MIBs requires the network management software license. The network management software is enabled for a unit if the `network-management-enabled` parameter in the `base` profile is set to `yes`.



Caution Currently, the alarm MIBs do not support redundancy. If a backup slot card or control module switches over to replace one that has failed, all current alarm information indicated by the MIBs is lost.

MIB tables

The alarm MIB consists of a generic alarm model and lists active and cleared alarms. An alarm model defines the possible states an alarm can assume as well as the object ID (OID) of the notification (trap) that is sent out when an alarm changes state.

To access alarm information on a system, you can query the following tables:

Table	Indicates
`alarmModelTable`	Information applicable to all instances of all alarms for a given system. If a notification is not represented in the `alarmModelTable`, it is not an alarm state transition. The table is indexed by { `alarmListName`, `alarmModelIndex`, `alarmModelState` }.
`alarmActiveTable`	List of alarms currently occurring on a system. You can query this table upon device discovery and rediscovery to determine which alarms are currently active on the device. The table is indexed by { `alarmListName`, `alarmActiveDateAndTime`, `alarmActiveIndex` }.
`alarmActiveVariableTable`	Notification variable bindings associated with the alarms in the `alarmActiveTable`. The table is indexed by { `alarmListName`, `alarmActiveIndex`, `alarmActiveVariableIndex` }.

Table	Indicates
alarmActiveStatsTable	Current and total raised alarm counts as well as the last time an alarm was raised and cleared per named alarm list. The table is indexed by { alarmListName }.
alarmClearTable	List of alarms no longer active on the system. The table is indexed by { alarmListName, alarmClearDateAndTime, alarmActiveIndex }.
ituAlarmTable	International Telecommunication Union Telecommunication Standardization Sector (ITU-T) alarm information for possible alarms on the system, including alarm severity and event type. The table is indexed by { alarmListName, alarmModelIndex, ituAlarmPerceivedSeverity }.
ituAlarmActiveTable	ITU-T information for active alarms entries. The table is indexed by { alarmListName, alarmActiveDateAndTime, alarmActiveIndex }.
ituAlarmActiveStatsTable	ITU-T alarm statistics information. The table is indexed by { alarmListName }.

Specifying the maximum number of alarms in alarmClearTable

To set the maximum number of alarms in alarmClearTable, set the new alarm-clear-table-limit parameter in the snmp profile.

The alarm-clear-table-limit parameter specifies the maximum number of alarms that can be stored in alarmClearTable. Specify a value from 1 through 200. The default value is 100. For example, the following sample commands specify that up to 150 alarms can be stored in alarmClear Table:

```
admin> read snmp
SNMP read

admin> set alarm-clear-table-limit = 150

admin> write
SNMP written
```

Clearing alarms from the alarmActiveTable and alarmClearedTable

To clear the alarms in alarmActiveTable and alarmClearTable, disable the associated trap profile by setting the active-enabled parameter in the trap profile to no. When the trap profile is disabled, the alarm model table reports RowStatus as NOT_IN_SERVICE.

Deleting an alarm model table

To delete an alarm model table, delete the corresponding trap profile.

MIB traps

Following are the traps supported by the alarm MIBs:

```
alarmRaise NOTIFICATION-TYPE
          OBJECTS     { alarmModelIndex,
```

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

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

TAOS modifications to the alarm MIBs

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

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

Supported alarms

Following are the alarms supported by the alarm MIBs:

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

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

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

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

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

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

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

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

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

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

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

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

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

```
ALARM_IMA_LINK_LIF, ALARM_IMA_LINK_LODS, ALARM_IMA_LINK_RFI,
ALARM_IMA_LINK_TX_MIS, ALARM_IMA_LINK_RX_MIS, ALARM_IMA_LINK_TX_FAULT,
ALARM_IMA_LINK_RX_FAULT, ALARM_IMA_LINK_TX_UN, ALARM_IMA_LINK_RX_UN,
ALARM_IMA_GROUP_STARTUP, ALARM_IMA_GROUP_CFG, ALARM_IMA_GROUP_CFGFE,
ALARM_IMA_GROUP_LINKS, ALARM_IMA_GROUP_LINKSFE, ALARM_IMA_GROUP_BLOCK,
ALARM_IMA_GROUP_TIME,
----------------------------------------------------------------------
state: cleared, raise
resource type: RESOURCE_IF
resource id: ifIndex
ALARM_DSX1_LINE_ERROR
---------------------
state: cleared, raise
no resource associated
ALARM_DSX3_LINE_ERROR
---------------------
state: cleared, raise
no resource associated
```

SNMP MIB load order

Simple Network Management Protocol (SNMP) management information bases (MIBs) are located in the same directory as the software release. To download the MIBs, log in to Lucent OnLine Customer Support at `http://www.lucent.com/support`.

The following list shows the Lucent Access Enterprise MIBs and industry-standard MIBs (file name begin with RFC) distributed with TAOS. The MIBs are listed in the recommended load sequence, which satisfies internal MIB dependencies.

Table 3-9. MIB load order (page 1 of 4)

Load order	MIB	Description
1	`rfc2578.mib`	SNMPv2-SMI
2	`rfc2579.mib`	SNMPv2-TC
3	`rfc1213.mib`	MIB-II
4	`ianaiftype.mib`	IANA ifType
5	`rfc2233.mib`	Interface Group MIB using SMIv2
6	`rfc1317.mib`	RS-232 MIB
7	`rfc2493.mib`	Performance History TC MIB
8	`rfc2495.mib`	DS1 MIB
9	`rfc2496.mib`	DS3 MIB

Table 3-9. MIB load order (page 2 of 4)

Load order	MIB	Description
10	rfc1315.mib	Frame Relay MIB
11	rfc1696.mib	Modem MIB
12	rfc1850.mib	OSPF MIB
13	rfc1850_2.mib	OSPF TRAP MIB
14	rfc2558.mib	SONET MIB
15	rfc2514.mib	ATM-TC MIB
16	rfc2515.mib	ATM MIB
17	rfc1398.mib	Ethermet-like MIB (dot3)
18	rfc1724.mib	RIP 2 MIB
19	rfc1215.trp	SNMP generic traps
20	rfc2571.mib	SNMPV3 Framework MIB
21	rfc2572.mib	SNMPV3 Message Processing And Dispatching MIB
22	rfc2574.mib	SNMPV3 User Based Security Model MIB
23	rfc2575.mib	SNMP View Based ACM MIB
24	rfc2573_1.mib	SNMPv3 Management Target MIB
25	rfc2573_2.mib	SNMPv3 Notification MIB
26	rfc2662_1.mib	ADSL TC MIB
27	rfc2662_2.mib	ADSL Line MIB
28	rfc1657.mib	BGP MIB
29	rfc1493.mib	BRIDGE MIB
30	rfc3014.mib	Notification Log MIB
31	ascend.mib	Lucent Access MIB
32	rfc3014ext.mib	Lucent Notification Log Extension MIB
33	atmftc.mib	ATM FORUM Definitions
34	atmfspvc.mib	ATM FORUM Soft PVC MIB

Table 3-9. MIB load order (page 3 of 4)

Load order	MIB	Description
35	atmfm4.mib	ATM FORUM M4 MIB
36	atmfpnni.mib	ATM FORUM PNNI MIB
37	atm2supp.mib	ATM Supplemental MIB
38	atmfima.mib	IMA MIB
39	event.mib	Lucent Access Event MIB
40	hashcode.mib	Lucent Access hash code MIB
41	call.mib	Lucent Access Call MIB
42	session.mib	Lucent Access Session MIB
43	lmodem.mib	Lucent Access LAN Modem MIB
44	radius.mib	Lucent Access RADIUS MIB
45	mcast.mib	Lucent Access Multicast MIB
46	firewall.mib	Lucent Access Firewall Control Protocol MIB
47	wan.mib	Lucent Access Wan MIB
48	sdsl.mib	Lucent Access SDSL interface MIB
49	adslcap.mib	Lucent Access ADSL CAP interface MIB
50	wandialout.mib	Lucent Access Wan Dialout Pkt MIB
51	ps.mib	Lucent Access Power Supply MIB
52	ms.mib	Lucent Access Multi-Shelf MIB
53	advanced.mib	Lucent Access Advanced Agent MIB
54	flash.mib	Lucent Access Flash MIB
55	misc.mib	Lucent Access Miscellaneous MIB
56	atmp.mib	Lucent Access ATMP MIB
57	asndl2tp.mib	Lucent Access L2TP MIB
58	srvcmgmt.mib	Lucent Access Service Management MIB
59	call_log.mib	Lucent Access Call Logging MIB
60	chassis.mib	Lucent Access Chassis MIB

Table 3-9. MIB load order (page 4 of 4)

Load order	MIB	Description
61	resource.mib	Lucent Access Resource Management MIB
62	watchdog.mib	Lucent Access Watchdog MIB
63	voip.mib	Lucent Access VoIP MIB
64	voipstats.mib	VoIP statistics MIB
65	sparing.mib	Lucent Access LIM and Trunk Sparing Status MIB
66	mgstat.mib	Media Gateway Status and Statistics MIB
67	debug.mib	Lucent Access Debug MIB
68	ping.mib	Remote PING MIB
69	cardcode.mib	Lucent Access card code MIB
70	rtpqos.mib	RTP QoS statistics MIB
71	ascend.trp	Lucent Access traps
72	ascendv3.trp	Lucent Access traps

Enhancements to the snmpMgrStats command

A TAOS unit configured as a Simple Network Management Protocol (SNMP) agent rejects a request from a configured SNMP manager if any one of the following error conditions occurs:

- The SNMP manager is not configured for the type of access (read or read-write) it is requesting.
- The community string it presents is invalid.
- The SNMP version of the request (SNMPv1 or SNMPv3) is not supported by the TAOS unit's agent.

In previous releases, the snmpMgrStats command displayed only the number of invalid access attempts by SNMP managers. In this release, the snmpMgrStats command has been enhanced to display the number of requests containing an invalid community name or SNMP version as well.

Following is sample output from the snmpMgrStats command that shows no invalid requests:

```
admin> snmpMgrStats
SnmpManager       Illegal Access       Invalid Version        Bad Community
       susha-sun              0                     0                    0
  200.140.143.46              0                     0                    0
```

Suppose that a TAOS unit's SNMP agent accepts only SNMPv1 messages and a manager running on host 200.140.143.46 sends an SNMPv3 request. When you run the snmpMgrStats command, the following output results:

```
admin> snmpMgrStats
SnmpManager       Illegal Access       Invalid Version        Bad Community
  200.140.143.46             0                     1                    0
```

Suppose that an SNMP manager running on host 200.140.143.46 sends a request with an invalid community name. When you run the snmpMgrStats command, the following output results:

```
admin> snmpMgrStats
SnmpManager       Illegal Access       Invalid Version        Bad Community
  200.140.143.46             0                     0                    1
```

New SNMP admin-state-modem-if profile for modem cards

In previous software releases, when the system detected a modem card, it created one of the following profiles for each modem on the modem card and assigned it an interface index:

- admin-state-phys-if profile MAX TNT and APX 8000 units
- admin-state-iana-if profile for APX 8100 units

The system saved the admin-state-phys-if and admin-state-iana-if profiles to nonvolatile RAM (NVRAM).

For example, for a 288-port MultiDSP 3 card on an APX 8100 unit, the system created 288 admin-state-iana-if profiles for that particular card.

In this release, the system no longer creates an admin-state-phys-if or admin-state-iana-if for each modem, but instead creates an admin-state-modem-if profile *for each modem card* and saves the admin-state-modem-if profile to NVRAM.



Note This feature does not affect the creation of the admin-state-iana-if and admin-state-phys-if profiles for the slot cards that are not modem cards.

Overview of the admin-state-modem-if profile

Following is a sample listing of the admin-state-modem-if profile for a 288-port MultiDSP3 card in slot 3. Parameter descriptions follow the profile listing.

```
[in ADMIN-STATE-MODEM-IF/{ shelf-1 slot-3 0 }]
device-address* = { shelf-1 slot-3 0 }
slot-type = madd3-card
base-modem-index = 1
modem-count = 288
```

Parameter	Specifies
device-address	Physical address of the device whose SNMP state is stored in this profile. This parameter is read-only.

Parameter	Specifies
slot-type	Type of modem slot card. If, at system startup, the actual type of the device address is different than this type we know that slot cards have been changed and the old snmp interfaces can be deleted. This parameter is read-only.
base-modem-index	The SNMP modem index number assigned to the first modem on the slot card. This parameter is read-only.
modem-count	The number of modems in this modem card. This parameter is read-only.

Upgrading and downgrading issues

When you upgrade to TAOS 10.1.0, the system creates an admin-state-modem-if profile only for every modem slot card.

After the upgrade, the modem index values (mdmIndex) values stored in the newly created admin-state-modem-if profiles might not be the same as the mdmIndex values stored in the previous admin-state-iana-if profiles of the corresponding modems on the modem cards.

If you are downgrading to a previous release, you must enter the nvram command for the system to create the necessary admin-state-phys-if and admin-state-iana-if profiles for the modems in the model slot cards.

modem-table-index parameter no longer in admin-state-phys-if and admin-state-iana-if profiles

The modem-table-index parameter is no longer available in the following admin-state-phys-if and admin-state-iana-if profiles. The SNMP modem index number assigned by the system to the first modem on the slot card is now reported by base-modem-index parameter in the admin-state-modem-if profile.

Changes to the if-admin and modem commands

This release include add a new -d option for if-admin command and modifies and output of the modem command.

New -d option for the if-admin command

The if-admin -d command displays the modem device address mappings for the physical address of a modem slot card.

Note The -d option is applicable *only* with modem cards.

```
admin> if-admin -d {1 3 1}
 SNMP-IF   DEVICE ADDRESS   STATUS
     1   -   {{{  1  3  1 }  0 }  0 }   active
```

If no modem card is present in the queried slot, the system displays the following message:

```
admin> if-admin -d {1 9 1}
No modem is present corresponding to this address
```

The help screen for the `if-admin` command is now as follows:

```
admin> if-admin -?
usage: if-admin -a|l|m|d|? [ interface ]|[physical Address]
       -a  list (a)available SNMP interface numbers
       -l  (l)ist SNMP interface/device address mappings
       -m  list (m)odem device address mappings
       -d  list modem (d)evice address mappings for the given physical
address
       -?  display this summary
```

Modified output for the `modem -a` and `modem -d` commands

The output of the modem `-a` and modem `-d` commands no longer show the `sAdm` field. The value reported by the `sAdm` field was always `UP`. The new output for the `modem -a` command is as follows:

```
admin> modem -a
Modems available for use:
                          (dvOp  dvUpSt  dvRq  mDis)
  Modem {  1  9  1 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  2 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  3 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  4 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  5 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  6 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  7 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  8 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9  9 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9 10 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9 11 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9 12 }     (Up    Idle    UP    ENABLE  )
  Modem {  1  9 13 }     (Up    Idle    UP    ENABLE  )
```

Destructive `snmpset` commands disabled on the secondary controller

With this release, you can only use the `snmpset` command with the MIB objects listed in Table 3-10 only on the primary controller.

In the examples shown in Table 1-1, the IP address of the secondary controller is 110.110.110.33. If you use snmpset command with the MIB objects listed in Table 3-10 from the secondary controller, the system generates an error message.

Table 3-10. MIB objects which you can no longer set using the snmpset command from the secondary controller

MIB object	Specifies

ssnActiveValidFlag	Disable a user session. For example:
	`snmpset 110.110.110.33 write ssnActiveValidFlag.414510263 i invalid`
	`Error in packet.`
	`Reason: (genError) A general failure occured`

ssnStatusValidFlag	Disable a user session. For example:
	`snmpset 110.110.110.33 write ssnStatusValidFlag.4086 i invalid`
	`Error in packet.`
	`Reason: (genError) A general failure occured`

slotAdminStatus	Modify the status of a slot card. For example:
	`snmpset 110.110.110.33 write slotAdminStatus.6 i down`
	`Error in packet.`
	`Reason: (genError) A general failure occured`

wanLineUsage	Quiesce a line. For example:
	`snmpset 110.110.110.33 write wanLineUsage.21 i lu-trunk`
	`Error in packet.`
	`Reason: (genError) A general failure occured`

resourceConfig	Enable or disable a device. For example:
	`snmpset 110.110.110.33 write resourceConfig.6.96 i disable`
	`Error in packet.`
	`Reason: (genError) A general failure occured`

internetProfile-Action	Create, delete, or modify a profile. NVRAM profiles can no longer be created/deleted/modified using the snmpset command from the secondary controller.
	The following sample command attempts to create a new connection profile jj from the secondary controller. In the following command, 106 is the ASCII value of the character j.
	`snmpset 110.110.110.33 write internetProfile-Action-o.2.106.106 i createProfile`
	`Error in packet.`
	`Reason: (genError) A general failure occured`
	`Failed object: internetProfile-Action-o."jj"`

Table 3-10. MIB objects which you can no longer set using the `snmpset` *command from the secondary controller*

MIB object	Specifies

	The following `snmpset` command attempts to delete a existing connection profile `jj`.
	`snmpset 110.110.110.33 write internetProfile-Action-o.2.106.106 i deleteProfile`
	`Error in packet.`
	`Reason: (genError) A general failure occured`
	`Failed object: internetProfile-Action-o."jj"`

	The following `snmpset` command attempts to set the `active` parameter in the `connection` profile `jj` to `yes`.
	`snmpset 110.110.110.33 write internetProfile-Active.2.106.106 i yes`
	`Error in packet.`
	`Reason: (genError) A general failure occured`
	`Failed object: internetProfile-Active."jj"`

Signaling System 7 (SS7) features

TAOS 10.1.0 includes the following SS7 features.

Conversion of `ss7-gateway` to `media-gateway` settings

In this release, the new `media-gateway` profile replaces the `ss7-gateway` profile in earlier releases. The system automatically preserves the configuration information in the `ss7-gateway` profile and migrates it to the new `default media-gateway` profile during an upgrade to this release. For details, see "Upgrading and Downgrading" on page 1-1.

