



MAX TNT[®] True Access[™] Operating System (TAOS) 9.1.0

Release Note

Copyright © 2001 Lucent Technologies Inc. All rights reserved.

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

Notice

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

Safety, Compliance, and Warranty Information

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

Security Statement

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

Trademarks

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

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

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

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

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

Ordering Information

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

Feedback

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

Customer Service

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

Finding information and software

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

Obtaining technical assistance

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

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Table of Contents

Customer Service	iii
About this release note	1
How to use this release note.....	1
TAOS 9.1.0 features.....	1
Feature requests in TAOS 9.1.0	4
Notices, known issues, and caveats.....	5
Notice of TAOS license and upgrade changes.....	5
Price change for base TAOS software	5
Price change for upgrades and maintenance to TAOS 9.1.0 software	5
Distribution change for TAOS 9.1.0 software	5
TAOS software license agreement change	5
Notice of memory requirement in TAOS 9.1.0	6
Notice of support for new shelf controller	6
Notice of support for Universal Port on the 96-port MultiDSP slot card	6
Notice about MultiDSP cards	6
Notice about upgrading slot cards.....	7
Notice of tunnel server lookup behavior change	7
Notice of new default value for the log-call-progress attribute	8
Notice of discontinued support for AppleTalk and ARA routing.....	8
Notice of nonsupport for WORM-ARQ on the 96-port MultiDSP slot card.....	9
Notice of discontinuance of configurable RADIUS port and ID space	9
Notice of discontinued software support	9
Notice of deprecated management features	9
Notice of discontinuance of support for store and forward fax	10
Notice of change in supported values for the signaling mode	10
Notice of a tunneling configuration requirement.....	10
Notice of Allow-Unencrypted-Tunnel-Password parameter	11
Notice of parameter name changes in the External-Auth profile.....	11
Notice of modified behavior during IPCP negotiation	12
Notice about default settings in the Call-Logging profile.....	12
Notice about a change in the terminal server password length.....	13
Notice of TAOS interoperability with SS7 signaling software.....	13
Notice concerning call signaling support on T1/E1 slot cards.....	13
Notice of change in egress call routing configuration	14
Notice about LAN-modem profiles	15
Known issue using X.21 cables with BSTDX9000 cables on SWAN2 slot cards	15
Known issue handling full BGP Internet routing table	15
Known issue linking more than one PVC to a single traffic shaper	15
Known issue of no TOS marking support on OC3 ATM2 slot cards	16
Known issue of ISDN trunk signaling dependencies.....	17

Known issue of True-Connect-Enable parameter dependencies	17
Known issue of same audio codec required to report call progress	18
Known issue of audio codecs and frames per packet.....	18
Caveats in this release	18
Upgrade and downgrade procedures	21
Requirements and recommendations	21
Memory requirement in TAOS 9.1.0.....	21
32MB JEDEC DRAM card required for this release	21
Obtaining the TAOS 9.1.0 software	21
Local access to the unit recommended	22
Saving the system configuration.....	23
Upgrade instructions	23
Before you begin upgrading	23
Upgrading a standalone MAX TNT unit	24
Upgrading a multishelf MAX TNT unit	24
Downgrade instructions	25
Downgrading a standalone MAX TNT unit	25
Downgrading a multishelf MAX TNT unit	26
WAN access server features in TAOS 9.1.0	29
Support for OC3-ATM2 slot card.....	29
Support for SWAN2 slot card	29
New SWAN2 slot card hardware features	29
SWAN2 slot card status lights	29
SWAN2 cables.....	30
New SWAN2 subtype for the Load command	30
SWAN2 line speeds supported	30
New Line-Rate parameter	31
New log message	31
Examples of setting the clock rate	31
Microsoft point-to-point compression (MPPC) is enabled	32
Command line changes	32
RADIUS changes.....	33
SS7-IPDC: On PSTN trunk disconnection, notify signaling gateway and keep calls	33
Overview.....	33
Command line changes	34
Differentiated services code point (DSCP) support	35
Differentiating class of service	35
Command line changes	36
RADIUS support.....	37
SS7: Command-level generation of DS0 test tones	38
Command usage.....	38
Events that interrupt continuous test tones	39
Related log messages	39
Examples showing usage and log messages	40
T1 channel idle pattern support.....	41
Modem manager features in TAOS 9.1.0	41
Firmware versions for digital modems	41

Firmware versions for MultiDSP cards	41
Support for V.92 and V.44 modem standards.....	42
V.92 enhancements	42
V.44 enhancements	46
Authentication and accounting features in TAOS 9.1.0	47
Support for selection of authentication method for command-line-interface users.....	47
Support for DNIS fallback	48
Maximum accounting checkpoint interval increased.....	48
Command-line interface changes.....	48
Support for selecting PAP authentication before CHAP	49
Command-line interface support	49
RADIUS support.....	49
RADIUS session-based checkpoint accounting.....	50
Command-line interface changes.....	50
RADIUS Ascend-NAS-Port-Format (13) value included in Access-Request packets	50
Call logging support for DS3, DS3/ATM2, and OC3 slot cards	50
New attributes for progress call logging packet.....	51
Support for limiting the number of simultaneous users of a shared profile.....	51
Routing features in TAOS 9.1.0	52
BGP routing support	52
Overview.....	52
Creating BGP policies	61
Examples.....	68
Support for network routes for multiple customer premises equipment (CPEs)	96
Overview of network routing.....	96
Enabling support for network routes	97
How network routes affect the routing table	98
Using pseudogateways with Ascend-Private-Route (104).....	100
Configuring a pseudogateway	100
Sample pseudogateway configuration	101
Tunneling features in TAOS 9.1.0	102
L2TP command that displays domain, tunnel, and call statistics	102
Command line changes.....	103
Verifying Peer Host Name In L2TP Authentication.....	103
Command-line interface changes.....	104
External-interface changes.....	104
253-character limit for L2TP tunnel server specification	104
Command-Line Interface (CLI) changes	104
RADIUS changes.....	104
RFC 2867 RADIUS tunnel accounting support for L2TP	105
Command-line interface changes.....	105
RADIUS changes.....	106
RFC 2867 RADIUS tunnel accounting support for L2F	107
RADIUS changes.....	107
Command-line changes.....	111

Management agent features in TAOS 9.1.0 112

SNMP: Flash MIB supported.....	112
Changes to MIB objects.....	112
Added MIB objects	113
New MIB group	113
New commands.....	114
SNMP: Support for virtual routers (VRouters).....	115
Using context names	115
Interface changes	115
SNMP: View-based access control implementation	116
Overview.....	116
Command-line interface configuration	116
MIB definitions	120
SNMP: Support for displaying and modifying profiles	123
SNMP: Sending coldstart traps over a slot-card interface	125
SNMP: Link-status trap enhancements.....	125
Command-line interface changes.....	125
SNMP changes.....	126
SNMP: DOT3 MIB implemented.....	127
New objects.....	127
Maximum number of SNMP host entries increased	128
SNMP: Enhancements provide SNMPv3 support and remove host list limitation	129
Command-line interface changes.....	129
Configuring host security.....	130
Parameter reference	130
Discontinued parameters.....	131
SNMP: New trap for unauthorized access	132
New Ascend Security Alert trap	132
New syslog messages.....	132
SNMP: New attributes added to RADIUS accounting and call-logging packets	133
Ascend-Dsl-Physical-Channel (10037)	133
Ascend-Dsl-Physical-Line (10021)	133
Ascend-Dsl-Physical-Slot (10020)	133
Ascend-Line-Type (10017).....	133

MultiVoice features in TAOS 9.1.0 134

SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x.....	134
VoIP call-persistence	134
User Interface Changes	134
Sequential dialing (H.323 caller originated disconnect).....	146
New Next Call parameter	146
Enabling next calls.....	146
Three calling card features using IPDC	147
Voice announcement playlists	148
Break-in voice announcements	149
In-Call DTMF detection	150
ITU G.168-2000 echo canceller.....	157
Overview.....	157
DTMF Carriage in header of RTP per IETF RFC 2833	158
Background.....	158
User Interface Changes	159