The `ss7-gateway` parameter values are converted to equivalent `media-gateway` parameters as listed in Table 3-11:

Table 3-11. Parameter conversion equivalents

`SS7-GATEWAY` parameter	`MEDIA-GATEWAY` equivalent
`enabled`	`active`
`control-protocol`	`protocol-type`
`primary-ip-address`	`mgc-address[1]:ip-address`
`primary-tcp-port`	`mgc-address[1]:port-number`
`secondary-ip-address`	`mgc-address[2]:ip-address`
`secondary-tcp-port`	`mgc-address[2]:port-number`

Table 3-11. Parameter conversion equivalents (Continued)

SS7-GATEWAY parameter	MEDIA-GATEWAY equivalent
bay-id	ipdc-options:bay-id
system-type	ipdc-options:system-type
transport-options:type	transport-options:type
transport-options:device-id	transport-options:ddl-options:device-id
transport-options:t1-duration	transport-options:ddl-options:t1-duration
transport-options:t2-duration	transport-options:ddl-options:t2-duration
transport-options:t3-duration	transport-options:ddl-options:t3-duration
transport-options:window-size	transport-options:ddl-options:window-size
transport-options:ack-threshold	transport-options:ddl-options:ack-threshold
transport-options:heart-beat	transport-options:heartbeat
transport-options:tos:active	tos-sig-options:active
transport-options:tos:marking-type	tos-sig-options:marking-type
transport-options:tos:dscp	tos-sig-options:dscp
transport-options:tos:precedence	tos-sig-options:precedence
transport-options:tos:type-of-service	tos-sig-options:type-of-service
use-system-ip-address-as-source	mg-sig-address:type
ipdc-source-adddress	mg-sig-address:ip-address
vrouter	mgc-address[1]:vrouter mgc-address[2]:vrouter
congestion-control:congestion-control-type	ipdc-options:congestion-control:congestion-control-type
congestion-control:cl1-level	ipdc-options:congestion-control:cl1-level
ipdc-options:congestion-control:cl1-level	ipdc-options:congestion-control:cl2-action
signaling-heartbeat:enabled	ipdc-options:heartbeat:enabled

Table 3-11. Parameter conversion equivalents (Continued)

SS7-GATEWAY parameter	MEDIA-GATEWAY equivalent
signaling-heartbeat:interval	ipdc-options:heartbeat:interval
resilience-options:type	ipdc-options:resilience-options:type
resilience-options:duration	ipdc-options:resilience-options:duration
pri-tunneling-options:enabled	ipdc-options:pri-tunneling-options:enabled
pri-tunneling-options:duration	ipdc-options:pri-tunneling-options:duration

Support for multiple media gateway controllers

In previous software versions, communication between TAOS and an SS7 signaling gateway was defined in the `ss7-gateway` profile. The TAOS system operated as a media gateway, with one media gateway controller (MGC) controlling its resources.

With this software version, the system can interoperate with multiple MGCs. The TAOS system can operate multiple virtual media gateways, with each virtual media gateway communicating with one MGC and controlling a subset of the system's resources. For example, you might assign half the lines of a T1 or E1 slot card to one MGC and half to another. In the event of an MGC failure, this configuration ensures that you do not lose all connectivity.



Note Currently, all virtual media gateways in the system must use the same media gateway control protocol. TAOS does not currently enable multiple media gateway control protocols at the same time.

To enable support for multiple MGCs, and to allow for future support of additional signaling protocols, the `ss7-gateway` profile has been replaced by the new `media-gateway` profile. For details about how the system automatically converts an existing `ss7-gateway` configuration to the default `media-gateway` profile, see "Conversion of `ss7-gateway` to `media-gateway` settings."

In addition, T1 and E1 line profiles now contain a `media-gateway` parameter for associating the line with a particular MGC.

Overview of `line-interface` settings

Following are the parameters, shown with default settings, for associating a T1 or E1 SS7 trunk with a particular MGC:

```
[in T1/{ any-shelf any-slot 0 }:line-interface]
media-gateway = ""

[in E1/{ any-shelf any-slot 0 }:line-interface]
```

```
media-gateway = ""
```

Parameter	Setting
media-gateway	Name of the media-gateway profile that defines communications to a particular MGC. With the default null value, the system uses the profile named default.

For example, the following commands configure a media-gateway profile and then apply it to an E1 line:

```
admin> new media-gateway one
MEDIA-GATEWAY/one read
admin> set protocol-type = ipdc
admin> set mgc-address 1 ip-address = 2.2.2.2
admin> set mgc-address 1 port-number = 2100
admin> set active = yes
admin> write -f
MEDIA-GATEWAY/one written
admin> read e1 { 1 1 2 }
E1/{ shelf-1 slot-1 2 } read
admin> set line-interface enabled = yes
admin> set line-interface signaling-mode = ss7-data-trunk
admin> set line-interface media-gateway = one
admin> write -f
E1/{ shelf-1 slot-1 2 } written
```

Overview of media-gateway settings

Each media-gateway profile represents a link to one MGC. The profile contains settings that enable the system to receive and respond to media gateway control messages from that MGC. Following are the parameters, shown with default settings, of an unconfigured system-generated default media-gateway profile:

```
[in MEDIA-GATEWAY/default]
name* = default
active = no
protocol-type = h248
mgc-address = [ { "" 0.0.0.0 2944 } { "" 0.0.0.0 2944 } { "" 0.0.0.0 2944 }+
mg-sig-address = { interface-dependent 0.0.0.0 }
mg-rtp-address = { system-default 0.0.0.0 }
h248-options = { text 3000 { no 0 } { 8000 6000 9000 [ { "" "" } { "" "" } +
ipdc-options = { "" IASCAPX1B { sig-queue-depth 60 send-info-to-mgc 120 rej+
transport-options = { tcp no { 0 1000 3000 30000 7 6 } }
voip-options = { g711-ulaw 2 no yes 19 2 /current g711-ulaw 6000 0 inband 2+
dialed-gw-options = { disabled disabled disabled ring-tone-on-alerting disa+
rt-fax-options = { no yes yes yes yes 0 no 14400 no }
tos-rtp-options = { no precedence-tos 00 000 normal }
tos-sig-options = { no precedence-tos 00 000 normal }
```

```
sip-options = { 500 4000 6 10 { 0.0.0.0 "" 5060 compact } { 0.0.0.0 "" 5060+
```

Parameter or subprofile	Setting
`name`	Profile name, up to 23 characters. The profile name labels the MGC associated with the profile, and is used to assign T1 or E1 lines to that MGC. (See "Overview of `line-interface` settings" on page 3-102 for details.)
`active`	Activates/deactivates the `media-gateway` profile. Set to `yes` to make the profile's configuration usable.
`protocol-type`	Protocol to be used to communicate with the MGC. Following are valid values: `h248` — H.248 (MEGACO) Multimedia Gateway Protocol Standard. *Not currently supported.* `sip` — Session Initiation Protocol. *Not currently supported.* `asgcp` — Access SS7 Gateway Control Protocol (ASGCP), used for terminating data calls in an SS7 network. The MGC must be a Softswitch ICD or ICDplus (formerly ASG). For details, see the *Physical Interface Guide* for your platform. `q931-plus` — Q.931 with extensions for IMT signaling over IP (DSS1 over IP). `ipdc` — IP Device Control (IPDC) includes interoperability with sections of IPDC 0.15.1, including PRI tunneling. This protocol is used for terminating both voice and data calls in an SS7 network.
`mgc-address`	An array of 8 indexed subprofiles for specifying MGC destination IP information. Only `mgc-address[1]` and `mgc-address[2]` are currently used. See "IP configuration to primary and secondary MGCs" on page 3-105.
`mg-sig-address`	Subprofile for specifying the source IP address to use in signaling packets transmitted on this interface. See "Source IP address in transmitted signaling packets" on page 3-106.
`mg-rtp-address`	Subprofile for configuring the default source address for RTP packets. *Not currently supported.*
`h248-options`	Subprofile for configuring H.248 options. *Not currently supported.*
`ipdc-options`	Subprofile for configuring IPDC. See "IPDC options" on page 3-107.
`transport-options`	Subprofile for fine-tuning a signaling link. See "Transport options" on page 3-110.

Parameter or subprofile	Setting
`voip-options`	Subprofile for configuring Voice over IP (VoIP) parameters common to all protocol types. *Not currently supported.* For details about the current method of configuring VoIP options, see the *MultiVoice® for APX/MAX TNT Configuration Guide.*
`dialed-gw-options`	Subprofile for configuring the call processing behavior of the ingress gateway. *Not currently supported.* For details about the current method of configuring ingress gateway settings, see the *MultiVoice® for APX/MAX TNT Configuration Guide.*
`rt-fax-options`	Subprofile for configuring real-time fax. *Not currently supported.* For details about the current method of configuring real-time fax, see the *MultiVoice® for APX/MAX TNT Configuration Guide.*
`tos-rtp-options`	Subprofile for configuring RTP packet priorities in the IP type-of-service (TOS) byte. *Not currently supported.* For details about the current method of configuring TOS for RTP packets, see the *MultiVoice® for APX/MAX TNT Configuration Guide*
`tos-sig-options`	Subprofile for configuring signaling packet priorities in the IP type-of-service (TOS) byte. See "TOS prioritization for signaling packets" on page 3-111.
`sip-options`	Subprofile for configuring SIP options. *Not currently supported.*

IP configuration to primary and secondary MGCs

Currently, only the first two subprofiles (`mgc-address[1]` and `mgc-address[2]`) are used, to specify the destination IP information of a primary and secondary MGC. Following are the relevant parameters, shown with default settings:

```
[in MEDIA-GATEWAY/default:mgc-address[N]]
vrouter = ""
ip-address = 0.0.0.0
port-number = 2944
```

Parameter	Setting
`mgc-address[N]: vrouter`	Name (up to 23 characters) of the virtual router through which the MGC is reached. With the default null value, the global virtual router is used. With the name of valid configured virtual router, if the media gateway source address is interface dependent, the IP address of the virtual router interface is used as the source address for outbound signaling traffic on the interface.
`mgc-address[N]: ip-address`	Destination IP address of the MGC. At least one valid MGC IP address is required for SS7 operations.
`mgc-address[N]: port-number`	TCP port to use for communication with the MGC.

For example, the following commands specify the IP address and TCP port of an MGC:

```
admin> read media-gateway default
MEDIA-GATEWAY/default read
admin> set active = yes
admin> set protocol-type = ipdc
admin> set mgc-address 1 ip-address = 1.1.1.1
admin> set mgc-address 1 port-number = 5000
admin> write -f
MEDIA-GATEWAY/default written
```

Source IP address in transmitted signaling packets

Following are the parameters, shown with default values, for specifying the source IP address to use signaling packets

```
[in MEDIA-GATEWAY/default:mg-sig-address]
type = interface-dependent
ip-address = 0.0.0.0
```

Parameter	Setting	
type	The source IP address to use in transmitted signaling packets. Following are valid values:	
	system-default	If the connection to the MGC does not use a virtual router, use the system IP address specified in the ip-global profile. If the connection specifies a virtual router, use the IP address of that virtual router.
	specific	Use the ip-address value specified in this subprofile.
	interface-dependent	Use the IP address of the local interface on which signaling packets are transmitted.
ip-address	IP address to use as the source address when type is set to specific.	

For example, the following commands display the system IP address and then configure the system to use that source address in signaling packets to the MGC:

```
admin> get ip-global system-ip-addr
[in IP-GLOBAL:system-ip-addr]
system-ip-addr = 3.3.3.3
admin> read media-gateway default
MEDIA-GATEWAY/default read
admin> set mg-sig-address = system-default
admin> write -f
```

```
MEDIA-GATEWAY/default written
```

IPDC options

Following are the parameters, shown with default values, for specifying the IPDC communications:

```
[in MEDIA-GATEWAY/default:ipdc-options]
bay-id = ""
system-type = IASCAPX1B
congestion-control = { sig-queue-depth 60 send-info-to-mgc 120 reject-+
heartbeat = { no 3 }
resilience-options = { release-all 0 }
pri-tunneling-options = { no 60000 }
module-type-reporting = standard
dtmf-incall-reporting = no
```

Parameter or subprofile	Setting
`bay-id`	MGC-specific value to send as an ASCII string in the device registration message.
`system-type`	MGC-specific value to send as an ASCII string in the device registration message to the MGC.
`congestion-control`	Subprofile for configuring congestion control. See "IPDC RTE congestion control" on page 3-108.
`heartbeat`	Subprofile for using IPDC Request Test Echo (RTE) messages for signaling heartbeat. See "IPDC RTE signaling heartbeat" on page 3-108.
`resilience-options`	Subprofile for holding active calls if loss of synchronization occurs on the SS7 trunk. See "Resilience for PSTN loss of signal" on page 3-108.
`pri-tunneling-options`	Subprofile for configuring Primary Rate Interface (PRI) tunneling on T1 or E1 trunks. See "PRI tunneling" on page 3-108.
`module-type-reporting`	Type of module to report to the MGC via network management system (NMS) message during registration or when a slot card bounces. For platforms other than the APX 8100, leave the default `standard` setting.
`dtmf-incall-reporting`	Reporting of in-call dual-tone multifrequency (DTMF) tones to the MGC via Notify Tones (NTN) messages. If this parameter is set to `yes` and in-call DTMF collection is requested via tag `0x75`, the system reports the collected DTMF digits in NTN messages. The value of this parameter is ignored if DTMF tone passing method is set in the `voip` profile to `dtmf-tone-passed-outofband`.

IPDC RTE congestion control

Following are the parameters, shown with default settings, for configuring IPDC RTE congestion control:

```
[in MEDIA-GATEWAY/default:ipdc-options:congestion-control]
congestion-control-type = sig-queue-depth
cl1-level = 60
cl1-action = send-info-to-mgc
cl2-level = 120
cl2-action = reject-new-calls
```

The default value of `congestion-control-type` is now named `sig-queue-depth` instead of the `l3-queue-depth` default in earlier software versions. Otherwise, these parameters are identical to those in the `congestion-control` subprofile of the `ss7-gateway` profile in earlier software versions. For details, see the *Physical Interface Guide* for your platform.

IPDC RTE signaling heartbeat

Following are the parameters, shown with default settings, for configuring IPDC RTE signaling heartbeat:

```
[in MEDIA-GATEWAY/default:ipdc-options:heartbeat]
enabled = no
interval = 3
```

These parameters are identical to those in the `signaling-heartbeat` subprofile of the `ss7-gateway` profile in earlier software versions. For details, see the *Physical Interface Guide* for your platform.

Resilience for PSTN loss of signal

Following are the parameters, shown with default settings, for configuring resilience:

```
[in MEDIA-GATEWAY/default:ipdc-options:resilience-options]
type = release-all
duration = 0
```

These parameters are identical to those in the `resilience-options` subprofile of the `ss7-gateway` profile in earlier software versions. For details, see the *Physical Interface Guide* for your platform.

PRI tunneling

The `pri-tunneling-options` subprofile contains settings for associating the status of a T1 or E1 D channel with the status of its associated IPDC signaling link. To support this association, the system creates a volatile `pritunl-stat` profile for each active `media-gateway` profile that specifies a `protocol-type` of `ipdc`. The `pri-tunl-stat` profile contains a flag that indicates to the system whether to bring up the D channel of PRI tunneling lines.

Following are the parameters, shown with default settings for a T1 system, for configuring this option:

```
[in MEDIA-GATEWAY/default:ipdc-options:pri-tunneling-options]
enabled = no
duration = 60000
```

Parameter	Setting
enabled	Enables/disables an association between PRI status and the IPDC signaling link status. When this parameter is set to no, the D channel of a line configured for tunneled PRI signaling remains operational even when the IPDC signaling link is unavailable. If it is set to yes, the D channel is brought down following the failure of an IPDC signaling link to the MGC. The default is no for T1 systems, and yes for E1 systems.
duration	Number of milliseconds to wait before updating the pritunl-stat profile following a change in status of the IPDC signaling link. This duration prevents the system from change D channel status for temporary status changes ("flapping") of the IPDC signaling link. The default setting is 60000 for both T1 and E1 systems.

For example, the following commands create two media-gateway profiles that will be applied to two E1 lines:

```
admin> new media-gateway mgc-one
MEDIA-GATEWAY/mgc-one read
admin> set active = yes
admin> set protocol-type = ipdc
admin> set mgc-address 1 ip-address = 1.1.1.1
admin> set mgc-address 1 port-number = 2000
admin> set mgc-address 2 ip-address = 1.1.1.1
admin> set mgc-address 2 port-number = 2001
admin> set ipdc-options pri-tunneling-options duration = 1000
admin> write -f
MEDIA-GATEWAY/mgc-one written
admin> new media-gateway mgc-two
MEDIA-GATEWAY/mgc-two read
admin> set active = yes
admin> set protocol-type = ipdc
admin> set mgc-address 1 ip-address = 2.2.2.2
admin> set mgc-address 1 port-number = 2100
admin> set mgc-address 2 ip-address = 2.2.2.2
admin> set mgc-address 2 port-number = 2101
admin> set ipdc-options pri-tunneling-options duration = 1000
admin> write -f
MEDIA-GATEWAY/mgc-two written
```

The next set of commands configures the two E1 line profiles:

```
admin> read e1 { 1 2 7 }
E1/{ shelf-1 slot-2 7 } read
```

```
admin> set line-interface enabled = yes
admin> set line-interface signaling-mode = tunneled-pri-signaling
admin> set line-interface media-gateway = mgc-one
admin> write -f
E1/{ shelf-1 slot-2 7 } written
admin> read e1 { 1 2 8 }
E1/{ shelf-1 slot-2 8} read
admin> set line-interface enabled = yes
admin> set line-interface signaling-mode = tunneled-pri-signaling
admin> set line-interface media-gateway = mgc-two
admin> write -f
E1/{ shelf-1 slot-2 8 } written
```

With these profiles, if one of the IPDC signaling links fails, the corresponding `pritunl-stat` profile is updated to instruct the system to bring down the D channels of the associated E1 line. For example:

```
admin> get pri-tunl-stat mgc-one
[in PRITUNL-STAT/mgc-one]
bring-up-d-channel = no
```

When the signaling link is available again, the volatile profile is updated again (to a `yes` value), and the system restores the D channels.

Log messages associated with the link failures indicate the number of lines affected by the failure. This is shown in the following examples:

```
Apr 24 16:01:09 10.6.0.30 1/2: 2 lines with Tunneled PRI signaling will be
down because IPDC signaling link is down.
Apr 24 16:06:08 10.6.0.30 1/2: 1 line with Tunneled PRI signaling will be
down because IPDC signaling link to "mgc-one" is down.
```

Transport options

The simple data delivery layer (DDL) uses TCP/IP for reliable transmission between the media gateway and MGC. Following are the parameters, shown with default settings, for configuring transport and DDL options:

```
[in MEDIA-GATEWAY/default:transport-options]
type = tcp
heartbeat = no
ddl-options = { 0 1000 3000 30000 7 6 }
[in MEDIA-GATEWAY/default:transport-options:ddl-options]
device-id = 0
t1-duration = 1000
t2-duration = 3000
t3-duration = 30000
window-size = 7
ack-threshold = 6
```

These parameters are identical to those in the `transport-options` subprofile of the `ss7-gateway` profile in earlier software versions. For details, see the *Physical Interface Guide* for your platform.

TOS prioritization for signaling packets

Following are the parameters, shown with default settings, for configuring TOS priorities for signaling traffic:

```
[in MEDIA-GATEWAY/default:tos-sig-options]
active = no
marking-type = precedence-tos
dscp = 00
precedence = 000
type-of-service = normal
```

These parameters are identical to those in the `transport-options:tos` subprofile of the `ss7-gateway` profile in earlier software versions. For details, see the *Physical Interface Guide* for your platform.

CLID Presentation Indicator support for IPDC

IPDC revision 0.19.1 defines how the IPDC protocol supports Calling Line Identification Presentation (CLIP) in call setup requests (RCSI packets). With this software version, TAOS extracts the CLIP information if it is present in the RCSI message and forwards it to RADIUS, where it may be used for CLID authentication, accounting, or call-logging purposes. The CLIP information is present only if it is forwarded by the gateway controller in the IPDC RCSI packets.

How new CLIP information is passed to TAOS

For SS7 incoming data calls that include CLIP information, the RCSI message will look like the following:

```
1864.97: NMI message dump:
Protocol=0x4b, Correlator (4): 00000003
Message: 0x0001
Tag ID=0x07, Data (2): 00 01
Tag ID=0x0d, Data (2): 00 05
Tag ID=0x15, Data (2): 00 03
Tag ID=0x17, Data (1): 09
Tag ID=0x18, Data (3): 31 32 33
Tag ID=0x19, Data (3): 32 33 34
Tag ID=0xb2, Data (4): 01 00 04 03
Tag ID=0xa4, Data (16): 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36
End of NMI message.
```

The CLID number is presented in Tag 0x18. This was also true in previous releases.

The additional CLIP information is presented in Tag 0xb2, whose format is as follows:

- Octet 1 - Screening Indicator
- Octet 2 - Address Presentation Restriction Indicator
- Octet 3 - Nature of Address Indicator
- Octet 4 - Numbering Plan Indicator

RADIUS support for CLIP information

The following RADIUS attributes can display CLIP information if it is present in Tag 0xb2 of an RCSI packet. The attributes are shown with sample values passed from the gateway controller:

- `Ascend-Calling-Id-Screening = User-Provided-Passed`
- `Ascend-Calling-Id-Presentation = Allowed`
- `Ascend-Calling-Id-Type-Of-Number = Network-Specific`
- `Ascend-Calling-Id-Numbering-Plan = Telex`

If Tag 0xb2 is not present, the following attributes are displayed with the values Unknown:

- `Ascend-Calling-Id-Type-Of-Number = Unknown`
- `Ascend-Calling-Id-Numbering-Plan = Unknown`

For example, the following connection request record sent to RADIUS shows the CLIP information displayed. In this instance, Tag 0xb2 was present in the RCSI packet. The relevant fields are shown in bold type.

```
User-Name = "123"
Password = <hidden>
NAS-IP-Address = 210.210.210.155
NAS-Identifier = "210.155"
NAS-Port = 130
#Anonymous# = 02 11 00 0d 00 00 00 02
NAS-Port-Type = Sync
Service-Type = Call-Check
Calling-Station-Id = "123"
Ascend-Calling-Id-Type-Of-Number = Network-Specific
Ascend-Calling-Id-Numbering-Plan = Telex
Ascend-Calling-Id-Presentation = Allowed
Ascend-Calling-Id-Screening = User-Provided-Passed
Called-Station-Id = "234"
Acct-Session-Id = "384650447"
Ascend-Data-Rate = 56000
Ascend-Xmit-Rate = 56000
```

Following is an example of a RADIUS accounting STOP packet. (Similar attributes would be visible in START and CHECKPOINT packets.) In this example, CLIP information was not available, because Tag 0xb2 was not present in the RCSI packet for this session. The relevant settings are shown in bold type.

```
Event-Timestamp = 1017168683
User-Name = "myk"
NAS-IP-Address = 210.210.210.136
NAS-Identifier = "apxfa"
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 15587
#Anonymous# = 02 11 00 0d 00 00 00 02
NAS-Port-Type = Sync
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "385329794"
```

```
Acct-Authentic = Local
Acct-Session-Time = 217
Acct-Input-Octets = 879876
Acct-Output-Octets = 879787
Acct-Input-Packets = 14769
Acct-Output-Packets = 14767
Ascend-Data-Rate = 56000
Ascend-Disconnect-Cause = 180
Ascend-Connect-Progress = 60
Ascend-PreSession-Time = 3
Ascend-Pre-Input-Octets = 144
Ascend-Pre-Output-Octets = 151
Ascend-Pre-Input-Packets = 8
Ascend-Pre-Output-Packets = 8
Ascend-First-Dest = 4.4.5.5
Ascend-Xmit-Rate = 56000
Ascend-Modem-PortNo = 93
Ascend-Modem-SlotNo = 13
Ascend-Modem-ShelfNo = 1
Calling-Station-Id = "123"
Ascend-Calling-Id-Type-Of-Number = Unknown
Ascend-Calling-Id-Numbering-Plan = Unknown
Called-Station-Id = "234"
Framed-Protocol = PPP
Framed-IP-Address = 4.5.6.7
Ascend-Global-Call-Id = "31323334-3536-3738-3930-313233343536"
```

Following is another sample STOP record that shows that the CLIP information was present in the RCSI packet for this session. The relevant fields are shown in bold type.

```
Event-Timestamp = 1017163936
User-Name = "myk"
NAS-IP-Address = 210.210.210.136
NAS-Identifier = "apxfa"
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 15586
#Anonymous# = 02 11 00 0d 00 00 00 02
NAS-Port-Type = Sync
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "385329787"
Acct-Authentic = Local
Acct-Session-Time = 132
Acct-Input-Octets = 608491
Acct-Output-Octets = 609465
Acct-Input-Packets = 10221
Acct-Output-Packets = 10237
Ascend-Data-Rate = 56000
Ascend-Disconnect-Cause = 180
Ascend-Connect-Progress = 66
Ascend-PreSession-Time = 1
Ascend-Pre-Input-Octets = 101
Ascend-Pre-Output-Octets = 105
```

```
Ascend-Pre-Input-Packets = 6
Ascend-Pre-Output-Packets = 7
Ascend-First-Dest = 4.4.5.5
Ascend-Xmit-Rate = 56000
Ascend-Modem-PortNo = 79
Ascend-Modem-SlotNo = 13
Ascend-Modem-ShelfNo = 1
Calling-Station-Id = "123"
Ascend-Calling-Id-Type-Of-Number = Network-Specific
Ascend-Calling-Id-Numbering-Plan = Telex
Ascend-Calling-Id-Presentation = Allowed
Ascend-Calling-Id-Screening = User-Provided-Passed
Called-Station-Id = "234"
Framed-Protocol = PPP
Framed-IP-Address = 4.5.6.7
Ascend-Global-Call-Id = "31323334-3536-3738-3930-313233343536"
```

Navis® call-logging support for CLIP information

Call logging uses the same attributes and operates in the same way as RADIUS accounting packets. Following is a sample call-logging STOP record that shows CLIP information in Tag 0xb2. The relevant fields are shown in bold type.

```
Event-Timestamp = 1017163936
User-Name = "myk"
NAS-IP-Address = 210.210.210.136
NAS-Identifier = "apxfa"
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 15586
#Anonymous# = 02 11 00 0d 00 00 00 02
NAS-Port-Type = Sync
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "385329787"
Acct-Authentic = Local
Acct-Session-Time = 132
Acct-Input-Octets = 608491
Acct-Output-Octets = 609465
Acct-Input-Packets = 10221
Acct-Output-Packets = 10237
Ascend-Data-Rate = 56000
Ascend-Disconnect-Cause = 180
Ascend-Connect-Progress = 66
Ascend-PreSession-Time = 1
Ascend-Pre-Input-Octets = 101
Ascend-Pre-Output-Octets = 105
Ascend-Pre-Input-Packets = 6
Ascend-Pre-Output-Packets = 7
Ascend-First-Dest = 4.4.5.5
Ascend-Xmit-Rate = 56000
Ascend-Modem-PortNo = 79
Ascend-Modem-SlotNo = 13
Ascend-Modem-ShelfNo = 1
```

```
Calling-Station-Id = "123"
Ascend-Calling-Id-Type-Of-Number = Network-Specific
Ascend-Calling-Id-Numbering-Plan = Telex
Ascend-Calling-Id-Presentation = Allowed
Ascend-Calling-Id-Screening = User-Provided-Passed
Called-Station-Id = "234"
Framed-Protocol = PPP
Framed-IP-Address = 4.5.6.7
Ascend-Call-Direction = Ascend-Call-Direction-Incoming
Ascend-Service-Type = Ascend-Service-Type-PPP
```

MultiVoice® features

TAOS 10.1.0 includes the following MultiVoice® features.

Simultaneous single-stage dialing VoIP and modem calls

On an incoming time-division multiplexing (TDM) channel, a gateway can support modem or Voice over IP (VoIP) functionality on a call-by-call basis. In this release, the new `dnis-or-voip` value for the `default-call-type` parameter in the `t1` and `e1` profiles enables you to specify that modem calls or single-stage VoIP calls can be processed by the gateway. This feature applies only to single-stage calls.

Configuring a unit to process modem or single-stage VoIP calls

To configure a unit to process modem or single-stage VoIP calls, set the following parameters:

Parameter	Location	Setting
`default-call-type`	`t1` or `e1` profile	Specify `dnis-or-voip` as the default call type associated with all incoming calls on this trunk.
`call-type`	`dnis` profile	Specify `digital` or `voice` as the call type to be associated with a given destination number.

How calls are processed when `default-call-type` is set to `dnis-or-voip`

When the gateway receives a call, it checks the dialed number against modem numbers specified by the `dnis` profile. When `default-call-type` is set to `dnis-or-voip`, a call is processed on the basis of the `call-type` setting and whether the dialed number matches the number specified by a `dnis` profile. Following are the different ways in which a call can be processed:

Setting of `call-type` parameter	DNIS match?	Result
`voice`	Yes	Call is processed as a modem call.
`digital`	Yes	Call is processed as a digital call.

Setting of `call-type` parameter	DNIS match?	Result
`voice` or `digital`	No	Call is processed as a VoIP call.

ISDN cause code verification

The new `cause-code-verification-enabled` parameter appears in the `t1` profile. If you set `cause-code-verification-enabled` to `yes` (the default), the T1 module validates the cause code for the switch type. If the cause code is not defined for the switch type, the unit uses `Invalid Element Content (cause code 100)` instead of the cause code received from the switch. Specifying `yes` enables the validation of the cause code for a switch type during processing and generation of the following public switched telephone network (PSTN) Q.931 messages:

- Progress
- Release
- Release Complete
- Disconnect

If you set `cause-code-verification-enabled` to `no`, the T1 module does not validate the cause code for the configured switch type. The cause code received from the switch is always used to generate the outgoing PSTN Q.931 message.

New features for G.723.1 and G.728 codecs

This release provides support for enabling the following features for G.723.1 and G.728 codecs:

- Dual-tone multifrequency (DTMF)-tone-passing using RFC 2833
- Quality of service (QoS) statistics and adaptive-jitter-buffer

The previous implementation of G.728 and G.723 did not support RFC2833 or QoS. These new features are supported in TAOS 10.1.0 and later releases, but they are not backwardly compatible with older TAOS versions (9.0, 9.1 and 10.0).

The voice payload travels properly through third-party gateways. However, QoS statistics are ignored by third-party gateways if they do not recognize the QoS Real Time Protocol (RTP) extension.

The following table shows the supported features by codec:

Table 3-12. Features supported by codec

codec	QoS Polling	RFC2833	Adaptive Jitter Buffer
G.711 mu-law	yes	yes	yes
G.711 a-law	yes	yes	yes
G.729	yes	yes	yes
G.728	yes	yes	yes
G.723	yes	yes	yes
G.723 6.4kps	yes	yes	yes

Note MultiDSP modem firmware must be upgraded from V0.2.4 to V0.2.8 or later, digital signal processor (DSP) firmware must be upgraded from V4.0.14 to V4.0.26 or later, and remote access server (RAS) firmware from V0.2002.0 to V0.2004.0 or later.

RFC 2833 for DTMF-tone-passing

The `dtmf-tone-passing` parameter permits the passing of DTMF tones using RTP packets, as defined in RFC 2833. The payload type can either be fixed (94) or be configured through dynamic payload type. The `dtmf-tone-passing` parameter is available for all supported `packet-audio-mode` parameters in the `voip` profile.

Note The `frgsm` setting for the `packet-audio-mode` parameter is not supported.

DTMF tone passing for RFC 2833 is enabled by setting the `dtmf-tone-passing` parameter in the `voip` profile to `rfc2833`.

Parameter	Setting
`dtmf-tone-passing`	Valid values are: ■ `dtmf-tone-passed-inband`—DTMF tones passed inband. ■ `dtmf-tone-passed-outofband`—The DTMF tones are sent out of band via H245 as signals with tone and duration information. ■ `rfc2833`—DTMF tones passed via RFC 2833. ■ `dtmf-tone-passed-outofband-alphanumeric`—The DTMF tones are sent out-of-band via H.245, with alphanumeric characters indicating specific tones and no duration information.

Request packet pass-through call (RCCP) message processing

RCCP messages that turn DTMF detection on or off are processed normally with the following exceptions:

- If a TAOS unit receives an RCCP message from the softswitch that attempts to turn on DTMF detection (tag 0x75 is set to 01) in which tag 0x3E contains a

value other than 96-127, that message is rejected. The TAOS unit responds with a release channel request (RCR) message with a cause code for invalid information contents (0x64).

- If a TAOS unit receives an RCCP message from the softswitch that attempts to turn off DTMF detection (tag 0x75 is set to 00) in which tag 0x3E contains a value other than 96-127, it is ignored. The TAOS unit does not reply to it in the accept packet pass-through call (ACCP) message.
- If a TAOS unit receives an RCCP message from the softswitch that attempts to turn on DTMF detection that does not contain tag 0x3E, it returns an ACCP message set to the default value of 94.

Request modify packet pass-through call (RMCP) message processing

The following descriptions apply to a TAOS unit that has DTMF tone detection turned off.

- If a TAOS unit receives an RMCP message from the softswitch that attempts to turn on DTMF detection (tag 0x75 is set to 01) in which tag 0x3E contains a value within the range of 96-127, it returns an accept modify packet pass-through call (AMCP) message with tag 0x75 set to 01. Tag 0x3E is set to the value received in the RMPC message.
- If a TAOS unit receives an RMCP message from the softswitch that attempts to turn on DTMF detection (tag 0x75 is set to 01) that does not contain tag 0x3E, it returns an AMCP message with tag 0x75 set to 01. Tag 0x3E is set to the default value of 94.
- If a TAOS unit receives an RMCP message from the softswitch that attempts to turn on DTMF detection (tag 0x75 is set to 01) in which tag 0x3E does not contain a value within the range of 96-127, it returns an AMCP message with tag 0x75 set to 00. The call remains connected and uses inband tone passing instead of RFC2833 tone passing.

The following descriptions apply to a TAOS unit that has DTMF tone detection turned on.

- If a TAOS unit receives an RMCP message from the softswitch that attempts to turn off DTMF detection (tag 0x75 is set to 00) that does not contain tag 0x3E, it returns an AMCP message with tag 0x75 set to 00. Tag 0x3E is not be included in the AMCP message.
- If a TAOS unit receives an RMCP message from the softswitch that attempts to turn off DTMF detection (tag 0x75 is set to 00) in which tag 0x3E contains a value within the range of 96-127, it returns an AMCP message with tag 0x75 set to 00, but does not return tag 0x3E.

Quality of Service (QoS) statistics

The `rtpqos-polling-enable` parameter enables the collection of statistics for both directions of calls exchanged through RTP header extensions. The information is then available to a call logging (CL) server at the end of each call. The statistics exchange is

available only for MultiVoice™. This capability is available for all supported `packet-audio-mode` parameters in the `voip` profile.

Parameter	Setting
`rtpqos-polling-enable`	Valid values are: `yes`—rtpqos polling enabled `no`—rtpqos polling disabled



Note The `frgsm` setting for the `packet-audio-mode` parameter is not supported.