IPDC support for VoIP DTMF playout	159
IPDC Changes.....	159
Call Flow - Basic Operation	161
Call Flow - Out-of-band DTMF Transport.....	162
Reporting call failures in cause codes.....	164
Background.....	164
Implementation Details.....	164
H.323 (v2) fastStart support.....	165
H.323 (v2) fast connect call flow	165
Reverting to the H.245 connection	166
H.245 call flow	166
Using fastStart with H.245 tunneling	166
Terminating the H.323 V2 Fast Connect Procedure.....	167
New Faststart Enable parameter	167
Enabling fastStart.....	167
External Interface Changes	167
H.323 Annex D T.38 Fax Support	167
Feature definition	167
User Interface.....	168
Additional Navis Support for RTP Payload Information.....	168
Feature definition	168
User Interface Changes	169
External Interface Changes	170
Problems corrected in TAOS 9.1.0	173
Data corrected problems	173
MultiVoice corrected problems	177

About this release note

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

This release note describes all of the new features that have been introduced in TAOS 9.1.0 for MAX TNT™ units.

The section “Upgrade and downgrade procedures” on page 21 describes how to upgrade and downgrade your system software.

Caution: You must use the software procedures in “Upgrade and downgrade procedures” on page 21 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.

How to use this release note

The Table of Contents on page v and the tables in the following section list the TAOS 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 feature.

For information about obtaining the software described in this release note, see “Obtaining the TAOS 9.1.0 software” on page 21.

TAOS 9.1.0 features

Table 1 through Table 7 show the built-in features that have been added to TAOS 9.1.0.

Table 1. MAX TNT TAOS 9.1.0 WAN access server features

Feature	Introduced in
“Support for OC3-ATM2 slot card” on page 29	TAOS 9.1.0
“Support for SWAN2 slot card” on page 29	TAOS 9.1.0
“Microsoft point-to-point compression (MPPC) is enabled” on page 32	TAOS 9.1.0
“SS7-IPDC: On PSTN trunk disconnection, notify signaling gateway and keep calls” on page 33	TAOS 9.1.0
“Differentiated services code point (DSCP) support” on page 35	TAOS 9.1.0
“SS7: Command-level generation of DS0 test tones” on page 38	TAOS 9.1.0
“T1 channel idle pattern support” on page 41	TAOS 9.1.0

Table 2. MAX TNT TAOS 9.1.0 Modem manager features

Feature	Introduced in
“Firmware versions for digital modems” on page 41	TAOS 9.1.0

Table 2. MAX TNT TAOS 9.1.0 Modem manager features (continued)

Feature	Introduced in
“Firmware versions for MultiDSP cards” on page 41	TAOS 9.1.0
“Support for V.92 and V.44 modem standards” on page 42	TAOS 9.1.0

Table 3. MAX TNT TAOS 9.1.0 Authentication and accounting features

Feature	Introduced in
“Support for selection of authentication method for command-line-interface users” on page 47	TAOS 9.1.0
“Support for DNIS fallback” on page 48	TAOS 9.1.0
“Maximum accounting checkpoint interval increased” on page 48	TAOS 9.1.0
“Support for selecting PAP authentication before CHAP” on page 49	TAOS 9.1.0
“RADIUS session-based checkpoint accounting” on page 50	TAOS 9.1.0
“RADIUS Ascend-NAS-Port-Format (13) value included in Access-Request packets” on page 50	TAOS 9.1.0
“Call logging support for DS3, DS3/ATM2, and OC3 slot cards” on page 50	TAOS 9.1.0
“New attributes for progress call logging packet” on page 51	TAOS 9.1.0
“Support for limiting the number of simultaneous users of a shared profile” on page 51	TAOS 9.1.0

Table 4. MAX TNT TAOS 9.1.0 Routing features

Feature	Introduced in
“BGP routing support” on page 52	TAOS 9.1.0
“Support for network routes for multiple customer premises equipment (CPEs)” on page 96	TAOS 9.1.0
“Using pseudogateways with Ascend-Private-Route (104)” on page 100	TAOS 9.1.0

Table 5. MAX TNT TAOS 9.1.0 Tunneling features

Feature	Introduced in
“L2TP command that displays domain, tunnel, and call statistics” on page 102	TAOS 9.1.0
“Verifying Peer Host Name In L2TP Authentication” on page 103	TAOS 9.1.0
“253-character limit for L2TP tunnel server specification” on page 104	TAOS 9.1.0

Table 5. MAX TNT TAOS 9.1.0 Tunneling features

Feature	Introduced in
“RFC 2867 RADIUS tunnel accounting support for L2TP” on page 105	TAOS 9.1.0
“RFC 2867 RADIUS tunnel accounting support for L2F” on page 107	TAOS 9.1.0

Table 6. MAX TNT TAOS 9.1.0 Management agent features

Feature	Introduced in
“SNMP: Flash MIB supported” on page 112	TAOS 9.1.0
“SNMP: Support for virtual routers (VRouters)” on page 115	TAOS 9.1.0
“SNMP: View-based access control implementation” on page 116	TAOS 9.1.0
“SNMP: Support for displaying and modifying profiles” on page 123	TAOS 9.1.0
“SNMP: Sending coldstart traps over a slot-card interface” on page 125	TAOS 9.1.0
“SNMP: Link-status trap enhancements” on page 125	TAOS 9.1.0
“SNMP: DOT3 MIB implemented” on page 127	TAOS 9.1.0
“Maximum number of SNMP host entries increased” on page 128	TAOS 9.1.0
“SNMP: Enhancements provide SNMPv3 support and remove host list limitation” on page 129	TAOS 9.1.0
“SNMP: New trap for unauthorized access” on page 132	TAOS 9.1.0
“SNMP: New attributes added to RADIUS accounting and call-logging packets” on page 133	TAOS 9.1.0

Table 7. MAX TNT TAOS 9.1.0 MultiVoice features

Feature	Introduced in
“SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x” on page 134	TAOS 9.1.0
“Sequential dialing (H.323 caller originated disconnect)” on page 146	TAOS 9.1.0
“Three calling card features using IPDC” on page 147	TAOS 9.1.0
“ITU G.168-2000 echo canceller” on page 157	TAOS 9.1.0
“DTMF Carriage in header of RTP per IETF RFC 2833” on page 158	TAOS 9.1.0
“IPDC support for VoIP DTMF playout” on page 159	TAOS 9.1.0
“Reporting call failures in cause codes” on page 164	TAOS 9.1.0
“H.323 (v2) fastStart support” on page 165	TAOS 9.1.0

Table 7. MAX TNT TAOS 9.1.0 MultiVoice features (continued)

Feature	Introduced in
“H.323 (v2) fast connect call flow” on page 165	TAOS 9.1.0
“H.323 Annex D T.38 Fax Support” on page 167	TAOS 9.1.0
“Additional Navis Support for RTP Payload Information” on page 168	TAOS 9.1.0

Feature requests in TAOS 9.1.0

Table 8 lists the identification numbers for features requested for the MAX TNT:

Table 8. Feature requests in TAOS 9.1.0

Feature ID	Description
510486	“Verifying Peer Host Name In L2TP Authentication” on page 103
510463	“RFC 2867 RADIUS tunnel accounting support for L2TP” on page 105, and “RFC 2867 RADIUS tunnel accounting support for L2F” on page 107
510387	“SS7-IPDC: On PSTN trunk disconnection, notify signaling gateway and keep calls” on page 33
260794	“253-character limit for L2TP tunnel server specification” on page 104
510411	“Support for selecting PAP authentication before CHAP” on page 49
510471	“Support for network routes for multiple customer premises equipment (CPEs)” on page 96
260984	“SS7: Command-level generation of DS0 test tones” on page 38
261197	“RADIUS Ascend-NAS-Port-Format (13) value included in Access- Request packets” on page 50
510523	“SNMP: Enhancements provide SNMPv3 support and remove host list limitation” on page 129

Notices, known issues, and caveats

Notice of TAOS license and upgrade changes

Starting with the release of TAOS 9.1.0, the following changes are now in effect for TAOS base software and TAOS software upgrades, service, and maintenance.