Adaptive jitter buffer

The `ena-adap-jitter-buffer` parameter enables the algorithm that allows the jitter buffer depth to be determined at run-time so that the jitter buffer can be optimized for both delay and voice quality. `ena-adap-jitter-buffer` is available for all `packet-audio-mode` parameters in the `voip` profile.

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



Note The `frgsm` setting for the `packet-audio-mode` parameter is not supported.

`ss7voip` debug command modified to report tone passing method

If you use the `ss7voip` debug command with the `-s` option, the current method of DTMF tone passing is displayed for each session. If a session is using RFC 2833 tone passing, the dynamic payload type associated with the session is also printed, as shown in the following example:

```
admin> ss7voip -s
        SS7VOIP Session 145b6bc0
        ====================
        ss7CallRef(4):  1
        routeID:        2
        dsp:            {{ 1 6 3 } 0}
        VOIP call persistence mode: Disabled
        DTMF detection: In Progress
        voipPortMode:   1
        listenIp:       28.28.28.28
        listenRtpPort:  2000
        sendIp:         1.2.3.4
        sendRtpPort:    2001
        packetAudioMode:        0
        framesPerPacket:        2
        rtpSocket:      6014
        portReady:      TRUE
```

```
sessName:       V:SS7:1
sessUp:         TRUE
DTMF passing:   RFC2833        (new)
DTMF Payload Type:      0x66   (new)
```

Special trunk group for hairpin calls

A new `hairpin-trunk-group` parameter in the `voip` profile specifies a trunk group for use with hairpin calls (calls sent back in the direction from which they were transmitted).

If the `use-trunk-group` parameter is enabled in the `system` profile, hairpin calls seek outgoing trunks that match the `hairpin-trunk-group`. The `trunk-group` parameter in the `t1` or `e1` profile is used for the match.

You can use the hairpin trunk group only if the `use-trunk-group` parameter is set to `yes` in the `system` profile. The `num-digits-trunk-groups` parameter in the `system` profile determines the active digits.

Parameter	Setting
`hairpin-trunk-group`	If `system:use-trunk-group` is set to `yes`, this parameter specifies a trunk group for use with hairpin calls. The setting of the `system:num-digits-trunk-groups` parameter determines the active digits. The valid range is 0 through 9999, consistent with the values of the `t1:trunk-group` parameter. With the default setting of `0`, any trunk group is chosen.

For example, the following parameter settings set `hairpin-trunk-group` to 7, consistent with the `Trunk Group` in the T1 or E1 profile.

```
hairpin-trunk-group = 789
num-digits-trunk-groups = 1
```

Enhanced speech transmission for VoIP G.711 codec

The new `g711-voice-natural` parameter provides a special filter that enhances the perception of transmitted speech. This feature is now configurable on a trunk line interface basis. The enhancement applies only to supported G.711 μ-law and G.711 a-law codecs.

`g711-voice-natural` is administered through the T1 or E1 trunk profile. Each trunk has its own configuration. The `g711-voice-natural` parameter applies to both H.323 calls and IPDC calls established over these trunks. As a call is being established, session information (such as audio mode) is sent to the MultiDSP card. The T1 or E1 profile is read at the start of a call so that the initial session information sent to the MultiDSP card contains the `g711-voice-natural` mode. This means that on originating calls, G.711 encoder applies `g711-voice-natural` processing if it is enabled.

Modifications to the `g711-voice-natural` parameter take effect only on new calls. Existing calls are not affected.

Voice enhancement is automatically tuned off during voice announcements and transparent fax/modem calls.

Configuring frames per packet for each codec

You can configure each of the available codecs and the number of frames per packet to negotiate using the `codec-options` subprofile. By default, all codecs are enabled and their frames per packet are set to 2. You can disable codecs selectively as required by your network. You cannot, however, disable the codec specified as preferred codec in the `packet-audio-mode` parameter.

Separate frames per packet settings for each codec

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



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

G.723 codec operates at 5.3kps and 6.4kps

In compliance with the ITU-T Recommendation for G.723 coder, when G.723 codec is enabled, it operates at either 5.3kps or 6.4kps. By setting `g723-enabled` to `yes` in `voip:codec-options`, the codec is enabled at both bit rates. The `g723-fpp` parameter determines the number of voice frames per RTP packet for the codec at both bit rates.

Configuring codec settings

Following are the parameters available in `voip:codec-options`.

Parameter	Setting
`g711-ulaw-enabled`	Enables G.711 mu-law codec. Valid values are `yes` (default) or `no`.
`g711-ulaw-fpp`	Number of voice frames per RTP packet for G.711 mu-law codec. Valid values are whole numbers from 1-10. The default value is 2.
`g711-alaw-enabled`	Enables G.711 a-law codec. Valid values are `yes` (default) or `no`.
`g711-alaw-fpp`	Number of voice frames per RTP packet for G.711 a-law codec. Valid values are whole numbers from 1-10. The default value is 2.

Parameter	Setting
`g723-enabled`	Enables G.723 codec at both 5.3kps and 6.4kps. Valid values are `yes` (default) or `no`.
`g723-fpp`	Sets the number of voice frames per RTP packet for G.723 codec at both 5.3kps and 6.4kps. Valid values are whole numbers from 1-10. The default value is 2.
`g728-enabled`	Enables G.728 codec. Valid values are `yes` (default) or `no`.
`g728-fpp`	Number of voice frames per RTP packet for G.728 codec. Valid values are whole numbers from 1-10. The default value is 2.
`g729-enabled`	Enables G.729 codec. Valid values are `yes` (default) or `no`.
`g729-fpp`	Number of voice frames per RTP packet for G.729 codec. Valid values are whole numbers from 1-10. The default value is 2.
`frgsm-enabled`	*Currently not supported.* Enables FRGSM codec. Valid values are `yes` (default) or `no`.
`frgsm-fpp`	*Currently not supported.* Number of voice frames per RTP packet for FRGSM codec. Valid values are whole numbers from 1-10. The default value is 2.

MultiVoice® control of trunk gain and loss

Gain (volume) control for a call can now be configured in transmit and receive directions for each time division multiplex (TDM) trunk interface. Input Pads configure gain or loss for input from a TDM interface. Output pads configure loss for output to a TDM interface.

Gain can be configured within the following ranges:

- Input Pads— from -3 to +9 dB in 1 dB steps
- Output Pad—from 0 to -12 dB in 1 dB steps



Note Negative values indicate loss. Positive values indicate gain. The value zero means no loss or gain is provided.

Configured values apply for the life of a call, including voice and break-in announcements. The input and output pad configurations also apply for selfcalls and hairpin calls, and apply to both H.323 calls using internet protocol device control (IPDC). When the `input-pad` and `output-pad` parameters are changed, changes take affect on new calls. Existing calls are not affected.

`voip-gain-control` subprofile

T1 and E1 `line-interface` subprofiles include a new `voip-gain-control` subprofile that holds the new configuration parameters `input-pad` and `output-pad`. The default

setting for both of these new parameters is `0db` (zero decibels). Configuration of these parameters for T3 lines is done through the individual T1 profiles.

The following sample commands show the `voip-gain-control` subprofile, added to the `line-interface` subprofile in the T1 and E1 profiles.

```
admin> read t1 {1 1 1}
T1/{ shelf-1 slot-1 1 } read

admin> list line-interface
[in T1/{ shelf-1 slot-1 1 }:line-interface]
enabled = no
frame-type = esf
encoding = b8zs
...
r1-modified = no
ss7-continuity = { loopback single-tone-2010 }
voip-gain-control = { 5db-gain 3db-loss}
...

admin> list voip-gain-control
[in T1/{ shelf-1 slot-1 1 }:line-interface:voip-gain-control]
input-pad = 5db-gain
output-pad = 3db-loss
```

The following table describes the valid settings for the new `input-pad` and `output-pad` parameters.

Parameter	Specifies
`input-pad`	Amount of call loss or gain for input from the TDM interface. The default setting is `0db`. Valid values are: ■ `0db` ■ `1db-loss` ■ `2db-loss` ■ `3db-loss` ■ `1db-gain` ■ `2db-gain` ■ `3db-gain` ■ `4db-gain` ■ `5db-gain` ■ `6db-gain` ■ `7db-gain` ■ `8db-gain` ■ `9db-gain`

Parameter	Specifies
`output-pad`	Amount of call loss for output toward the TDM interface. The default setting is `0db`. ■ `0db` ■ `1db-loss` ■ `2db-loss` ■ `3db-loss` ■ `4db-loss` ■ `5db-loss` ■ `6db-loss` ■ `7db-loss` ■ `8db-loss` ■ `9db-loss` ■ `10db-loss` ■ `11db-loss` ■ `12db-loss`



Note When the input pad is configured to apply a gain to the TDM signal, use care to avoid saturation. If the largest value of the input signal is already near its range limit, and additional gain is applied through the input pad, the signal will saturate at the maximum value allowed. Large amounts of saturation can cause severe speech distortion.

Echo cancellation support for all audio codecs

TAOS 10.1.0 supports an echo canceller for G.728 and G.723.1 codecs, compliant with the International Telecommunications Union's (ITU) G.168-2000 standard. This echo canceller provides up to 64ms echo tail cancellation to cancel the echo from severe hybrid impedance mismatch. Previously, the ITU G.168-2000 standard for echo cancellation was available for the G.711 and G.729A codecs.

No configuration is required.

Enhanced MultiDSP support for G.723

G.723 is now available for the MultiDSP-240 and MultiDSP-288 slot cards. You can set the `packet-audio-mode` parameter to `G723` or `G723-6.4kps`.

New `packet-audio-mode` parameter values

If you have MultiDSP-240 and MultiDSP-288 slot cards in the same chassis, you can now set the `packet-audio-mode` to `G723` and `G723-6.4kps` (and `G729`, `G711-ulaw`, and `G711-alaw`), but you cannot use the values `G728` and `frgsm`.

If you have a MultiDSP-96 slot card with a MultiDSP-240 or MultiDSP-288 slot card in the same chassis, the `packet-audio-mode` parameter can only be set to `G711-ulaw`, `G711-alaw`, or `G729`.

If any MultiDSP-480 slot card is active, `packet-audio-mode` can only be set to `G711-ulaw` and `G711-alaw`.

New `call-route-type` parameter value

The `call-route-type` parameter in the `call-route` profile has a new value of `G723-call-type` for call-route tables of type number 9. G.723 and G.723-6.4kbps are now supported for all MultiDSP-240 and MultiDSP-288 slot cards.

Silence suppression and adaptive jitter buffer

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

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

E1 R2 cause codes enhancement

With this release, TAOS gateway units recognize and map E1 R1/R2 Group II forward and Group B backward signaling for Voice over IP (VoIP) call handling. This capability provides end-to-end transport of the R2 group B signal received at the egress Gateway. In scenarios that do not have E1 R1/R2 trunks at both ends of the call, the Group II and Group B signals are mapped or spoofed as required.

Several scenarios are accommodated:

- End-to-end connection between MF-R2 trunks—a virtual MF-R2 call setup with `true-connect` enabled. This scenario is like an extension to the `true-connect` feature, which suspends connection of a subscriber until the call is actually answered by the far end.
- Call from an MF-R2 trunk to an ISDN line—The Group B signal used for a setup response is the E1 `group-b-answer-signal` on the ingress gateway. This is triggered on the receipt of the alerting signal and depends on the `signaling-model` parameter that is set in the `voip` profile. Call failure group B signals are mapped from the ISDN disconnect cause code received at the egress gateway, as shown in the following table.

Initial signal	Mapped signal
R2 group A National congestion (SIGA_4)	ISDN no circuit available (cause code 34)
R2 group A International exchange congestion (SIGA_15)	ISDN no circuit available (cause code 34)

Initial signal	Mapped signal
ISDN special information tone (cause code 4)	R2 group B special information tone (SIGB_2)
ISDN user busy (cause code 17)	R2 group B subscriber line busy (SIGB_3)
ISDN no circuit available (cause code 34)	R2 group B congestion (SIGB_4)
ISDN unassigned number (cause code 1)	R2 group B unallocated number (SIGB_5)
ISDN destination out of order (cause code 27)	R2 group B subscriber line out of order (SIGB_8)
ISDN no circuit available (cause code 34)	Default for any non-connecting B signal.



Note E1 R2 cause codes are CCITT ITU Q.441 signals, and are implemented specifically for H.323. They are not currently supported by other VoIP protocols.

- Call from an ISDN line to an MF-R2 trunk—The cause code mapping follows what is described in the preceding table. Alerting and proceeding are triggered by the Group B signal. If the `signaling-model` parameter in the `voip` profile is not set to `fast-proceeding`, the R2 signaling might exceed the T303 time-out. The calling party class is taken from the `group-ii-signal` parameter in the E1 `line-interface` profile of the egress gateway.
- Call from an MF-R2 trunk to a channel associated signaling (CAS) trunk—CAS provides very little information, so all R2 signals are spoofed at the incoming trunk. All of the R2 signals are generated locally based on hard coded values or E1 parameters set in the ingress gateway. The call does not proceed with a positive group B signal until alerting is seen from the egress gateway. Because alerting is not a CAS signal, the R2 signals do not truly reflect the signaling of the far-end VoIP peer. This depends largely on the setting of the `signaling-model` parameter in the E1 `line-interface` profile.
- Call from a CAS trunk to an MF-R2 trunk—Call setup handled simply by H.323. Alerting may be delayed, depending upon the setting of the `signaling-model` parameter in the E1 `line-interface` profile.

New parameters

The parameter `true-setup-status` is added to the `voip` profile to allow reporting of the virtual status of the distant line via VoIP at call setup time. This allows this feature to be disabled where it does not meet the needs of national networks. The parameter can be enabled by entering a setting of `yes`, or disabled with a setting of `no`. The default, `no`, is shown in the following example.

```
[in VOIP/{0 0}]
true-setup-status = no
```

The group-b-no-charge-signal parameter has been added to the E1 line-interface profile. The following table shows the valid values for this parameter.

Parameter	Settings
group-b-no-charge-signal	Valid values are: ■ signal-b-1 ■ signal-b-2 ■ signal-b-3 ■ signal-b-4 ■ signal-b-5 ■ signal-b-6 ■ signal-b-7 (the default) ■ signal-b-8 ■ signal-b-9 ■ signal-b-10 ■ signal-b-11 ■ signal-b-12 ■ signal-b-13 ■ signal-b-14 ■ signal-b-15

Some specific national R2 specifications allow for a group B response of "subscriber line-free" so that the called subscriber line is not charged for a toll call. The group-b-no-charge-signal parameter specifies the group B signal that is sent by an egress gateway as the "subscriber line-free" signal.

On a ingress gateway, the setting of this parameter is used to detect the no charge signal from the distant end. This parameter is checked dynamically during the R2 signaling stage of the call. Changes to this parameter occur instantaneously.

If the true-setup-status parameter in the voip profile is not enabled, all R2 calls are acknowledged by the signal identified by the group-b-answer-signal parameter in the E1 line-interface profile.

Silence suppression for G.728 codec

Because no method for silence compression is defined in the ITU G.728 standard, Lucent is implementing proprietary voice activity detector (VAD) discontinuous transmission (DTX) algorithms for use with G.728. The object of the VAD is to discriminate between active and inactive speech segments. The DTX algorithm determines when to transmit comfort noise information to the distant gateway. The distant gateway uses a Comfort Noise Generator (CNG) to synthesize background (comfort) noise.

Setting silence suppression for G.728 codec on a MAX TNT or APX unit

The settings of the `silence-det-cng` parameter that enable silence detection are now effective when the `packet-audio-mode` parameter in the `voip` profile is set to `g728`. These options were not previously effective for this codec. Specify one of the following `silence-det-cng` settings to enable or disable this feature:

- no—disables silence detection and comfort noise generation
- yes—enables silence detection and comfort noise generation

Complex codecs are not allowed in a MAX TNT or APX device with a functioning MultiDSP2 card. If a MultiDSP2 card is available in the unit when the `packet-audio-mode` is set to `g728`, the `voip` profile is not updated and an error message is displayed.

The silence threshold cannot be set manually when the `packet-audio-mode` parameter is set to `g728`. If the `packet-audio-mode` is g728 and an attempt is made to set the `silence-threshold` parameter, the `voip` profile is not be updated and an error message is displayed.

Calling Line Identification (CLID) indicator enhancement

In TAOS 10.1, transmission of the Calling Party Number information element from an incoming voice over IP (VoIP) call on an E1/T1 interface over H.225/Q.931 to the receiving unit. Calling party number information, including calling line identification presentation (CLIP) and calling line identification restriction (CLIR) indicators, is passed from the incoming ISDN setup message over H.225/Q.931 to the destination gateway for inclusion in the outgoing ISDN setup message.

This capability improves calling line identification (CLID) interconnectivity between networks by transparent end-to-end transmission of the presentation indicator field of the calling party information element. You can configure individual E1 or T1 ports (ingress and egress ports) to override this field in both ends of the network.

Because gateways might misinterpret the CLID as a result of encoding the Calling Party Number information element, you can configure the sending of this element between gateways on a unit-wide basis by using the `extended-clid-support` parameter. in the `voip` profile. By default, this parameter is set to `no`. This setting is unnecessary if third party equipment operates completely in accordance with specification H.225/Q.931.

Example scenario

The following scenario, illustrated in Figure 3-3, describes the sequence of events that occurs for transmission of CLID from an incoming call to the receiving unit.

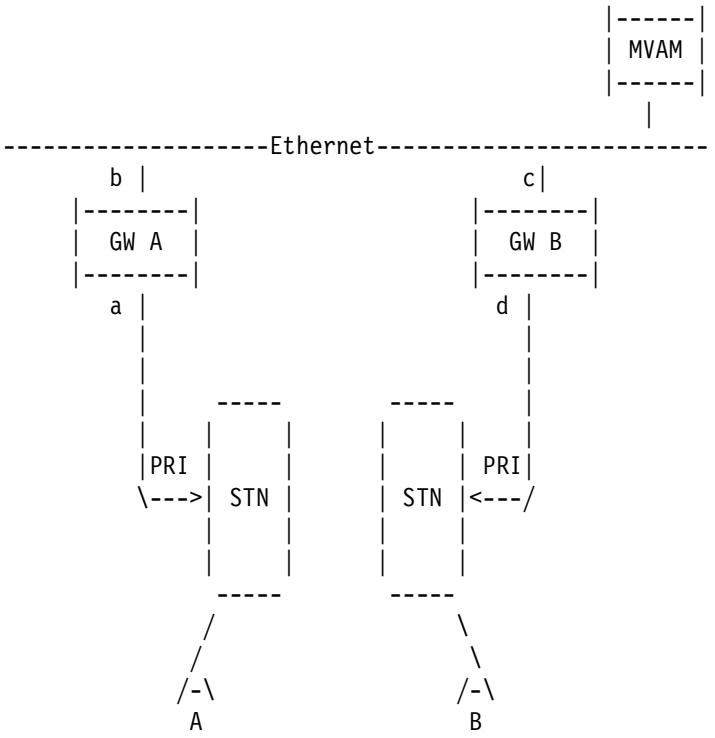
1. Phone A dials gateway A (GW A). From the incoming Q.931 setup message, the gateway extracts and stores the Calling Party information element from the ingress call a.
2. GW A contacts the MultiVoice Access Manager (MVAM) over H.323 and is given the IP address of gateway B (GW B).
3. If `extended-clid-support` is set to `yes`, GW A sends the Calling Party information element over H.225/Q.931 to GW B, calls b to c.

Changing this parameter affects all modules on the unit because whether the destination gateway is able to decode the calling party information element is unknown. In case it is not, to avoid misinterpretation of the CLID, `extended-clid-support` defaults to `no`. If decoding is in full accordance with H.225/Q.931 this is not a problem.

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

The E1 and T1 `tx-clir-flag-in-voip` parameter is set to `no` by default.

Figure 3-3. Sequence of events in passing CLID to outgoing ISDN setup message



Note The presentation and screening indicators are passed only when present on the ingress line as part of Q.931, which excludes T1 channel associated signaling (CAS) and E1/R2 signaling.

Enabling CLID indicator transmission

To enable CLID indicator transmission for calls on a line interface, in the T1 or E1 profile for the line interface, set the `tx-clir-flag-in-voip` to `yes`. By default, this parameter is set to `no`.

```
[in E1/{ shelf-1 slot-9 1 }:line-interface]
enabled = yes
t-online-type = none
frame-type = g703
..
pri-prefix-number = ""
```

```
tx-clir-flag-in-voip = yes
trailing-digits = 2
t302-timer = 10000
..
```

To configure CLID indicator transmission on a unit-wide basis, in the `voip` profile, set the `extended-clid-support` parameter to `yes`. By default, this parameter is set to `no`.

```
[in VOIP/{ 0 0 }]
voip-index* = { 0 0 }
gatekeeper-ip = 134.112.45.220
gk-mlg-control = no
vpn-mode = yes
single-dial-enable = no
...
call-hairpin = no
call-keep-alive-timeout = 300
clid-suppress = no
extended-clid-support = yes
true-connect-enable = no
g711-transparent-data = no
..
```

IP Device Control support for Voice over IP tones

In TAOS 10.1.0, a MultiVoice® gateway can generate call progress tones (busy, alerting, etc.) over a MultiDSP slot card using IP Device Control (IPDC) Revision 0.12 protocol signaling.

IPDC defines a specification for generating tones, such as dual-tone multifrequency (DTMF) or arbitrary frequencies, but it does not have a means for signaling several common call progress tones (dial tone, alerting, busy, network busy and unobtainable). These tones have been defined defined in TAOS and are used already by H.323 Voice over IP (VoIP) in TAOS.

In TAOS 10.1, this capability has been added to the IPDC VoIP implementation. In addition, the TAOS implementation of IPDC also can generate a foreign country-specific call progress tone .

These proprietary extensions include a country identifier added to the `NSUP` message the MultiVoice® gateway sends to the softswitch. The country identifier corresponds to the `country` setting in the `system` profile. This setting can be used by the softswitch to associate a country-of-origin with a MultiVoice® gateway for the subsequent signaling of country-specific call progress tone generation on that or another MultiVoice® gateway.

The second extension includes a new tone type added to the Set Tone or Announcement (`STN`) message. This tone type signifies that the tone string in the `STN` identifies one of the well-known call progress tones and that the `STN` message also contains a country identifier. The MultiVoice® gateway uses the tone string and country identifier to generate a country-specific call progress tone.

TAOS capability has also been extended to enable the TAOS unit to process `STN` messages when the current DS0 state is loopback, in addition to idle.

Changed NSUP message Tag 0xC1 (Country Identifier)

The new NSUP message tag is 0xC1 (country identifier). The tag length is 1 byte and the tag value is one of the following:

0xC1 value	Country name
0x01	argentina
0x02	australia
0x03	belgium
0x04	china
0x05	costa rica
0x06	finland
0x07	france
0x08	germany
0x09	hong kong
0x0A	italy
0x0B	japan
0x0C	korea
0x0D	mexico
0x0E	netherlands
0x0F	new zealand
0x10	singapore
0x11	spain
0x12	sweden
0x13	switzerland
0x14	us
0x15	uk
0x16	brazil

The country names are possible values of the country setting in the system profile. The list corresponds to the list of countries for which country-specific call progress tones are supported in TAOS (already used by H.323 VoIP). The value for tag 0xC1 is the numeric equivalent of the value country in the system profile.

For example, the following commands result in tag 0xC1 with a value of 0x15 when an NSUP message is sent:

```
admin> read system
SYSTEM read
admin> list
[in SYSTEM]
...
country = us
...
```

```
Protocol=0x4b,  Correlator (4): 80000037
Message: 0x0081
Tag ID=0x01, Data (1): 01
Tag ID=0x02, Data (6): 64 74 6e 74 31 34
Tag ID=0x03, Data (9): 49 41 53 43 54 4e 54 31 42
Tag ID=0x04, Data (2): 00 10
Tag ID=0x05, Data (8): 31 32 33 34 35 36 37 38
Tag ID=0xc1, Data (1): 15
```

Note that as additional countries are added to the `system` profile, new numeric values for tag 0xC1 become possible. The numeric representation of a country is of significance to the MultiVoice® gateway only, however. The gateway passes it to the softswitch in the `NSUP` message, which stores it and later passes it back to a MultiVoice® gateway in an `STN` message.

Changed STN message tag 0x49 (Tone Type)

The new tag value is tag `0x49: 0x41` (Call Progress Tone). Value 0x41 signals that the STN message contains a request to apply or cancel a call progress tone.

Associated with tag `0x49` is a set of new values to indicate the type of call progress tone to generate. These values are specified in tag `0x33` (Tone String) whenever `0x49` has value `0x41`, as follows.

Tag 0x33 value	Call progress tone
1	dial tone
2	alerting tone
3	busy tone
4	network busy tone
14	unobtainable tone

TAOS also supports two other call progress tones: pin tone and error tone. They are not country-specific, however, and are relevant only for the H.323 VoIP implementation in TAOS.

The tag `0xC1` (defined earlier) is added to the STN message whenever the STN message contains a request to apply or cancel a call progress tone (when tag `0x49` has the value `0x41`).

The value of tag `0xC1` is used as the country of origin when determining the frequency, duration and cadence of the call progress tone. If tag `0xC1` is omitted, the value of `country` in the `system` profile is used as the country of origin.

STN/ASTN usage

The semantics of the `STN` messages and Acknowldegement of `STN` (`ASTN`) messages remain the same as for other tones and announcements.

- To start a call progress tone, send an `STN` message with tag 0x4A set to 0x00 (Apply Tone).
- To stop a call progress tone, send an `STN` message with tag 0x4A set to 0x01 (Cancel Tone).

All of the five supported call progress tones play continuously until explicitly canceled.

If the MultiVoice® gateway is unable to accept an `STN` call progress tone request, it responds with an `ASTN` with status `0x01` (operation failed).

Interoperability with softswitches

The TAOS 10.1 modifications to the IPDC implementation are fully interoperable with any softswitch supporting IPDC Revision 0.12.

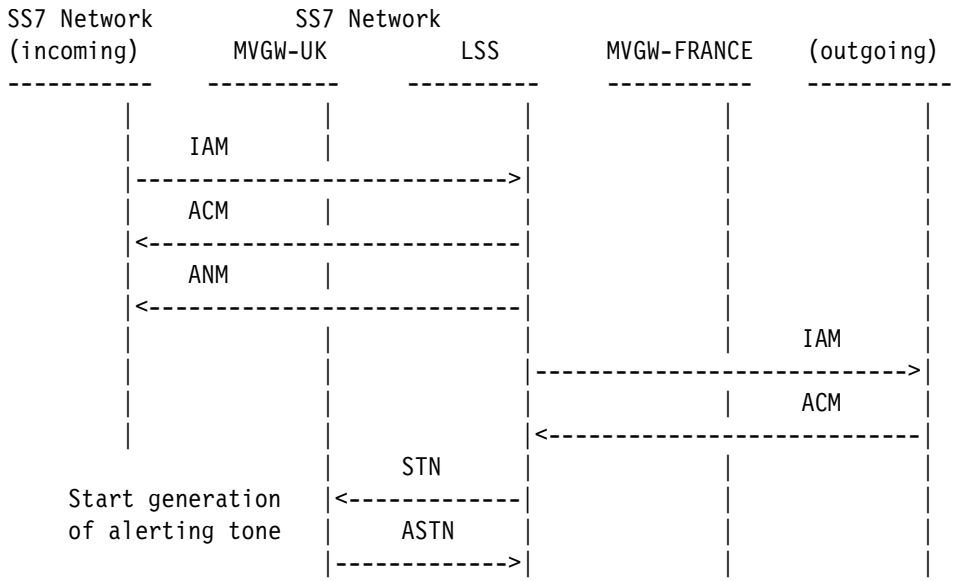
Compliance with IPDC requires that unrecognized tags are ignored. (See "IPDC Use Cases Document", Revision 1.1, Level (3) Communications, Inc). For example, a softswitch running Revision 0.12 receives an `NSUP` with `Tag 0xC1`. Because the softswitch does not recognize the tag, it ignores it and processes the `NSUP` as if `Tag 0xc1` had not been included.

Call Flow: Ringing, then answered

The following section illustrates the call flow in a scenario involving two MultiVoice® gateways, one in the United Kingdom (MVGW-UK) and one in France (MVGW-FRANCE) and one Lucent SoftSwitch (LSS).

The calling party is in UK, the called party is in France. To allow the calling party to hear an alerting tone specific to France, the LSS sends MVGW-UK an `STN` with `tag 0xC1 = 0x07, tag 0x49 = 0x41, tag 0x33 = "2", tag 0x4A = 0x00` and other tags as required for `STN`.

Note that the LSS received `tag 0xC1 = 0x07` from MVGW-FRANCE when MVGW-FRANCE sent an NSUP to the LSS.



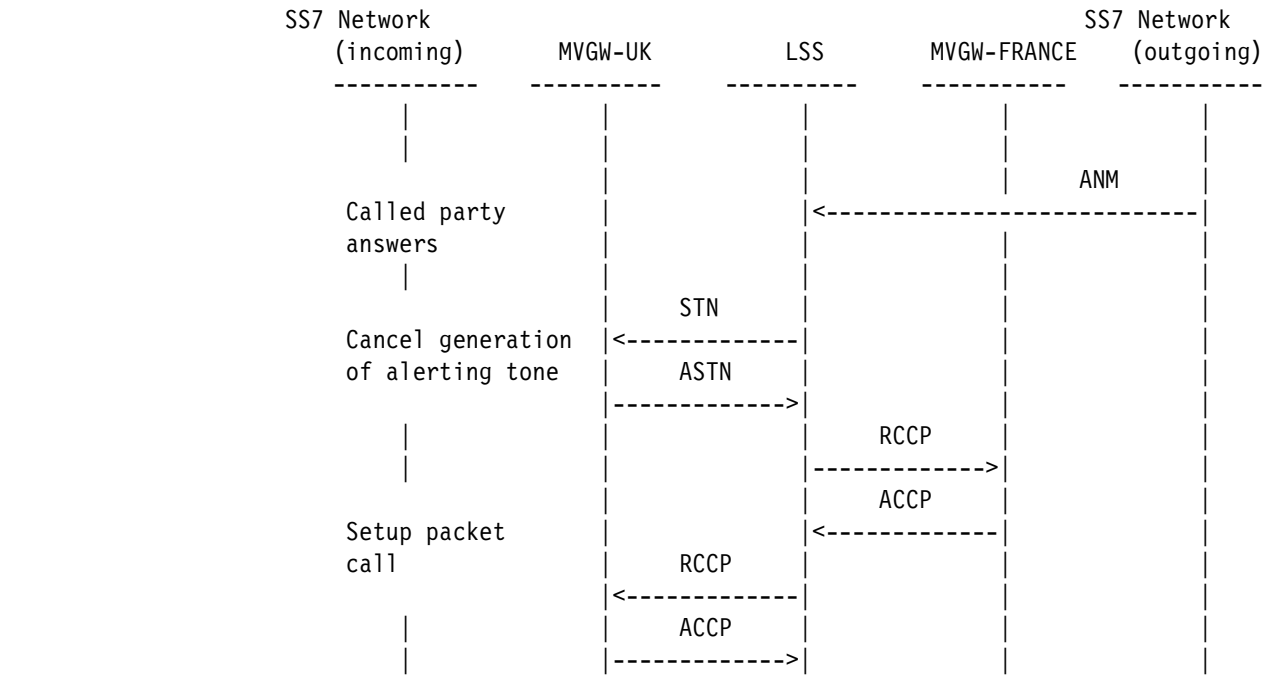
The message content follows:

```
LSS->MVGW: (STN - apply "alerting" call progress tone)

    Protocol=0x4b,  Correlator (4): 00000000
    Message: 0x0073
    Tag ID=0x07, Data (2): 00 01
    Tag ID=0x0d, Data (2): 00 01
    Tag ID=0x15, Data (2): 00 01
    Tag ID=0x49, Data (1): 41
    Tag ID=0x4a, Data (1): 00
    Tag ID=0x32, Data (1): 01
    Tag ID=0x33, Data (1): 32
    Tag ID=0xc1, Data (1): 07
MVGW->LSS: (ASTN - command started)

    Protocol=0x4b,  Correlator (4): 00000000
    Message: 0x0074
    Tag ID=0x07, Data (2): 00 01
```

When the called party answers, the LSS stops the alerting tone by sending MVGW-UK an STN with the same tags as above except tag 0x4A = 0x01. The packet call can then be set up.



The message content follows:

```
 LSS->MVGW: (STN - cancel "alerting" call progress tone)

        Protocol=0x4b,  Correlator (4): 00000000
        Message: 0x0073
        Tag ID=0x07, Data (2): 00 01
        Tag ID=0x0d, Data (2): 00 01
        Tag ID=0x15, Data (2): 00 01
        Tag ID=0x49, Data (1): 41
        Tag ID=0x4a, Data (1): 01
        Tag ID=0x32, Data (1): 01
        Tag ID=0x33, Data (1): 32
        Tag ID=0xc1, Data (1): 07

    MVGW->LSS: (ASTN - command completed)

        Protocol=0x4b,  Correlator (4): 00000000
        Message: 0x0074
```

If call setup never progresses to the point where a packet call is actually set up (an `RCCP--Request Pass Through Packet Call`) is sent and accepted by the MultiVoice® gateway), but at least one call progress tone has been generated, and it is time to take down the call, then when VoIP call persistence is enabled on the gateway, the Softswitch must send the gateway an RCR at the end of the call so that the gateway can free the resources that were used to generate the call progress tone or tones.