Price change for base TAOS software

With the release of TAOS 9.1.0, the MAX TNT, APX 8000, MAX 3000 and MAX 6000 hardware platforms and TAOS software are priced separately. The TAOS software license is now a mandatory item for any new order. The license grants licensees the right to use the base TAOS 9.1.0 software on the specific platform purchased. *The right to upgrade to a subsequent TAOS minor or major software release that includes new operating system software features is no longer included as part of the base TAOS software license.*

Price change for upgrades and maintenance to TAOS 9.1.0 software

Upgrades to TAOS 9.1.0 software and subsequent releases for the MAX TNT, APX 8000, MAX 3000, and MAX 6000 platforms are available through Lucent Worldwide Services as part of an annual Software Upgrade and Maintenance Service contract. These contracts are priced separately for each platform and include the following software and services:

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

Only customers with an established Software Upgrade and Maintenance Service contract are authorized to upgrade designated TAOS-enabled units to TAOS 9.1.0 and to download the required TAOS 9.1.0 software files.

Distribution change for TAOS 9.1.0 software

TAOS 9.1.0 and subsequent general-availability TAOS software releases are no longer available from <ftp.ascend.com>. Upgrades to TAOS 9.1.0 and all subsequent releases and updates (maintenance releases) will be available instead from the Lucent Worldwide Services software front-end Web site at <http://www.eSight.com>.

TAOS software license agreement change

Lucent Technologies is introducing a new software license agreement that grants you a personal, nontransferable, nonexclusive right to use TAOS 9.1.0 in object code form only, and its accompanying documentation. The agreement prohibits you from loading or using TAOS software on any unit of Lucent equipment other than the unit for which you purchased the software, unless otherwise agreed upon in writing by Lucent.

Notices, known issues, and caveats

Notice of memory requirement in TAOS 9.1.0

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

Notice of memory requirement in TAOS 9.1.0

To upgrade to TAOS 9.1.0, your TAOS unit must be equipped with the 32MB flash card. Please contact your Lucent sales representative to purchase the 32MB flash card.

Notice of support for new shelf controller

TAOS 9.1.0 supports both shelf controller model TNT-SP-SC-SS and shelf controller model TNT-SP-SC in single-shelf configurations.

Note: The single-shelf controller TNT-SP-SC-SS does not power up if an earlier version of TAOS (TAOS 8.0.3 or TAOS 8.0-103.2) is installed on it.

Notice of support for Universal Port on the 96-port MultiDSP slot card

The following is a correction to the *APX 8000 TAOS 9.0 Release Note* and the *MAX TNT TAOS 9.0 Release Note*.

The 96-port MultiDSP slot card currently supports mixing voice and data services on the same card. The following combination of services are supported:

- 96 VoIP and modem sessions, in any combination, with VoIP using either the G.729 or G.711 audio codec
- 96 VoIP sessions using either the G.729 or G.711 audio codec
- 96 modem sessions

A total of 96 ports is supported on this card.

Notice about MultiDSP cards

In TAOS 9.1.0, you can combine 48-port and 96-port MultiDSP cards in a MAX TNT unit for V.90 and ISDN dial-up termination.

Notice about upgrading slot cards

If you replace a Fast (100 MB) Ethernet-1 slot card (TNT-SL-E100) with a newer Ethernet card (TNT-SL-E10-100 or TNT-SL-E100-V-C) that supports MultiVoice, you must write new Ethernet profiles for the new card. The old Ethernet profiles do not carry forward.

If you replace an older Hybrid Access slot card (TNT-SL-HA128 or TNT-SL-HA192) with a newer Hybrid Access card (TNT-SL-HDLC2 or TNT-SL-HDLC2-EC-C), you must write new profiles for the new cards.

If you replace a Series56 modem card (TNT-SL-48MOD-S56, TNT-SL-48MOD-SGL, TNT-SL-48MOD-S-C or TNT-SL-48MODV3-S-C) with a MultiDSP card (TNT-SL-ADI-C, TNTV-SL-ADI-C, or APX8-SL-96DSP), you must write new profiles for the new cards.

When changing the slot card type for any slot, execute the `slot -r` command after downing (`slot -d`) or removing the existing card and before inserting a different slot card type.

Notice of tunnel server lookup behavior change

TAOS 9.1.0 adds the new `tunnel-server-pre-sccrq-lookup` parameter in the L2-TUNNEL-GLOBAL profile which can be set to either `yes` or `no`, and controls whether a TUNNEL-SERVER profile will be looked up before starting an L2TP tunnel.

If the user authentication record does not include a Tunnel-Password attribute and L2TP tunnel authentication is enabled, the TAOS unit can retrieve a matching TUNNEL-SERVER profile to specify or override any of the following attributes:

- Tunnel-Client-Auth ID
- Tunnel-Server-Auth ID
- Tunnel-Password

When the `tunnel-server-pre-sccrq-lookup` parameter is set to `yes`, the TAOS unit will attempt to find a matching TUNNEL-SERVER profile before establishing an L2TP tunnel. The TUNNEL-SERVER profile is located using the string specified in the Tunnel-Server-Endpoint attribute.

When the `tunnel-server-pre-sccrq-lookup` parameter is set to the default value of `no`, the TAOS unit will delay trying to find a TUNNEL-SERVER profile until after receiving the 'Hostname' attribute from the remote L2TP server. The TUNNEL-SERVER profile is located using the string received on the 'Hostname' attribute from the remote L2TP server. This is the same behavior that existed in TAOS 8.0.x.

Note: The tunnel attempt will fail if a matching TUNNEL-SERVER profile cannot be located when L2TP tunnel authentication is enabled and the user authentication record does not include a Tunnel-Password attribute.

Notice of new default value for the log-call-progress attribute

In order to maximize the efficiency of outbound call placement, the default value of the `log-call-progress` attribute has been set to `no`. If you have been using `log-call-progress`, and want to continue to do so, you will need to re-enable this feature after installing this version of TAOS. This release removes the default restriction on parallel-dialing. (See “Notice of memory requirement in TAOS 9.1.0” on page 6). With this restriction removed, the number of calls per second which can be supported increases by 10% to 20%.

Notice of discontinued support for AppleTalk and ARA routing

TAOS 9.1.0 discontinues support for AppleTalk, which includes the AppleTalk Remote Access Protocol (ARAP) and AppleTalk Control Protocol (ATCP) for the MAX TNT unit.

A MAX TNT unit can no longer act as an AppleTalk router, but a Macintosh workstation can continue to access the Internet and IP-based services by means of a MAX TNT unit.

This release discontinues support for the following profiles and subprofiles that are associated with AppleTalk and AppleTalk Remote Access (ARA):

- Atalk-Global profile
- Atalk-Interface profile
- Answer-Defaults > ARA-Answer subprofile
- Connection > ARA-Options subprofile
- Connection > Appletalk-Options subprofile

In addition, in the Connection profile, the Encapsulation-Protocol parameter can no longer be set to `ara`.

Notice of nonsupport for WORM-ARQ on the 96-port MultiDSP slot card

WORM-ARQ is not currently supported on the 96-port MultiDSP slot card. In TAOS 9.1.0, WORM-ARQ for personal digital cellular (PDC) phones is supported *only* on the 48-port MultiDSP slot card. NTT DoCoMo developed the WORM-ARQ technology to maintain transmission quality for PDC wireless phones in Japan. The Lucent Technologies WORM-ARQ license can be enabled only for the 48-port MultiDSP slot card.

Notice of discontinuance of configurable RADIUS port and ID space

In TAOS 8.0.x, the default settings for User Datagram Protocol (UDP) source ports and ID spaces for communication with a RADIUS server specified the use of a unique source port for each card and a distinct ID space for both authentication and accounting requests. However, the MAX TNT unit could be configured to use a single source port and ID space system wide, to accommodate certain RADIUS server daemons that had a system-unique requirement.

Because no known RADIUS servers continue to maintain this requirement, and because the unit's port density makes the use of a single port and ID space undesirable, with TAOS 9.0.0 and TAOS 9.1.0, the MAX TNT always uses port-unique source ports and always sends RADIUS authentication and accounting requests with distinct RADIUS IDs. The following parameters are therefore no longer supported and have been removed from the External-Auth profile:

```
[EXTERNAL-AUTH]
rad-id-space = distinct
rad-id-source-unique = port-unique
```

Note: The `rad-ip-space` and `rad-id-source-unique` parameters no longer appear in the External-Auth profile in TAOS 9.1.0. If you downgrade the unit to an earlier release, the parameters revert to their default values for that release.

Notice of discontinued software support

Software support has been discontinued for the MAX TNT Ethernet-0 slot card (TNT-SL-E10), the Fast (100 MB) Ethernet-1 slot card (TNT-SL-E100), and the older MAX TNT Hybrid Access slot cards (TNT-SL-HA128 and TNT-SL-HA192).

Notice of deprecated management features

Use of the `if-admin` diagnostic command is deprecated. The functionality that was provided by the `-d` (down) and `-u` (up) options of the command is now provided by `read`, `set`, and `write` operations on one of the following profiles:

- The Admin-State-Perm-If profile for permanent interfaces such as a nailed interface
- The Admin-State-Phys-If profile for physical interfaces such as a T1 line

The other options of the `if-admin` command are not supported.

Notices, known issues, and caveats

Notice of discontinuance of support for store and forward fax

Use of the `call-log-radius-compat` parameter in the Call-Logging profile is deprecated in this software version.

The `callActiveIfIndex` and `callStatusIfIndex` objects in the call MIB are not supported in this software version.

The following objects are supported in this software version, but will not be supported in future software versions:

- The `lmodem.mib`
- The `resetStat` group in `ascend.mib`
- The `consoleTable`, `doTable`, and `hostStatusTable` in `ascend.mib`

Notice of discontinuance of support for store and forward fax

The partnership between Lucent, OpenPort, and NetCentric allowed end-users to send fax transmissions over an IP network. This non-real-time method of sending faxes used less bandwidth than real-time faxing, and was more tolerant of busy signals, as faxes could be stored and retransmitted when the destination fax machine became available.

However, due to a lack of demand, a notice is being served on the End of Sale of store and forward fax capability using the ASP protocol.

Notice of change in supported values for the signaling mode

After you upgrade a MAX TNT unit that is configured as a MultiVoice gateway, the MAX TNT unit might generate a bad value error message for the value assigned to the Signaling-Mode parameter in the Line-Config subprofile of T1 profile. Error messages occur when you upgrade the TAOS unit from either of the following limited availability releases to TAOS 9.0.x:

- TAOS 8.0-103.x
- TAOS 8.0-118.x

When these two limited availability releases were compiled, the supported values for the Signaling-Mode parameter were defined as enumerated values, rather than hardcoded values, as is done for TAOS 9.0.x. Applying a saved configuration from either limited availability release to TAOS 9.0.x causes the bad value error.

To correct this error, you must reset the value of the Signaling-Mode parameter after applying the saved configuration and reinitializing the TAOS unit.

Notice of a tunneling configuration requirement

If you are configuring Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP) on a TAOS unit, you must set the `System-IP-Address` parameter of the IP-Global profile to specify a system IP address.

Notice of Allow-Unencrypted-Tunnel-Password parameter

The new `allow-unencrypted-tunnel-password` parameter was added to the Rad-Auth-Client subprofile of the External-Auth profile, which decides whether TAOS units should accept unencrypted tunnel passwords from RADIUS.

Prior to this release, TAOS units only accepted encrypted tunnel passwords. TAOS 9.1.0 adds the `allow-unencrypted-tunnel-password` parameter, which, if enabled, permits the TAOS unit to accept encrypted and unencrypted passwords. The default for the `allow-unencrypted-tunnel-password` parameter is NO.

Note: RFC 2868 states that the Tunnel-Password must be encrypted by RADIUS before being sent out.

Notice of parameter name changes in the External-Auth profile

In TAOS 8.0.x, the `dnis-password` and `clid-password` parameters were added to the External-Auth profile. With these parameters, you could set RADIUS passwords for DNIS and CLID preauthentication.

In TAOS 9.0.x, the `dnis-password` and `clid-password` parameters were moved to the password subprofile of the External-Auth profile. The parameter names were also changed, as shown in the following sample subprofile (shown with default values):

```
[in EXTERNAL-AUTH:password-profile]
clid = Ascend-CLID
dnis = Ascend-DNIS
```

If your unit is configured with DNIS and CLID passwords, after upgrading from TAOS 8.0.x to TAOS 9.0.x, the unit no longer recognizes the `dnis-password` and `clid-password` values that were set in prior releases and dial-in users might experience a busy tone.

To restore the DNIS and CLID preauthorization passwords, you must apply the value of the `dnis-password` and `clid-password` parameters (set in earlier TAOS 8.0.x releases), to the new `dnis` and `clid` parameters as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set password-profile dnis = secretdnis
admin> set password-profile clid = secretclid

admin> write
EXTERNAL-AUTH written
```

Notice of modified behavior during IPCP negotiation

With TAOS 9.1.0, the MAX TNT requires a valid System-IP-Addr setting to complete IPCP negotiation. For example, on an APX 8000 unit the following commands explicitly set the system address to the left shelf-controllers IP address:

```
admin> get ip-interface { { 1 left-controller 1 } 0 } ip-address
ip-address = 10.2.3.4

admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 10.2.3.4

admin> write
IP-GLOBAL written
```

Note: If the System-IP-Addr setting is null, the system terminates PPP connections during the IPCP negotiation phase.

Notice about default settings in the Call-Logging profile

In the Call-Logging profile, the default settings for the Call-Log-Limit-Retry and Call-Log-Timeout parameters are as follows:

```
[in CALL-LOGGING]
call-log-limit-retry = 0
call-log-timeout = 1
```

With call logging enabled and with these parameters left to their default values, if the connection to the call-logging host (such as a RADIUS accounting server or NavisAccess™) fails, the MAX TNT unit continues to send Start and Stop packets to the call-logging host indefinitely.

The setting of 0 (zero) for the Call-Log-Limit Retry parameter indicates an unlimited number of retries. A setting of 1 (one) for Call-Log-Timeout indicates that the MAX TNT unit waits only 1 second before retrying.

To avoid unlimited retries, Lucent recommends that you change the default settings of the Call-Log-Limit-Retry parameter from 0 to 2 or 3 and the Call-Log-Timeout parameter from 1 to between 5 and 10 seconds. For example:

```
admin> read call-logging
CALL-LOGGING read

admin> set call-log-limit-retry = 3

admin> set call-log-timeout = 10

admin> write
CALL-LOGGING written
```

Notice about a change in the terminal server password length

The current version of the *APX 8000/MAX TNT Reference* indicates a maximum value of 64 characters for the Password-For-Direct-Access parameter. However, the maximum allowable password length is 21 characters.

Notice of TAOS interoperability with SS7 signaling software

The MAX TNT unit supports two separate software licenses for integrating the units into Signaling System 7 (SS7) networks:

- Access SS7 Gateway Control Protocol (ASGCP). This method of integration enables the MAX TNT to terminate data calls in an SS7 network. The signaling gateway used must be Lucent Softswitch Internet Call Diversion (ICD) (formerly ASG).
- IP Device Control (IPDC). IPDC is a third-party proprietary protocol. This method of integration enables the MAX TNT to terminate both voice and data calls. The signaling gateway can be ICD for Softswitch or Lucent Softswitch.

TAOS 9.0.x supports interoperability with sections of IP Device Control (IPDC) 0.15.1, including PRI tunneling.

Notice concerning call signaling support on T1/E1 slot cards

When configuring call signaling support on E1 trunks:

- Do not configure R1/R2 multi-frequency (MF) signaling and R2 Dual-Tone Multi-Frequency (DTMF) signaling for different trunks on the same E1 slot card.

When configuring call signaling on E1 trunks, the MAX TNT loads only one tone look-up table per slot card. The tone look-up tables for R1/R2 MF and R2 DTMF signaling are unique to the call signaling type specified by the Signaling-Mode parameter. The MF tone look-up table will not support DTMF signaling, and the DTMF tone look-up table will not support R1/R2 MF signaling.

When configuring call signaling support on T1 trunks:

- Do not configure ISDN or inband, robbed-bit signaling and Feature Group D (FGD) signaling for different trunks on the same T1 slot card. The tone look-up tables for FGD are unique to the call signaling requirements for Access Tandem switching.
- Do not configure inband multi-frequency (MF) signaling and inband Dual-Tone Multi-Frequency (DTMF) signaling for different trunks on the same T1 slot card. The tone look-up tables are unique to the call signaling type specified by the Signaling-Mode parameter. The MF tone look-up table will not support DTMF signaling, and the DTMF tone look-up table will not support MF signaling.

Notice of change in egress call routing configuration

Internal changes made to MultiVoice in TAOS 8.0-118.1 still apply in TAOS 9.1.0, which cause the MAX TNT unit to check both the Call-Route and the T1 > Line-Interface > Channel-Config > Channel-Config#N profile when determining which slot and line is used to route the call. When determining call routes, MultiVoice will use:

- 1 The Trunk Group parameter in the Call-Route profile to identify slot cards where the call can be routed
- 2 The Trunk Group parameter at the T1 > Line-Interface > Channel-Config > Channel-Config#N profile to identify a line/DS0, if any are available, which can egress the call.

In the following example, T1 slot cards are installed in Slot 12 and Slot 13. For the T1 card in Slot 12 of the MAX TNT, all eight T1 trunks are assigned to trunk group 12 using the Trunk-Group parameter in both the Call-Route profile for the T1 slot card and the T1 > Line-Interface > Channel-Config > Channel-Config#N profiles for each DS0 as follows:

```
tnt45>list
[in CALL-ROUTE/{ { { shelf-1 slot-12 0 } 0 } 0 } ]
index* = { { { shelf-1 slot-12 0 } 0 } 0 }
trunk-group = 12
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = trunk-call-type

tnt45>list 1
[in T1/{ shelf-1 slot-12 1 }:line-interface:channel-config[1]]
channel-usage = switched-channel
trunk-group = 12
phone-number = ""
call-route-info = { any-shelf any-slot 0 }
```

When configuring call routing, you must provision the following:

- 1 At the least, a T1/E1 profile must have a trunk group set at the slot or line level which matches the trunk group prefixed to a call's dial string. Setting `trunk-group=0` is equivalent to specifying "any trunk group".
- 2 All channels on the same line must be specified with the same trunk group .
- 3 If a call is accepted onto a slot card, you must have at least one line and channel on that card with a matching Trunk Group in T1 > Line-Interface > Channel-Config

It is recommended to always create a Call-Route profile for each line of a T1 card. Specify the trunk group at the line level and for each channel at the channel level. In the following example, on the T1 slot card installed in Slot 7, the first T1 trunk is assigned to trunk group 7 using the Trunk-Group parameter in the Call-Route profile for that T1 trunk and the T1 > Line-Interface > Channel-Config > Channel-Config[1] profile as follows:

```
admin>list
[in CALL-ROUTE/{ { { shelf-1 slot-7 1 } 0 } 3 } ]
index* = { { { shelf-1 slot-7 1 } 0 } 3 }
trunk-group = 7
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = voip-call-type

admin>list 1
[in T1/{ shelf-1 slot-7 1 }:line-interface:channel-config[1]]
channel-usage = switched-channel
```



```
trunk-group = 7  
phone-number = ""  
call-route-info = { any-shelf any-slot 0 }
```

Though other methods may work in limited situations, these will not be discussed here as they usually do not scale to multiple T1 card configurations that use trunk groups.

Notice about LAN-modem profiles

LAN-Modem profiles contain entries for 96 devices. For the 96-port MultiDSP card, all 96 entries in the profile are used. For 48-port modem cards (Series56 modem card (TNT-SL-48MOD-S56), Series56 II (TNT-SL-48MOD-S-C), and Series56 III (TNT-SL-48MODV3-S-C) cards), only the first 48 entries are used. For the 48-port MultiDSP card (TNTP-SL-ADI-C or TNTV-SL-ADI-C), every other entry in a LAN-Modem profile is used (odd ports only, from 1 to 95).

Known issue using X.21 cables with BSTDX9000 cables on SWAN2 slot cards

X.21 cables have metric M3 threads on the DB-15 pinout. Customers using BSTDX9000 cables must replace the jack screws with the correct M3-threaded standoffs when connecting to any X.21-compliant interface.

Known issue handling full BGP Internet routing table

The TAOS unit might not route reliably if Border Gateway Protocol (BGP) is set to accept and inject the full Internet routing table (which currently consists of approximately 92,000 routes). Since the TAOS unit is not designed to be a full-fledged Internet core router, this is not considered to be a major problem. To prevent this situation, future versions might have an explicit limit beyond which the unit will not accept additional routes. It is currently recommended that you set BGP to accept a limited number of routes if it would otherwise be receiving too large a routing table.

Known issue linking more than one PVC to a single traffic shaper

In TAOS 9.1.0, when two or more Private Virtual Circuits (PVCs) are configured to use the same traffic shaper, one PVC can consume more than its proportional share of the shaper's transmit buffers, preventing other PVCs from transmitting at their maximum allowed bandwidth.

As long as none of the PVCs exceed their respective bandwidth limits, traffic shaping performs as expected. However, if one of the PVCs exceeds its bandwidth limit, it can use all of the traffic shaper's pool resources, potentially preventing all throughput from other PVCs in the pool. In cases where more than one PVC in a pool is requesting more than its allotted benefit, the PVC with the most traffic has the highest probability of obtaining pool resources.

Known issue of no TOS marking support on OC3 ATM2 slot cards

In TAOS 9.1.0, TOS (type of service) marking functionality is not supported on OC3-ATM2 slot cards using a connection profile, even though the fields within this CLI profile appear and can be manually modified.

The exact location of the `tos-options` subprofile within the connection profile is:

```
CONNECTION > ip-options > tos-options
```

The following is an example of the `tos-options` subprofile, named `test1`.