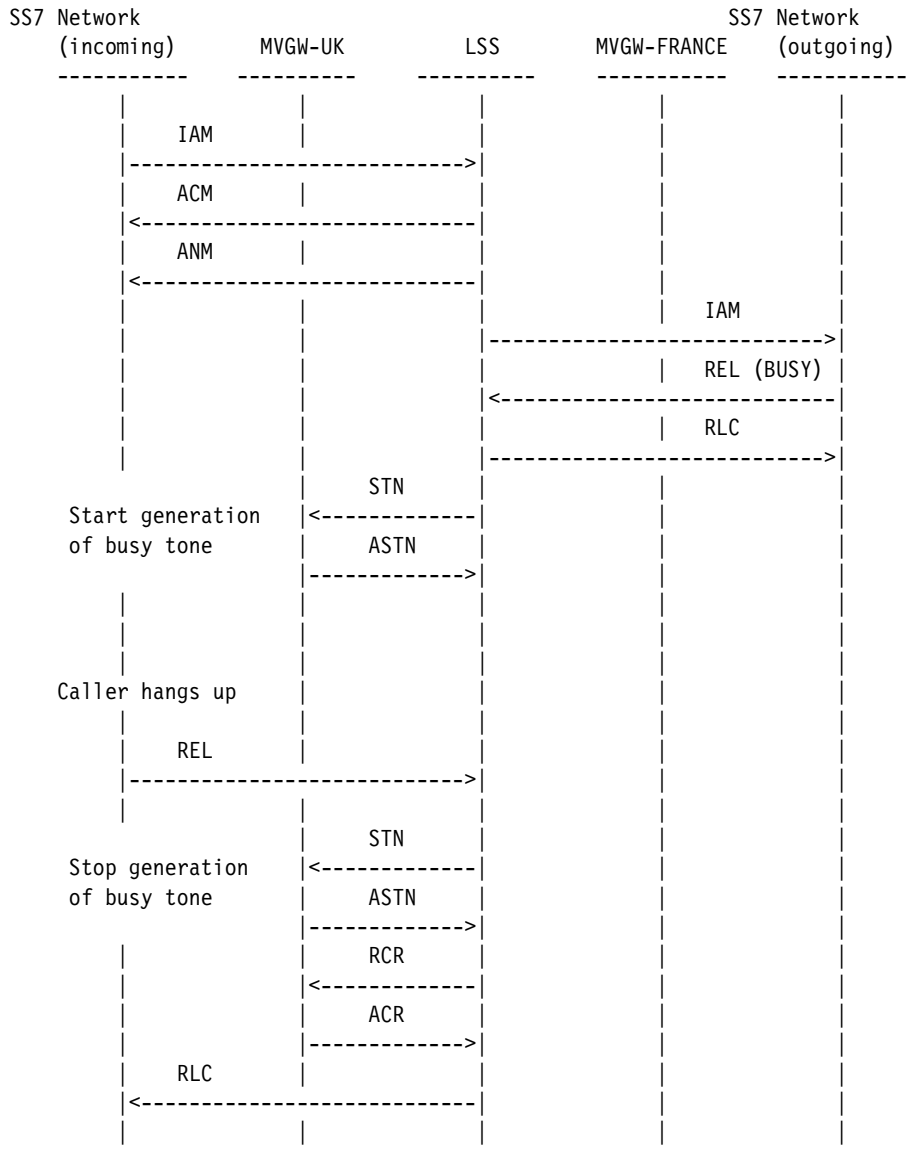
To see if VoIP call persistence is enabled, check the setting of `ss7voip-call-persistence` in the `voip` profile, as in the following example:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> list
[in VOIP/{ 0 0 }]
...
ss7voip-call-persistence = yes
...
```

Scenario: Busy, then hangup

In the following call flow scenario, the called party is busy. The softswitch directs the MultiVoice® gateway to generate a busy tone specific to France. After a short while, the calling party hangs up. Since VoIP call persistence is enabled, the softswitch must send the gateway an RCR to allow it to free the resources associated with call progress tone generation when VoIP call persistence is enabled.



The RCR allows the MultiVoice® gateway to free the resources (such as a MultiDSP slot card) associated with the VoIP call route that was set up for call progress tone generation when the first STN was received. If VoIP call persistence was disabled, the RCR would be unnecessary.

Including the NSF information element in Q.931 setup messages

In TAOS 10.1.0, users can configure the value sent in the Network Specific Facilities (NSF) information element of the Q.931 Setup message.

Call-by-call vs. network-specific-facilities parameters

The T1 line profile includes a `call-by-call` parameter to set the NSF information element (IE). The parameter is used only for network-to-network calls and for interfacing with specific service providers. The three high-order bits of the NSF IE are automatically set to 111 for parameterized, expansion, and feature/service.

To preserve the existing functionality of the `call-by-call` parameter, a new parameter has been added to set the full 8 bits of the NSF IE. This new parameter is called `network-specific-facilities` and is located in the T1 line profile, immediately following the `call-by-call` parameter.

The `network-specific-facilities` parameter is valid for both Voice over IP (VoIP) and RAS. Therefore, in a universal port application, if the VoIP calls should include NSF, you must use the `network-specific-facilities` parameter and set the `call-by-call` parameter to `0`.

The following table compares the two parameters:

	`call-by-call` parameter	**`network-specific-facilities` parameter**
Range	`0-31`	`0-255`
	Only the low 5-bits are relevant.	All 8 bits must be configured.
Parameter Usage	Non-VoIP only. Cannot be used with SIP or H.323.	Must be used for VoIP but also valid for non-VoIP.
Precedence	Higher	Lower
Bit Usage	High-order 3 bits set to 111 for AT&T — 111xxxxx.	All 8-bits must be explicitly set.

Configuring NSF IE values

As shown in the table above, all 8-bits of the desired NSF field for VoIP must be configured in the `network-specific-facilities` parameter, including any parameterization, expansion, and feature/service information if your service provider is AT&T. The possible NSF values for the 5ESS switch are described in detail in the following document:

`Lucent 5ESS-2000 Switch ISDN Primary Rate Interface Spec`

`5E10 and Later Software Releases`

`Document # 235-900-342, July 1998`

`Section 4.3.3.14`

As illustrated in Table 4.3-28 of the 5ESS document, most NSF values begin with 111 in bits 6-8. For example, MEGACOM is 11100011. Therefore, the value specified by the `network-specific-facilities` parameter must be set to 227—it should *not* be set to 3.

Other service providers may have different definitions for the individual bits in the NSF IE, so the full NSF must be configured explicitly in the value specified by the `network-specific-facilities` parameter.

Note Even if you need the high-order bits set to 111, you must use the `network-specific-facilities` parameter with the full 8-bits configured. MultiVoice® gateway users cannot use the `call-by-call` parameter.

Sample message

The following sample message assumes that the `network-specific-facilities` parameter is set to 227. The message is shown using the `pridisplay` command on the T1 card and only the relevant lines of the message are displayed:

```
PRI-XMIT-0/2(task "l1Task" at 0x8012b0d0, time: 892.43)
   Prot=08:Q.931 05: SETUP                call reference (Orig.) 00003
   ....
20:  Network-specific facilities
   02  length            Length = 2
   00  octet 3  00000000 '.'   0.
   e3  octet 3a 11100011 '.' 227.
   ....
```

New `network-specific-facilities` parameter

A new configuration parameter called `network-specific-facilities` has been added to the T1 line profile. The default value is zero, as shown:

```
admin> read t1 { 1 1 1 }
T1/{ shelf-1 slot-1 1 } read

admin> list
[in T1/{ shelf-1 slot-1 1 }]
       ....
network-specific-facilities = 0
```

When the `network-specific-facilities` parameter is set to zero, the NSF IE is not included in the outgoing Q.931 Setup message.

To include the NSF IE in the outgoing Q.391 Setup message, the full 8-bits must be configured and the `call-by-call` parameter must be set to zero. The range is `0` through `255`.

Handling of rogue RTP streams

In some cases, when a terminated or abandoned call under internet protocol device control (IPDC) is not cleared properly, the real-time protocol (RTP) connection for the call might not be cleared, and might continue to carry RTP packets. This invalid stream is referred to as rogue RTP. In this release, TAOS adds features to detect, report, and manage rogue RTP traffic.

Rogue RTP management

The following new subprofile, `rtp-problem-reporting`, has been added to the `voip` profile to enable and configure the parameters for detecting and handling rogue RTP streams.

```
[in VOIP/{ "" "" }:rtp-problem-reporting (new)]
enable = no
```

```
mult-media-rcpt-ok-time = 30
no-media-rcpt-ok-time = 60
```

Parameter	Setting
`enable`	`no` (the default): RTP problem reporting is disabled `yes`: RTP problem reporting is enabled
`mult-media-rcpt-ok-time`	Valid values from 1 to `65535` indicate the maximum number of seconds before multiple RTP streams are identified as rogue. The default setting is 30 seconds.
`no-media-rcpt-ok-time`	Valid values from 1 to `65535` indicate the number of seconds during which no RTP packets are received, before a reporting message is sent. The default setting is 360 seconds.

Rogue RTP detection

Two sets of conditions are used to indicate that a gateway is receiving rogue RTP packets. Both of the following conditions must be met before an RTP stream is identified as a rogue stream.

- Condition 1—At least two of the following must be true:
  - Conflicting synchronization source identifier (SSRC) information in RTP packet headers are detected on the port.
  - Too many RTP packet sequence number discrepancies are detected on the port.
  - More packets than expected are detected on the port.
  - Two RTP streams with different encoding types are detected on the port.
- Condition 2—Packets from at least two sources (IP address and port) are received on the port.

If these conditions persist for more than the number of seconds indicated by the `mult-media-rcpt-ok-time` parameter, the gateway clears the call with a release channel request (RCR) message and generates a syslog message.

The RCR message contains the following:

1. The cause code to indicate multiple streams (0x2B).
2. A new tag (defined in IPDC 0.18 as 0x69) to store source IP address and port of the RTP streams. There will be several of the these tags. The IP address and port pairs reflect the packets received in a small sampling window before sending the RCR message.

One of the following `LOG notice` messages is generated:

```
LOG notice, Shelf 1, Controller, Time: 12:14:58--
  No RTP stream received on RouteID 5
```

```
LOG notice, Shelf 1, Controller, Time: 13:17:12--
  Multiple RTP received on RouteID 6
  RogueSession:0 IP 135.92.52.181 port 2073
  RogueSession:1 IP 135.92.52.230 port 2073
```

Rogue RTP prevention

It is also possible for a gateway to send rogue RTP packets. If a softswitch does not inform the gateway that the far end has terminated its connection, the gateway continues to send RTP packets as a rogue RTP stream.

To prevent this situation, the gateway continues to monitor incoming RTP streams. Regardless of whether silence suppression is turned on, the gateway sends a periodic status message (defined as NRS in IPDC 0.18). If the gateway does not receive an RTP packet for the stream after the number of minutes specified in the `no-media-rcpt-ok-time` parameter, it sends an NRS an message. This message is sent again when twice the preceding time has elapsed, and repeated at intervals that continue to double the preceding interval. For example, if the value of the `no-media-rcpt-ok-time` parameter is set as 1, the NRS message is sent after 1 minute, and again after 2, 4, 8, 16 minutes, and increasingly greater intervals. A syslog message is also generated at each interval.

Support for new messages in ss7nmi output

The debug level command `ss7nmi -m` has been modified to display statistics for NRS messages as illustrated by the following.