```
[in CONNECTION/test1:ip-options:tos-options (changed)]
active = no
precedence = 000
type-of-service = normal
apply-to = incoming
marking-type = precedence-tos
dscp = 00
```

In this example of the `tos-options` subprofile, the `active` field is set to `no`. This indicates that TOS marking will not be activated on the IP packets. If the `active` field were set to `yes`, the expected behavior would be that each IP packet would have its TOS byte in the IP header set to a value defined by the `tos-options` subprofile. However, this is not supported in TAOS 9.1. Setting the `active` field to `yes` will not affect the TOS byte in any transmitted packets.

Note: This issue does not affect connection profiles configured for ingress host cards. More specifically, if a user's connection profile has TOS enabled, and the card connects to an ingress host card (e.g. 48-port MultiDSP slot card), packets sent from that profile will have the TOS byte marked in the IP header (on the ingress-host card), and this marking will remain even if the packets egress through an OC3-ATM2 slot card.

Known issue of ISDN trunk signaling dependencies

Using ISDN trunk signaling for the Signaling-Mode parameter in the T1/E1 > Line profile has the following configuration dependencies:

Configuration	VoIP call performance
<pre>t1 { n n n } line-interface signal-mode=isdn voip { n n } cause-code-transparency=yes cut-thru-enable-nearend=no sequential-call-enable=yes</pre>	When configured on an ingress MultiVoice gateway, can cause callers to hear four rings and then a prompt to dial the next number when SIT tones (invalid number format) are received from the far-end switched telephone network.
<pre>t1 { n n n } line-interface signal-mode=isdn voip { n n } cause-code-transparency=yes cut-thru-enable-nearend=no/yes</pre>	When configured on an ingress MultiVoice gateway, can cause callers to hear a fast busy signal, rather than call hearing a call failure message, when MultiVoice attempts to connect a call to an invalid DNIS.

Known issue of True-Connect-Enable parameter dependencies

Using the True-Connect-Enable parameter in the VoIP profile has the following configuration dependencies:

Configuration	VoIP call performance
<pre>voip { n n } true-connect-enable=yes single-dial-enable=yes</pre>	Causes the ingress MultiVoice gateway to wait until receiving the connect message from the egress public switched telephone network (PSTN) before reporting that the call is connected. Single-stage dialing must be enabled for call reporting to proceed correctly.
<pre>voip { n n } true-connect-enable=yes single-dial-enable=no</pre>	<p>Can cause the ingress MultiVoice gateway to block forward and/or reverse audio prior to receiving the connect message from the egress public switched telephone network (PSTN). When this condition occurs:</p> <ul style="list-style-type: none">• Announcements may not be heard by the calling party• DTMF digits entered for PIN and DNIS may not be collected by the MultiVoice gateway <p>Note: It is recommended that the True-Connect-Enable parameter be set to no when two-stage dialing is enabled.</p>

Known issue of same audio codec required to report call progress

When using voice announcements to report call progress on a MultiVoice gateway, the Packet-Audio-Mode and Voice-Ann-Enc parameters in the VoIP profile must use the same audio codec, as illustrated by the following:

Configuration	VoIP voice announcement performance
<code>voip { n n } packet-audio-mode=g711- ulaw voice-ann-enc=711-ulaw</code>	Causes the MultiVoice gateway to play voice announcements without affecting the quality of announcement play back.
<code>voip { n n } packet-audio-mode=g729 voice-ann-enc=g729</code>	Causes the MultiVoice gateway to play voice announcements without affecting the quality of announcement play back.

When the Packet-Audio-Mode or Voice-Ann-Enc parameters do not use the same audio codec, the caller might hear a buzzing and clicking before and after announcement play out.

Known issue of audio codecs and frames per packet

When using the G.711 audio codec, do not configure the Frames Per Packet parameter to a number greater than nine. The G.729 audio codec does support using 10 frames per packet.

Caveats in this release

You should be aware of the following issues in TAOS 9.1.0.

- As new features are added to each TAOS release, the amount of memory used by the operating system increases. TAOS units will report less available memory with each subsequent release.
- When you attempt to initiate terminal services such as TCP-clear, Rlogin, or Telnet using a scripted login, the TAOS unit might occasionally terminate calls abnormally, displaying a cause code 51 and progress code 40 in `Syslog` or RADIUS accounting records. This issue is aggravated by scripted logins when the responses are entered before the MAX TNT unit prompts input.
- Before changing an ATM connection's (VPI-VCI) assignment, you must disable the connection on a MAX TNT unit's OC3 (copper) ATM slot card (TNT-SL-OC3-C) or a MAX TNT unit's OC3 (fiber) ATM slot card (TNT-SL-OC3-F).
- Multilink Protocol (MP) 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 MAX TNT unchannelized DS3-ATM slot card (TNT-SL-UDS3A). Configurable receive and transmit data rate limits *are* supported on the unchannelized DS3 Frame slot card (TNT-SL-UDS3).

- LAN-Modem profiles contain entries for 96 interfaces. For the 96-port MultiDSP card, all 96 entries in the profile are used. For 48-port Digital Modem cards—Series56 (TNT-SL-48MOD-S56), Series56 II (TNT-SL-48MOD-S-C), and Series56 III (TNT-SL-48MODV3-S-C)—only the first 48 entries are used. For the 48-port MultiDSP slot card (TNTP-SL-ADI-C or TNTV-SL-ADI-C), every other entry in a LAN-Modem profile is used (odd ports only, from 1 to 95).
- When swapping boards of a different type in a MAX TNT unit, you must use the `slot -r` command before installing the new card. The `slot -r` command will remove the old board's profile.
- The Read-Access-Hosts and Write-Access-Hosts parameters in the SNMP profile are no longer available. These parameters appear to be active if you are logged in as the admin user and have debug enabled, but they must not be used. To assign read-only and/or read-write access to SNMP hosts, you must instead set parameters in the new SNMP-Manager profile. See “SNMP: Enhancements provide SNMPv3 support and remove host list limitation” on page 129.

Upgrade and downgrade procedures

This section shows how to upgrade and downgrade the TAOS software for a MAX TNT unit.

Requirements and recommendations

These recommendations for upgrading MAX TNT units help ensure a smooth upgrade. If you must downgrade from this release to a previous one, please see “Downgrade instructions” on page 25.

Memory requirement in TAOS 9.1.0

To upgrade to MAX TNT TAOS 9.1.0, your MAX TNT unit must be equipped with the 32MB flash card. Please contact your Lucent sales representative to purchase the 32MB flash card.

32MB JEDEC DRAM card required for this release

For this release, the MAX TNT requires a 32MB JEDEC DRAM card (model number TNT-SP-DRAM-32). New MAX TNT units now ship standard with the 32MB DRAM card.

The 32MB JEDEC DRAM card is not hot swappable. To install the card, you must turn off power to the MAX TNT, insert the card, and then power on the MAX TNT. For additional information about the card, contact your sales representative.

Obtaining the TAOS 9.1.0 software

The MAX TNT TAOS 9.1.0 software consists of the following files:

Filename	Descriptions
<code>tntsrb.bin</code>	The boot loader. Both T1 and E1 loads use the same boot loader software. Install the appropriate boot loader for your software release when upgrading or downgrading.
<code>tntr1.tar</code> and <code>tntr12.tar</code>	Tar files (T1 load) that contain images for the shelf controller and all T1-compatible slot cards.
<code>tntr1e.tar</code> and <code>tntr1e2.tar</code>	Tar files (E1 load) that contain images for the shelf controller and all E1-compatible slot cards.

If you need further assistance on obtaining the TAOS 9.1.0 software, see “Customer Service” on page iii.

To identify the software that you need based on the slot cards that have been physically installed in your chassis, refer to the following table. This table lists the contents of the tar files that contain the most commonly used slot-card images.

Minimally, you must load the first tar file (`tntr1.tar` or `tntr1e.tar`). If your MAX TNT chassis contains additional slot cards (for example, a SWAN slot card), then you must also load the second tar file (`tntr12.tar` or `tntr1e2.tar`).

The contents of the MAX TNT TAOS 9.1.0 tar files are listed in the following table:

Filename	Contents	
	Description	Slot-card images
tntrel.tar	Shelf controller	tntsr
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	T1-specific images	tnt8t1 tntt3 tntut1 tntpctfit
	MAX TNT modem images	tntcsmx tntcsm3v tntmdm56k
	MultiDSP	tntmadd
tntrel2.tar	STM-0	tntstm0
	UDS3	tntuds3
	DS3-ATM, DS3-ATM-2	tntds3atm tntds3atm2
	OC3-ATM	tntoc3atm tnt0c3atm2
	SWAN	tntswan tntswan2
	Analog modem	tntamdm
tntrele.tar	Shelf controller	tntsre
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	E1-specific images	tnt8e1 tntue1 tntpctfie
	MAX TNT modem images	tntcsmx tntcsm3v tntmdm56k
	MultiDSP	tntmadd
tntrele2.tar	E3-ATM	tnte3atm
	OC3-ATM	tntoc3atm tnt0c3atm2
	SWAN	tntswan tntswan2
	Analog modem	tntamdm

Local access to the unit recommended

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.

If your unit is configured with DNIS and CLID passwords, after upgrading from TAOS 8.x to TAOS 9.x, the unit will no longer recognize the `dnis-password` and `clid-password` values that were set in prior releases, and dial-in users may experience a busy tone.

Saving the system configuration

As a general practice, always 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 are 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 MAX TNT 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
```

Note: For additional information about the `save` command and its options, see the *APX 8000/MAX TNT Reference*.