```
admin> ss7nmi -m
IPDC message processing statistics:
        Message code      Received       Sent
        RCR   (0x0011):          1          0
        ACR   (0x0012):          0          1
        RCCP  (0x0013):          1          0
        ACCP  (0x0014):          0          1
        NMS   (0x0042):          0         30
        NLS   (0x0044):          0          6
        NRS   (0x0049):          0          1
        NSUP  (0x0081):          0          1
        ASUP  (0x0082):          1          0
```

DTMF events RTP payload set dynamically via IPDC

Lucent media gateway devices now set the payload type for dual-tone multifrequency (DTMF) digits dynamically over the real time protocol (RTP) stream, in accordance with RFC 2833 section 3.3 (Event Types). This payload type does not have a static number, but uses an RTP payload-type number established dynamically for each call using the IP device control (IPDC) protocol.

This feature utilizes an IPDC tag value of `0x3E` followed by DTMF payload indicator values ranging from 96 to 127 (decimal). If a value outside this range is received, the call will be rejected with a cause code of `0x41` (capability not implemented). This tag is only interpreted if the `dtmf-tone-passing` parameter in the `voip` profile is set to `rfc2833`. Otherwise the tag is ignored.



Note Specific IPDC details can be found in IPDC spec 0.18.1

Configuring two-stage dialing in SS7 networks

Two-stage dialing requires iterative DTMF detection and voice announcement transmission by the called TAOS unit prior to the setup of the actual call. This mechanism is supported in a way that is compliant with the IPDC standard. It is also supported with a Lucent-proprietary extension of IPDC identified as SS7 VoIP call persistence.

Selection between these behaviors is supported by a new TAOS parameter, `ss7voip-call-persistence` in the `voip` profile. Standard two-stage dialing behavior is supported when SS7 VoIP call persistence is disabled.

Enabling or disabling SS7 VoIP call persistence

To enable or disable VoIP call persistence, set the `ss7-voip-call-persistence` parameter in the `voip` profile. I

Parameter	Setting
`ss7-voip-call-persistence`	Specify one of the following values: ■ `disabled` (the default): standard IPDC two stage dialing is supported. ■ `enabled`: two-stage dialing, using the Lucent proprietary IPDC extension for call persistence is supported.

Standard behavior

If the `ss7-voip-call-persistence` parameter is disabled, the standard IPDC method for two-stage dialing is supported. The called TAOS unit responds to requests from a softswitch for DTMF detection or the transmission of an announcement by creating internal VoIP call routes for each of these actions. These internal VoIP call routes are deleted when their associated actions are completed. The creation and deletion of VoIP call routes during two-stage dialing impacts multiple hardware components within the unit.

In this release, the standard behavior of the TAOS unit is optimized to reduce internal overhead associated with the creation and deletion of internal VoIP call routes in support of standard two-stage dialing. The TAOS unit now creates a single internal VoIP call route for all DTMF and announcement actions required during two-stage dialing. The VoIP call route that supports these actions is torn down after the announcement or DTMF detection has completed, whichever occurs last.

VoIP call persistence

VoIP call persistence is introduced as an alternate way to handle two-stage dialing and further minimize associated overhead within the TAOS unit. If the `ss7-voip-call-persistence` parameter is enabled, a single internal VoIP call route is created prior to the actual setup of the call. This internal VoIP call route is maintained (persists) for all VoIP-related IPDC requests during the life of the call.

A single internal VoIP call route is created when the first Listen for Tone (LTN) or Send Tones (STN) message is received from the softswitch. This single VoIP call route supports DTMF detection, announcements, and end-to-end setup of the call. This

internal VoIP call route is deleted when a Release Channel Request (RCR) message is received from the softswitch.

When VoIP call persistence is enabled, the TAOS unit must be controlled by a softswitch that is compliant with SS7 VoIP call persistence. The softswitch must send an RCR message to terminate a call, even when an RCCP message to set up the end-to-end connection has not been sent. If an LTN or STN message has been sent to initiate a TDM call, an RCR message must also be sent before the Request Pass-Through Call Setup (RCST) message is sent to setup the TDM connection.

SS7 VoIP call persistence is a Lucent-proprietary extension of IPDC. SS7 VoIP call persistence is disabled by default to maintain compliance with standard implementations of IPDC.

New IPDC feature support

With this release support is provided for the following features under IPDC control:

- Break-in voice announcements
- Voice announcement playlists
- In-call DTMF detection and notification for call re-origination

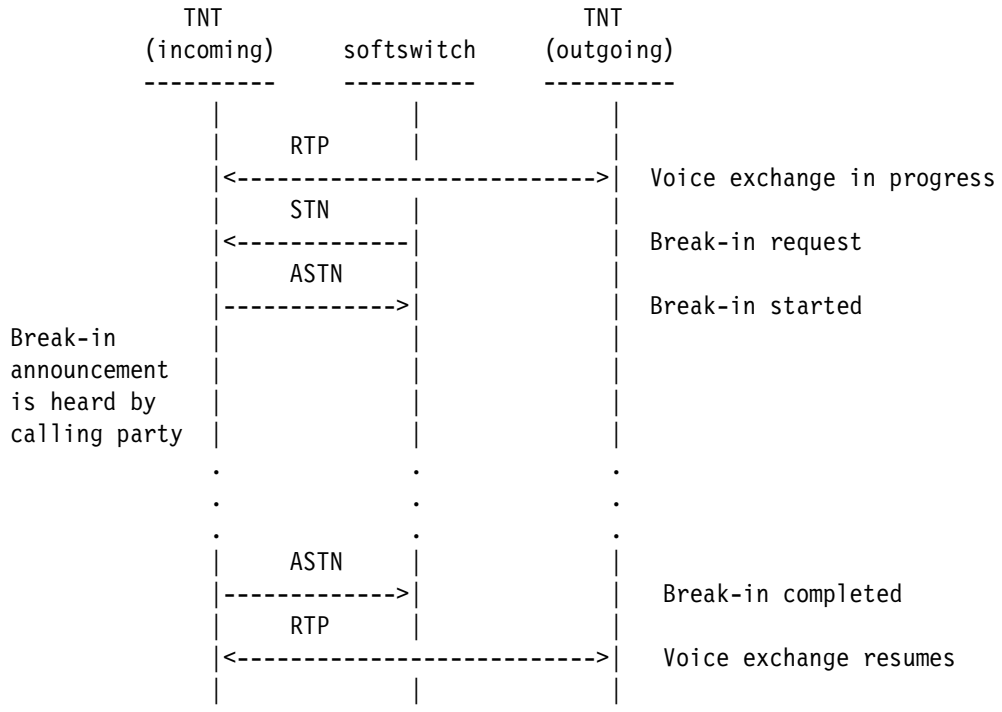
Break-in voice announcements

Support is provided for playing a voice announcement while a packet call is in progress. This support is provided for packet calls only. Support for break-in voice announcements utilizes existing IPDC send tones message (STN) and acknowledge result of send tones message (ASTN) messages without modification. Standard cancellation is fully supported.

Normal break-in announcement call flow

Transmission of RTP packets is suspended when a break-in voice announcement is playing. The party to which the announcement is directed hears the voice announcement, while the other party hears silence. Typically the announcement is directed to the calling party. In some instances the announcement can be directed to the called party.

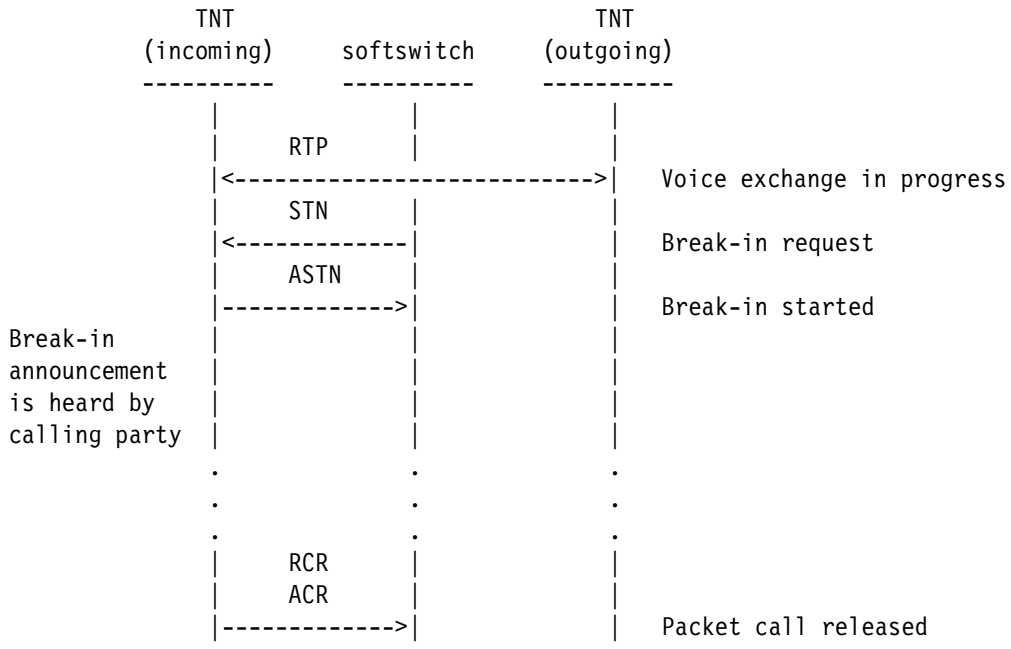
The following call flow example illustrates a break-in announcement that is directed to the calling party.



Break-in announcement call release flow

When a release channel request (RCR) message is received during the playing of a break-in announcement, the call is released and a release channel completed (ACR)

message is sent containing the RTP statistics for the packet call. The following call flow illustrates call release.



Voice announcement playlists

The tone string tag (0x33) of the STN message can now communicate a list of announcement file names to the gateway. Previously the Tone String tag could only contain the name of a single announcement file. It can now contain three types of information:

- A single announcement file name.
- A comma-separated list of announcement file names.
  The list can contain optional spaces after each comma.
- File names in a playlist format .
  The number of times a message is played (play count) and the delay before playing a message may be specified for each message on the list, and for the entire group of messages in the list.

The following examples illustrate each of these content options:

STN tag (0x33) format option	Example
A single file name	h323dns.au
A comma separated list with optional spaces.	h323dns.au, 1.au, 2.au
A playlist	(c,d,(filename,c,d)...(filename,c,d))
Variables: c = playcount (defatut = 1) d = delay (default = 0)	

In-call DTMF detection

The softswitch can now direct the gateway to perform DTMF detection and notification while a packet call is in progress. This capability is provided by modifications to the request confirm call parameters (RCCP), request modify call parameters (RMCP), and notify tone (NTN) messages.

DTMF digits entered during a call by one party while DTMF detection is enabled will be played out to the other party.

The constant DTMF tone detection tag (0x75) is now supported in RCCP, RMCP, and NTN messages. This tag supports the following values:

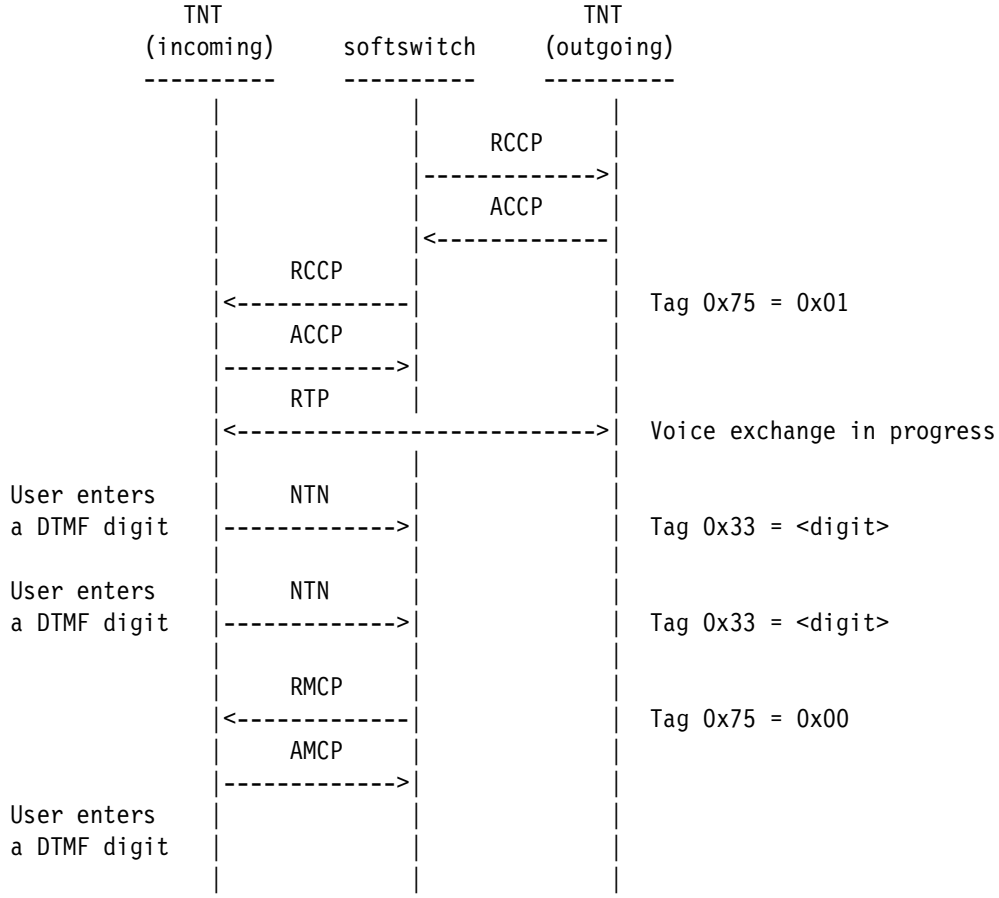
- 0x00 (DTMF tone detection off)
- 0x01 (DTMF tone detection on)

If the constant DTMF tone detection tag is not used in the RCCP message, DTMF tone detection is off by default.

The tone type (0x049) tag in NTN messages now supports the value 0x01 to indicate the DTMF tone type. The tone string (0x033) tag is used to contain the value of the DTMF digit that was detected.

Call flow for DTMF detection during call setup

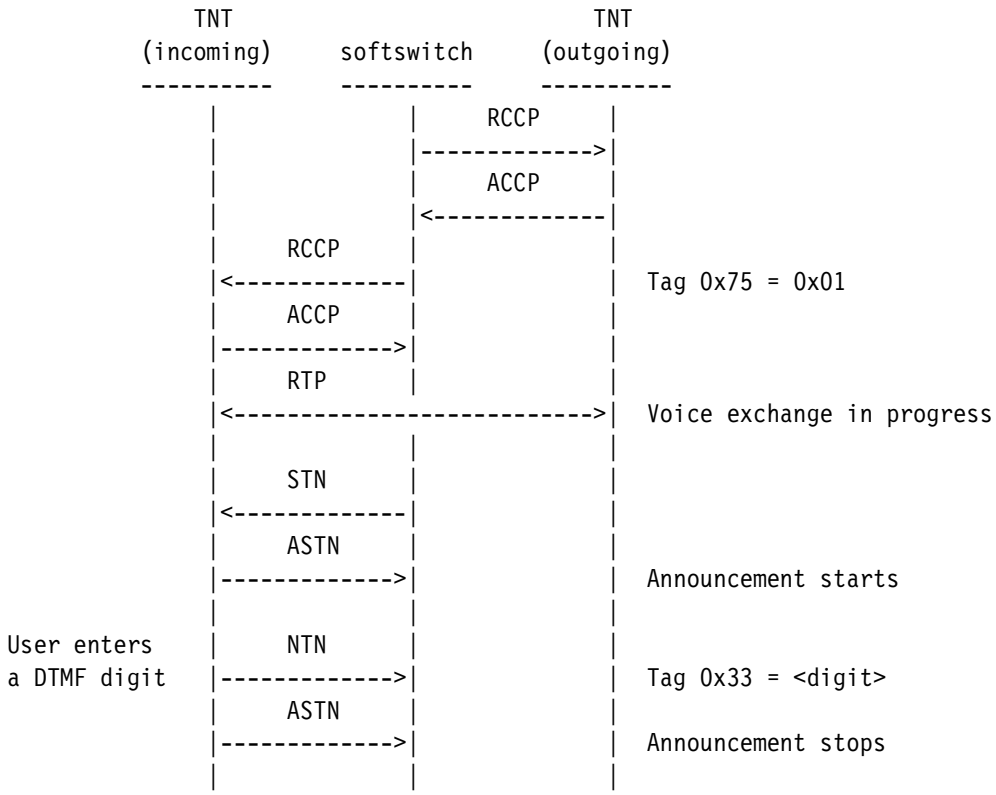
The following call flow illustrates the setup of a packet call with DTMF detection enabled. In this example, DTMF detection is disabled after 2 DTMF digits are entered.





Call flow for DTMF detection during break-in announcement

If in-call DTMF detection is enabled and a break-in announcement is played, the first DTMF entered stops the announcement, as illustrated below:



An RMCP message that is received by the gateway while a break-in announcement is playing will be rejected. A message reject (MRJ) message will be sent with Tag 0xfe (Cause Code) set to 0x65 (Message Not Compatible With Call State).

Note When DTMF is carried inband over IPDC, the first DTMF digit entered by one party during a break-in announcement is not played out to the other party.

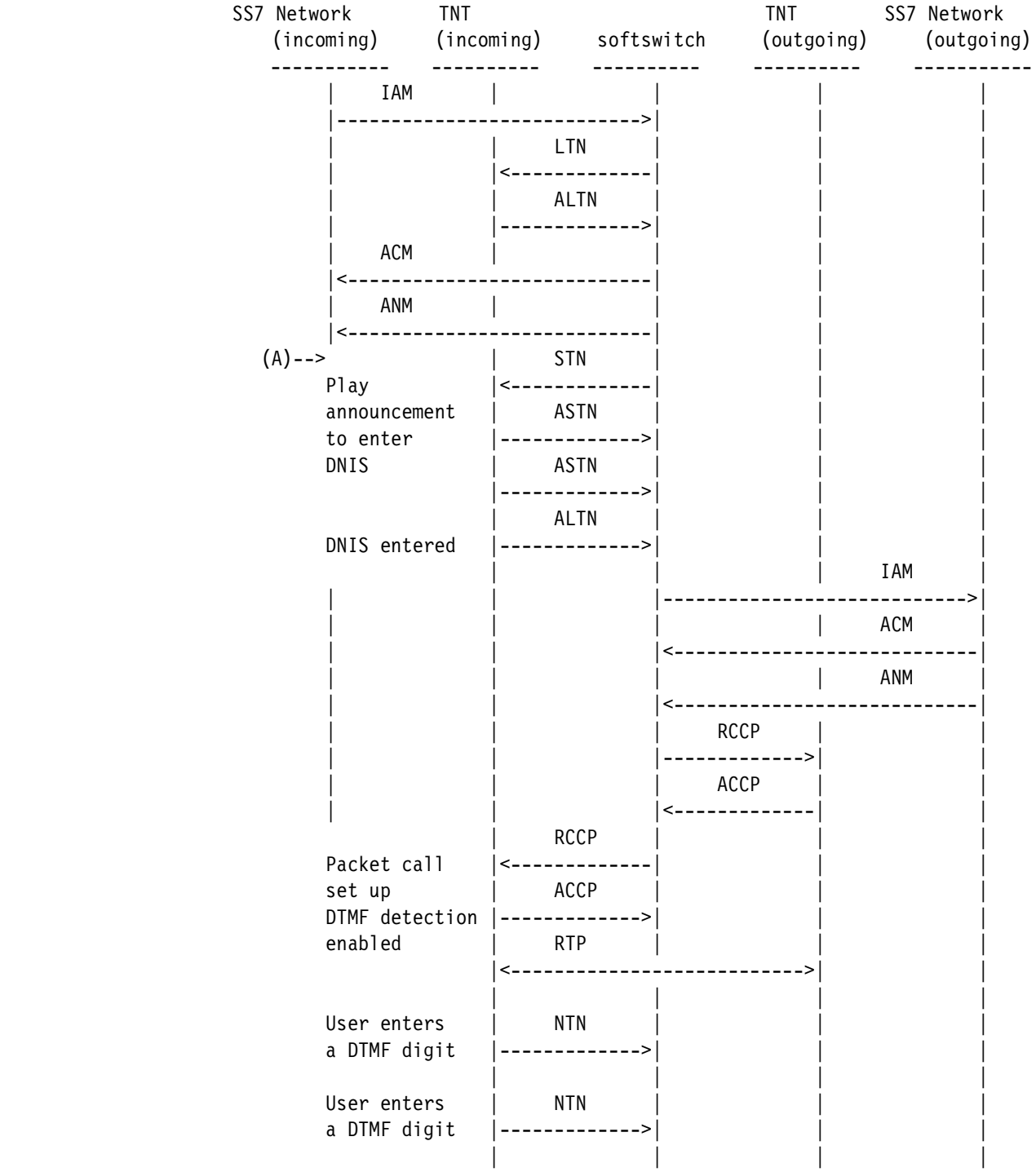
In-call DTMF detection for re-origination

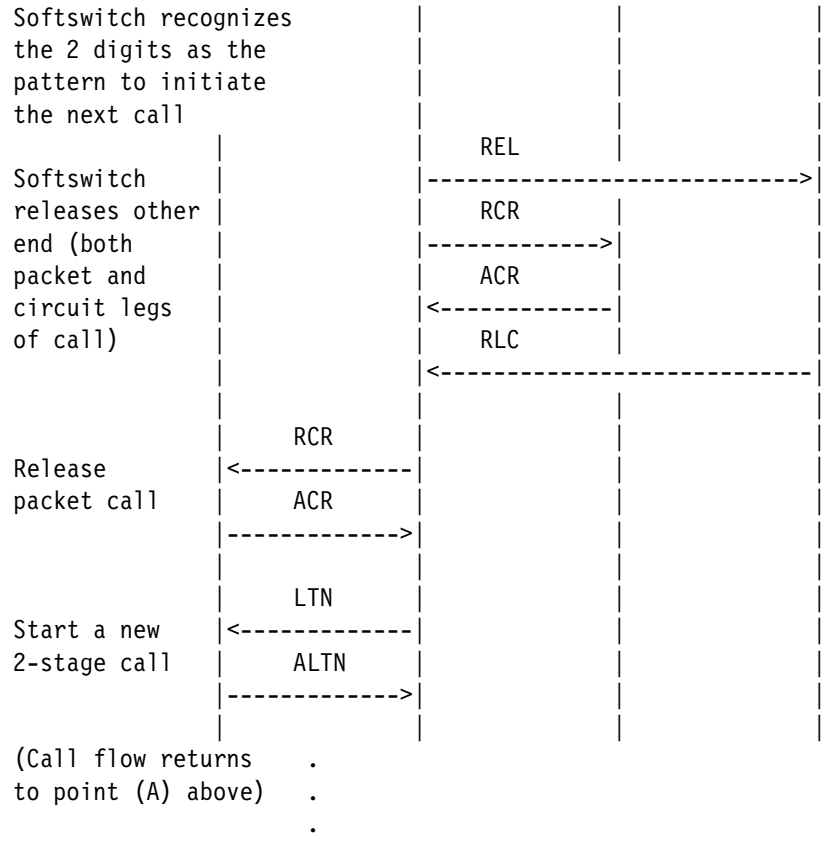
In-call DTMF detection can be combined with existing IPDC support on the gateway to provide call re-origination.

Using in-call DTMF detection, the gateway detects DTMF signals received during an active packet call and sends the digits from these signals in NTN messages to the softswitch. Each NTN message carries a single digit. The softswitch monitors the received digits for a pattern that indicates that the calling party wishes to terminate the active call and start a new one.

When the softswitch detects the specified pattern, it sends an RCR message to terminate the existing call and waits for the ACR message that indicates this has been accomplished. Signaling from the softswitch maintains the incoming TDM circuit with the PSTN and sends a listen for tones (LTN) message to start the two-stage dialing for the next call.

The following call flow shows how in-call DTMF detection is utilized for call re-origination.



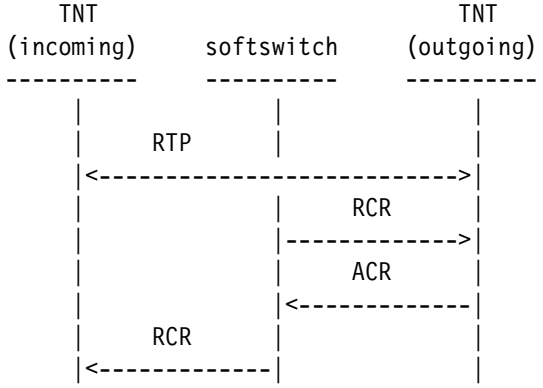


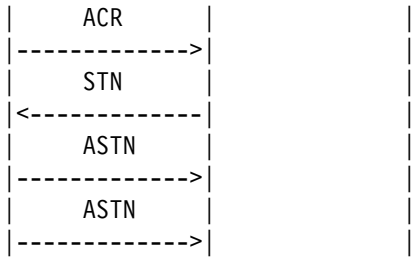
Note When call re-origination is signaled over SS7, VoIP does not use the `sequential-call-enable` and `next-call` parameters in the `voip` profile. These parameters are used when call re-origination is signaled over H.323 VoIP.

End-of-call break-in voice announcements

A break-in announcement can be played with VoIP call persistence enabled or disabled and can take place either before or after a call is released. However, the call flows for break-in announcements after call release vary slightly, depending on whether VoIP call persistence is enabled.

The following example illustrates an end-of-call break-in announcement played after call release, with VoIP call persistence mode disabled. The STN message in this example results in the setup of a new VoIP call route.

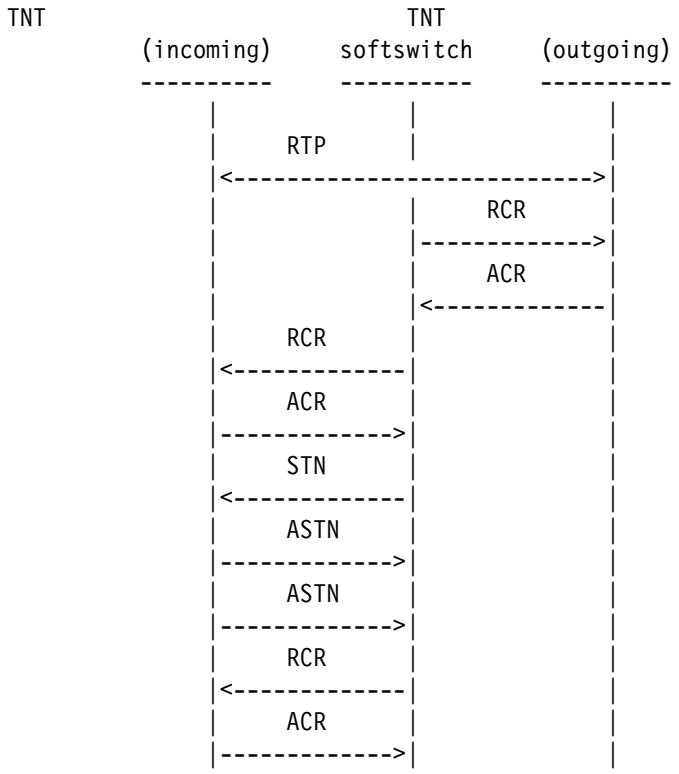




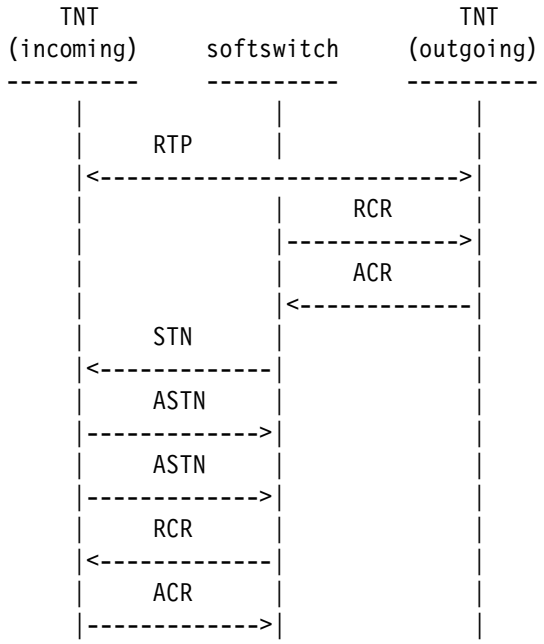
Note The preceding type of messaging is currently possible without support for break-in announcements.

The following example shows an end-of-call break-in played after call release, with VoIP call persistence mode enabled. The STN message in this example will result in the setup of a new VoIP call route. Also, a second RCR message is required to destroy the VoIP call route setup to play the break-in announcement.

Note If call re-origination is in progress, the second RCR is replaced with a LTN/STN/RCCP messages, signaling the start of the next call. The VoIP call route that was set up for the break-in announcement will then be re-used.



The following example illustrates an end-of-call break-in announcement played before call release, with VoIP call persistence mode enabled or disabled. The STN message in this example utilizes the existing VoIP call route for the call.



Note The preceding type of messaging is currently possible without support for break-in announcements.

Change Requests in TAOS 10.1.0 4

Table 4-1 lists the software change requests that have been fulfilled in TAOS 10.1.0.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 1 of 6)

Change request number	Description
7008089	TAOS units sometimes accepted incoming calls on a disabled T1 channel.
7008137	MultiVoice® tag 0x75 was not implemented according to IPDC specifications.
7008174	TAOS units sometimes generated warning 179 messages on MultiDSP and MultiDSP2 cards.
7008211	RADIUS accounting did not process accounting requests for OC3-ATM2 cards that were used for egress.
7008239	For APX units, the `ether-info` profile incorrectly reported the link state of the shelf controller's Ethernet interface as `unknown`. If the `ethernet:link-state-enable` was set to `yes`, the shelf controller Ethernet port did not work.
7008272	The LAC incorrectly sent a Link Control Protocol (LCP) `ConfReq` message to its dial-up peer after the receipt of an Incoming-Call-Connected (ICCN) control message. See "Configurable sending of LCP Configure Request message" on page 3-64 for more information.
7008273	For APX 1000 units, the `slot-info` profile did not display a valid serial number for 24-port T1 and E1 slot cards.
7008290	APX 8000 units generated warning 800 messages after powering up.
7008301	An issue related to RADIUS authentication caused TAOS units sometimes reset with a fatal error message FE 29.
7003876	If the `serial:auto-logout` parameter was set to `yes` and you reset the unit without the serial cable, the serial port did not work.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 2 of 6)

Change request number	Description
7007040 7006967	VoIP/H.323: The MAX TNT unit's handling of Call Identifier during Radvision method Call Transfer was inconsistent.
7007324	The MultiVoice® gateway did not wait for the Primary Registration Confirmation (RCF) packet before sending the secondary Registration Request (RRQ) packet.
6002142	Brazil R2 implementation has been improved in this release.
6002416	MAX TNT packets sometimes caused accounting server timeouts. See "Configurable resending of the Accounting Event packet" on page 3-86 for more information.
7006541	VoIP/H.323: Fast-connect mode calls placed by a vendor's IP telephony device did not include a voice path from the IP telephony device to the MAX TNT unit.
7006679	VoIP/H.323: MAX TNT units reset with warning message W104 and index 385 upon receipt of unexpected options in H.225 messages.
7006709	VoIP/H.323: MAX TNT units reset with warning message W104 and index 385.
7006716	VoIP/H.323: The PRI-mapping feature request did not work after a reset.
7006888	VoIP/H.323: MAX TNT units did not disconnect after receiving a Disengage Request (DRQ) message from a gatekeeper.
7006892	VoIP/H.323: Preferred codec was not supported in TAOS implementation of H.245.
7006893	VoIP/H.323: MAX TNT units had problems decoding nonstandard audio capabilities sent in an H.245 `TermCapabilitySet` message by the IP Voice Response (IPVR) device.
7006929	VoIP/H.323: MAX TNT units did not send dual-tone multifrequency (DTMF) signals to H.323-compliant devices during the fast-connect process.
7007015	SNMP: MAX TNT units reported an invalid value for `ipAdEntNetMask.`
7007049	A TAOS unit operating as a MultiVoice® gateway incorrectly issued a `906 Loss of lower layer connectivity` message.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 3 of 6)

Change request number	Description
7007058	The `disconnect-reason-type.mib` included definitions for cause codes that were not applicable to units that supported Signaling System 7 (SS7).
7007071	The out-of-band DTMF alphanumeric capabilities such Basic String, IA5 String, and General String were not presented in the H.245 request message sent by MAX TNT units.
7007103	High-Level Data Link Control 2 (HDLC2) cards reset frequently with fatal error FE42. The system also logged W179 and W104 warning messages.
7007110	The SNMP agent incorrectly populated RFC2233 MIB objects `ifType` and `ifSpeed` for the Ethernet3-ND card.
7007175	MAX TNT unit were unable to receive calls after the message `SAR rxInt with bad size` occurred.
7007260	Calls failed on TAOS units when a Session Initiation Protocol (SIP) `INVITE` message included a number portability database dip indicator (NPDI).
7007261	The `media-gateway:profile-version` parameter did not include a range that included `0` (zero) as a possible value.
7007269	MAX TNT units with E1 cards installed reset with Index 95 messages.
7007280	The `snmp-configuration-changed` trap incorrectly reported the user's name.
7007288	Egress calls placed by a TAOS unit failed when a destination trunk group tag was specified in another separate tag of the request universal resource indicator (request-URI).
7007292, 7007457	VoIP/H.323: MAX TNT units incorrectly decoded a setup packet sent by a Cisco analog telephone adaptor (ATA). The system released calls when decoding H.323v3 options of a setup message.
7007297	VoIP/H.323: MAX TNT units reset fatal error 29 upon receipt of an H.225 or H.225 setup message.
7007303	A user dialing into a MAX TNT unit using Multilink Protocol Plus™ (MP+) with Bandwidth Allocation Control Protocol (BACP) bypassed second channel authentication when entering a blank password. This situation occurred only when using RADIUS and CHAP.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 4 of 6)

Change request number	Description
7007323	When a TAOS unit started and registered, it sent a Service Change Request on all DS0 physical terminations with their current service state rather than to only those that were not in service.
7007351	V.120 calls with Q.931 message containing a v.120 bearer cap were rejected.
7007391	Terminal server Point-to-Point Protocol (PPP) delay was applied to v.120 and x.75 asynchronous called calls with Dialed Number Information Service (DNIS) pre-authentication.
7007398	Increasing `abnormal disconnect 185/40` were reported for MultiDSP2 cards.
7007417	The secondary controller of APX 8000 units sent a logging dirdo trap to the SNMP manager every 60-70 seconds.
7007451	Stacking between units running TAOS 9.1.2 and TAOS 10.0.1 resulted in invalid multilink headers.
7007514	The MAX TNT unit sent information about its T38 capabilities even when Real-time fax was not configured.
7007535	When an IP `TCP SYN` packet was sent to an unreachable TCP port (such as port 80) on the open vrouter interface or system address, the MAX TNT sent a TCP RST ACK reply packet from the main router interface.
7007536	VISA asynchronous calls were corrupted by normal response mode (NRM) link layer setup messages.
7007543	The system sometimes dropped calls after generating a warning message W179.
7007561	IP Device Control (IPDC) protocol NRS message tag 0x69 was missing when the source RTP port status was set to `active.`
7007570	Accept Packet Pass-Through Call (ACCP) messages did not return optional parameters included in the Request Packet Pass-Through Call (RCCP) message.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 5 of 6)

Change request number	Description
7007572	The MultiDSP firmware upgrade in this release resolves the following issues: ■ Scorpio AMR client modems were unable to train with lower V.34 symbol rates. ■ The unit failed to receive payload greater than 200 bytes at the HDLC-Normal Response Mode (HDLC-NRM) protocol layer. ■ Poor PCM upstream performance.
7007586	Frame relay direct backup did not work.
7007599	MAX TNT units sent accounting requests to an undefined RADIUS server.
7007616	The system did not create a private route if RADIUS was used to authenticate a dial-in user.
7007645	APX 8000 units running TAOS 10.0.1 with an apxenet card installed did not perform proxy ARP for connected users.
7007741	ATMP IPX attributes were not reported to RADIUS Accounting.
7007780	G.729 and G.723 calls failed if the `answer-defaults:clid-auth-mode` parameter was set to `dnis-pref`.
7007801	If a MAX TNT unit with an 8-port T1 card installed received an incoming call with called party subaddress, warning message W179 were logged for the 8-port T1 card.
7007845	Following an upgrade from TAOS 9.*x* to TAOS 10.0 or later, call route costs were set incorrectly.
7007845	See "New cost allocations for priority-based call routing" on page 3-22 for call routing issues that resulted from upgrading.
7007897	When terminal server was set to ASCII (`7-bit` parameter in the `terminal-server:modem-configuration` subprofile was set to `yes`), the system did not suppress bit-8 for outgoing data.
7007925	TAOS units negotiated the LCP option #27 for Multilink Protocol (MP) Multiclass Extension even when that feature was not enabled on the unit.
7007987	The `filterdisp` command did not display applied attribute-value pair (AVP) 242 Ascend-Data-Filter.

Table 4-1. Customer requests fulfilled in TAOS 10.1.0 (page 6 of 6)

Change request number	Description
7007991	IPDC: Message Reject (MRJ) messages were sent when Release Channel Request (RCR) messages with inactive Trans IDs were received.
7008313	If the `vc-fault-management` parameter in a `CONNECTION/"":atm-options` subprofile was set to a value other than the default value of `none`, OAM debugging was activated on an ATM-OC3 version 2 slot card.
7008346	The `userstat -ld` command displayed statistics only for up to 1535 users. This release increases the limit to 3000 users.
7008348	On some units running TAOS 10.0.2, `dnisGlobalCallsActive` in the DNIS management MIB reported unusually high values.
7008374	On MAX TNT units, the system was unable to detect the state of the Ethernet port. If `ethernet:link-state-enabled` was set to `yes`, the shelf was no longer accessible through the Ethernet port because its link state was unknown.
7008395	IPDC Request Modify Packet Pass-Through Call (RMCP) messages with zero-filled values in Tag 0x5f and 0x60 were not returned in Accept Modify Packet Pass-Through Call (AMCP) messages.
7008397	IPCP negotiation failed between a Cisco customer premises equipment (CPE) device and an APX 1000 unit running TAOS 10.0.2.
7008414	On MAX TNT units, the telnet daemon sometimes did not bind to TCP port 23 and Telnet sessions were refused.
7008445	The system sometimes generated warning W179 on the shelf controller.
7007415,7008331	Fatal error FE 29 related to the secondary controller occurred on some APX 8000 units.
N/A	Statistics reported by the `ss7nmi -m` command for each gateway were not being reset.

Notices, Known Issues, and Limitations

5

Notice in TAOS 10.1.0 5-1

Known issues and limitations in TAOS 10.1.0 5-2

If you are upgrading from a release earlier than TAOS 10.0.0, see the TAOS 10.0.0 Release Notes from at `http://www.lucent.com/support` for notices of changes introduced in that release.

Notice in TAOS 10.1.0

The following notices describe important information regarding TAOS software and hardware that is valid for software version TAOS 10.1.0.

Hot standby redundancy provided for APX 8000 systems

APX 8000 systems with dual controllers no longer require a special software license to enable hot standby redundancy. You enable hot standby mode by using the `sync-enabled` parameter in the `redundancy` profile.

Unsupported call type in this release

The `rt24-call-type` `call-route-type`, introduced in TAOS 10.0 for 48-port MultiDSP slot cards, is no longer supported with this software version. If you have 48-port MultiDSP cards in the system and restore a configuration from TAOS 10.0 (or a 10.0 maintenance release) that specifies this call type, the system fails to create a profile with this setting:

```
call-route-type = rt24-call-type
```

And instead saves the profile with this setting:

```
call-route-type = any-call-type
```

This profile causes no harm, but you might want to delete it.

V.92 client modem support

Not all V.92 client modems fully support all V.92 capabilities. Lucent recommends that end users regularly check with their manufacturers for firmware updates. V.92 capabilities are achieved only when the client modems are V.92 compatible, otherwise the modems fall back to V.90 or slower protocols. For V.92 PCM Upstream

connections, actual improvement over performance experienced with V.90 connections will vary on the basis of line conditions.

Unsupported parameters on the command-line interface

The command-line interface includes some parameters related to the session initiation protocol (SIP) and H.248 protocol. TAOS 10.1.0 does not support SIP or H.248.

Notice of parameter name changes in the `external-auth` profile

If you are upgrading from a TAOS 8.*x* release and Dialed Number Information Service (DNIS) and calling line ID (CLID) preauthentication was configured for your system using the `dnis-password` and `clid-password` parameters in the `external-auth` profile, the system will no longer recognize those passwords after upgrading to this release, and dial-in users might experience a busy tone.

In TAOS 9.0 and later releases, the `dnis-password` and `clid-password` parameters were changed to `dnis` and `clid`, respectively, and were moved from the `external-auth` profile to the `external-auth:password-profile` subprofile.

To restore the DNIS and CLID preauthorization passwords, apply the settings of the `dnis-password` and `clid-password` parameters (set in earlier TAOS 8.x releases), to the new `dnis` and `clid` parameters.

Known issues and limitations in TAOS 10.1.0

Be aware of the following known issues and limitations that are known to exist in the TAOS 10.1.0 release.

- Known MultiVoice® issues
  - A small percentage of calls might experience broken one-way voice path when using break-in announcements stored in G.729 format.
  - If your setup includes a 96-port MultiDSP slot card that interacts with a G.711 audio codec device, do not use two frames per packet when you expect to have a fully loaded network with 96 active calls. Set the `frames-per-packet` parameter to `4` or higher in the `voip` profile or accept the default setting of `2` for the `frames-per-packet` set to 2, but disable DSPs on the card with the `mdmdisable` command.

    The DSPs remain disabled even if you reset the chassis. If two frames per packet are maintained and no DSPs are disabled, voice quality might degrade after approximately 80 active calls.
  - If the `use-trunk-groups` parameter is set to `no` in the `system` profile, you must set the call-route `trunk-group` to `0`. The trunk groups defined in the `T1` or `E1` profile are not affected.
  - Under certain network conditions in the simulated test network, transparent fax v.17 calls sometimes downtrain or drop occasionally.
- The performance of the serial WAN 2 (SWAN2) slot declines by about 13 percent if the frame sizes are set to between 1024 and 1518 bytes long.
- Your unit might not route reliably if you configure Border Gateway Protocol (BGP) to accept and inject the full Internet routing table (which currently

consists of approximately 92,000 routes). TAOS units are not designed to be full-fledged Internet core routers, therefore this situation is uncommon. However, to prevent this situation, set BGP to accept a limited number of routes if it would otherwise be receiving too large a routing table. Future software versions might have an explicit limit beyond which it will not accept additional routes.

- If multiple OC3-ATM2 slot cards are configured for OC3 ingress, traffic is unable to pass through the egress slot card.
- If you are using NavisRADIUS, Attribute (21) must be a string instead of an integer in the dictionary file:

  ```
  ATTRIBUTE Ascend-H323-Conference-ID 21 string Lucent
  ```

  The following error message appears in the `navisradius.log` file if Attribute 21 is an integer:

  ```
  Invalid packet type for acct: 33
  ```

Limitations in TAOS 10.1.0

- A universal gateway (a TAOS unit) that is originating a VoIP call and has a MultiDSP 48-port, 240-port, or 288-port card installed supports the G.723 audio codec. MultiDSP 96-port cards do not support the G.723 audio codec.
- Multilink Protocol bonding of analog calls is supported, but some client modems and software might have compatibility problems.
- Configurable receive and transmit data rate limits are not supported on the unchannelized DS3-ATM slot card (TNT-SL-UDS3A). Configurable receive and transmit data rate limits are supported on the unchannelized DS3 frame relay slot card (TNT-SL-UDS3).
- Virtual path shaping is supported only on first-generation slot cards. This feature is not supported on second-generation OC3-ATM and DS3-ATM cards.