Upgrade instructions

These instructions show how to upgrade to TAOS 9.1.0 from TAOS version 8.0.x or later. If you are not sure which version the system is running, enter the `version` command. For example:

```
admin> version
Software version 8.0.4
```

Note: Under certain conditions, the `load tar` command might not recognize the slot cards and load only the shelf controller image during the upgrade procedure. If this occurs, reset the system and load the tar file again. The second `load tar` command will load the appropriate slot-card images for the system.

Before you begin upgrading

Before upgrading a standalone or multishelf unit, follow these preliminary steps:

- 1 Log into the system and save its configuration to a TFTP server. This step is optional but strongly recommended. For details, see “Saving the system configuration” on page 9.
- 2 Verify that the Load-Select profile is configured either to automatically load only required binaries or to load only selected binaries.

Upgrading a standalone MAX TNT unit

Note: The following steps are order sensitive. To help ensure a smooth upgrade, first perform the preliminary upgrade steps described in the preceding section, and then perform the following steps in the order in which they are shown.

To upgrade a standalone 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 tntsrbin
```

Note: If you upgrade from TAOS 9.0.x or higher, continue with step 4. Otherwise, continue with step 3.

- 3 Load the tar file. For example:

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

Note: Skip step 4.

- 4 Load the tar file. For example:

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

- 5 Restore the system configuration file (optional). For example:

```
admin> load config network 10.10.10.10 /tftpboot/config/testcfg
```

- 6 Reset the system as follows:

```
admin> reset
```

Note: In this release, the `dnis-password` parameter in the `password-profile` subprofile of the `EXTERNAL-AUTH` profile has been changed to `DNIS`.

Upgrading a multishelf MAX TNT unit

Note: For multishelf systems, the master shelf and each slave shelf must have a 32MB JEDEC DRAM card (model number TNT-SP-DRAM-32).

Note: MultiVoice is not supported on multishelf systems.

If you are upgrading a multishelf system, you must load the new boot loader to the slave shelves by using the `Loadslave` command. (The version of the `tntsrbin` file on the master shelf must match the `tntsrbin` version on the slave shelves. Otherwise, the slave shelves cannot load code from the master shelf.) In addition, you must load a link to a redundant image of the tar file located in onboard flash.

The following steps are order sensitive. To help ensure a smooth upgrade, first perform the preliminary steps described in “Before you begin upgrading” on page 23, and then perform the following steps in the order in which they are shown:

- 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 tntsrbin
```

- 3 Load the new boot loader to the slave shelves. For example, the following command loads the boot loader to a slave shelf with a rotary-switch setting of 2:

```
admin> loadslave 2 boot-sr
```

Note: If you are upgrading from TAOS 9.0.x or higher, skip step 4 and continue to step 5.

- 4 Load the tar file. For example:

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

Note: Skip step 5 and continue with step 6.

- 5 Load the tar file. For example:

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

- 6 Use the Loadslave command to load a link to the image2 file, which is a redundant compressed image of the of the binary in the NVRAM. For example, the following command loads the image to a slave shelf with a rotary-switch setting of 2:

```
admin> loadslave 2 image2
```

- 7 Restore the system configuration file (optional). For example:

```
admin> load config network 10.10.10.10 /tftpboot/config/testcfg
```

- 8 Reset the system, as follows:

```
admin> reset -a
```

Downgrade instructions

Because releases are not necessarily backward compatible, Lucent recommends that you always restore a backup configuration made under the previous version or one of its predecessors.

Note: If you must downgrade, you must have serial access to the MAX TNT. See the previous *MAX TNT TAOS 9.0 Release Notes* at <http://www.lucent.com/ins/doclibrary>.

Downgrading a standalone MAX TNT unit

To restore a previous software version (prior to TAOS 9.0.x), 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 tntsrbin
```

Note: If downgrading to a previous software version prior to 9.0.x, continue with step 3. Otherwise, continue with step 4.

- 3 Load the previous version of the tar file. For example, to load via TFTP from a local host:

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

Note: Skip step 4 and continue with step 5.

- 4 Load the previous version of the tar file files.

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

- 5 Clear all profiles by entering the nvram command. For example:

Upgrade and downgrade procedures

Downgrade instructions

- ```
admin> nvram
```
- 6 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
```
  - 7 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
```
  - 8 Reset the system. This step is required. For example:  

```
admin> reset
```

## Downgrading a multishelf MAX TNT unit

If you are downgrading a multishelf system, you must load the restored boot loader to the slave shelves by using the Loadslave command. (The version of the `tntsr.b.bin` file on the master shelf must match the `tntsr.b.bin` version on the slave shelves. Otherwise, the slave shelves cannot load code from the master shelf.) In addition, you must load a link to a redundant image of the restored tar file. To downgrade a multishelf unit, proceed as follows:

- 1 Format the flash card. For example:  

```
admin> format flash-card-1
```
- 2 Load the boot loader. For example:  

```
admin> load boot-sr network 10.10.10.10 tntsr.b.bin
```
- 3 Load the new boot loader to the slave shelves. For example, the following command loads the boot loader to a slave shelf with a rotary-switch setting of 2:  

```
admin> loadslave 2 boot-sr
```

**Note:** If you are downgrading to a TAOS version prior to 9.0.x, continue with step 4. Otherwise, continue with step 5.
- 4 Load the tar file. For example:  

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

**Note:** Skip step 5 and continue with step 6.
- 5 Load the tar files. For example:  

```
admin> load tar network 10.10.10.10 tntrel.tar tntrel2.tar
```
- 6 Use the Loadslave command to load a link to the `image2` file, which is a compressed image of the binary in the NVRAM. For example, the following command loads the image to a slave shelf with a rotary-switch setting of 2:  

```
admin> loadslave 2 image2
```
- 7 Clear all profiles by entering the `nvram` command. For example:  

```
admin> nvram
```
- 8 Log into the system (master shelf) 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 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
```

- 9** 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 /tftpboot/config/801-config
```

**Note:** Steps 10 and 11 are required and are order sensitive.

- 10** To enable the shelf controller as master shelf, reset the system as follows:

```
admin> reset
```

- 11** To enable the system as a multishelf system, reset the system as follows:

```
admin> reset -a
```



## WAN access server features in TAOS 9.1.0

### ***Support for OC3-ATM2 slot card***

A new OC3-ATM2 slot card is available for the MAX TNT unit. This slot card is similar to the OC3-ATM card and it supports some traffic shaping. The user interface is identical to that of the OC3-ATM slot card.

The OC3-ATM2 slot card supports:

- Quality of Service (QoS), through traffic shapers with configurable parameters for constant bit rate (CBR), variable bit rate (VBR), and unspecified bit rate (UBR)
- Permanent Virtual Circuits (PVCs)
- STS-3c/STM-1
- ATM OAM F5 for operation, administration, and maintenance

You can view or download the OC3-ATM2 slot card guide at  
<http://www.lucent.com/ins/doclibrary/library.html>.

### ***Support for SWAN2 slot card***

The Serial WAN 2 (SWAN2) slot card has four serial ports that can be used for nailed frame relay connections and Point-to-Point Protocol (PPP) connections. These four ports can be configured for either V.35 (V.36-compatible) or X.21 transmission. The SWAN2 slot card can support up to 120 Frame Relay permanent virtual circuits (PVCs).

The SWAN2 card comes equipped with two status lights. One X.21 cable or two V.35 cables are available for SWAN2 connections.

To support the SWAN2 slot card, the TAOS command-line interface now includes a change to the TAOS Load command and a parameter that enables you to more easily set the SWAN2 line speed if you use internal clocking. The new parameter is supported by a new log message.

### ***New SWAN2 slot card hardware features***

The SWAN2 slot card has hardware features similar to the SWAN slot card, except that its status lights operate differently and it uses both V.35 and X.21 cables. For information about the SWAN slot card hardware features, see the *MAX TNT Hardware Installation Guide*.

### **SWAN2 slot card status lights**

The SWAN2 slot card has two status lights:

- The left status light is amber when the slot card is starting up or in the event of a slot card failure, and off when the slot card is operating normally.
- The right status light is amber when the serial daughterboard is starting up or resetting, green when at least one of the four serial ports is operating, and off otherwise.

## SWAN2 cables

The following cables are available for the SWAN2 slot card:

- One V.35 cable to provide four V.35 data terminal equipment (DTE) interfaces
- One V.35 cable to provide four V.35 data circuit-terminating equipment (DCE) interfaces
- One X.21 cable to provide four X.21 interfaces

Cables have an encoded signature that allows the SWAN2 slot card to automatically determine whether the cable attached to its 120-pin port is data terminal equipment (DTE) or data circuit terminating equipment (DCE). The slot card then configures itself accordingly.

## New SWAN2 subtype for the Load command

The TAOS `load` command uploads a code image to flash or runs a remote configuration script. (For a complete command description, see the *APX 8000/MAX TNT Reference*.) The `load` command has the following syntax:

```
load [-v] load-type [-subtype] source [device]
```

The `load-type` syntax element can now be assigned a value of `swan2`, which you can use to load only the code image for the SWAN2 slot card. For example, the following command loads the SWAN2 slot card code image `tntswan2.fff` from a TFTP network host to a MAX TNT unit:

```
admin> load swan2 net tftp tntswan2.fff
```

You can also use the standard method of loading all slot card images, including the SWAN2 image. In the following example, the command loads tar files `tntrel1.tar` and `tntrel2.tar`, which contain the all the slot card images, from network host `i.p.a.d` to a MAX TNT unit:

```
admin> load tar net i.p.a.d. tntrel1.tar tntrel2.tar
```

## SWAN2 line speeds supported

You can now set the line rate generically on a SWAN2 slot card that uses internal clocking and is being used as a DCE device. The clock speed at the serial WAN port has no effect on the bandwidth of other WAN interfaces on the MAX TNT unit.

The electrical interfaces on the SWAN2 slot card support the following maximum lines speeds:

| Electrical interface | Maximum speed per port                                                      |
|----------------------|-----------------------------------------------------------------------------|
| V.35                 | 2.048Mbps in the United States<br>2.048Mbps in Europe in 64Kbps increments. |
| X.21                 | 2.048Mbps                                                                   |

When *externally* clocked, the SWAN2 slot card supports full-duplex, synchronous transmission at a maximum speed of 2.048Mbps at each of the four ports simultaneously, with the appropriate electrical interfaces.



When *internally* clocked, the SWAN2 slot card provides the clock, which can take discrete values from 50Hz to 2,048,000Hz.

## New Line-Rate parameter

The SWAN TAOS profile includes a new parameter, `line-rate`, in the Clocking subprofile of the Line-Config profile. You can use `line-rate` instead of the `divider` and `exp` parameters to set the internal clock speed for a SWAN2 slot card. You can set the new parameter to any of a large number of discrete values ranging from 50 bps to 2,048 Mbps.

**Note:** Although TAOS accepts any line rate up to 10 Mbps, the SWAN2 slot card is capable of generating only a limited number of discrete rates. If you enter a line rate that is not supported by the slot card, it defaults to the nearest supported rate.

## New log message

If you set the `line-rate` parameter to a nonsupported rate, the TAOS unit logs a message stating that the requested rate is different from the actual rate generated by the card. The message has the severity of a warning. Following is an example of a log message:

```
SWAN: requested line rate 900000 differs from actual line rate of
921600
```

## Examples of setting the clock rate

Following are clocking parameters with sample values:

For external clocking:

```
[in SWAN/{ shelf-1 slot-13 2 }:line-config:clocking]
clock-mode = external-clock
divider = 1
exp = 2
line-rate = 2048000
```

For internal clocking:

```
set clock=int
set line-rate=2049000
```

In the internal-clocking example, the value of 2049000 defaults to 2048000, which is the nearest supported value.

You can view or download the SWAN2 slot card guide at  
<http://www.lucent.com/ins/doclibrary/library.html>.

## **Microsoft point-to-point compression (MPPC) is enabled**

In this release of TAOS, MPPC is enabled. The `link-compression` parameter can now be set to the value of `mppc` in addition to `none`, `stac`, `stac-9`, and `ms-stac`. The `link-compression` parameter appears in the `ppp-answer` and `ppp-options` subprofiles of `ANSWER-DEFAULTS` and the `CONNECTION` profiles respectively.

Link-compression is set to `mppc` if both sides of the connection have agreed to use the specified compression method. See Chapter 1 of the *APX8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide* for details about negotiation.

### **Command line changes**

MPPC can be set as the link-compression option in the `ANSWER-DEFAULTS` and the `CONNECTION` profiles as shown below.

```
[in ANSWER-DEFAULTS:ppp-answer (new) (changed)]
enabled = yes
receive-auth-mode = no-ppp-auth
bi-directional-auth = none
substitute-send-name = ""
disconnect-on-auth-timeout = yes
bridging-group = 0
link-compression = mppc
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
cbcp-enabled = no
ipx-header-compression = no
mtu = 1524
auth-for-async-framed-users = required
max-pap-auth-retry = 0
```

```
[in CONNECTION/"":ppp-options (new) (changed)]
send-auth-mode = no-ppp-auth
bi-directional-auth = none
send-password = ""
substitute-send-name = ""
recv-password = ""
substitute-recv-name = ""
enabled = yes
fill-1 = 0
link-compression = mppc
mru = 1524
lqm = no
disconnect-on-auth-timeout = yes
lqm-minimum-period = 600
lqm-maximum-period = 600
acf-comp-enabled = no
pf-comp-enabled = no
async-control-char-map = ff:ff:ff:ff
cbcp-enabled = no
```

---

```

mode-callback-control = cbc-no-callback
delay-callback-control = 0
trunk-group-callback-control = 4
split-code-dot-user-enabled = no
mtu = 1524
auth-for-async-framed-users = required
max-pap-auth-retry = 0

```

## RADIUS changes

MPPC can be enabled in the RADIUS connection profile by setting Ascend-Link-Compression = Link-Comp-MPPC.

RADIUS example:

```

mppc Password = "Ascend"
 User-Service = Framed-User,
 Framed-Protocol = PPP,
 Framed-Address = 10.10.10.10,
 Framed-Netmask = 255.255.255.0,
 Ascend-Link-Compression = Link-Comp-MPPC

```

## ***SS7-IPDC: On PSTN trunk disconnection, notify signaling gateway and keep calls***

In this release of TAOS, the way that the TAOS unit responds to a loss of signal or synchronization on a digital T1 or E1 line has been changed to provide an option to hold calls active on that line for a specified period of time. To manage this new behavior, the resilience-options subprofile has been added to the SS7-GATEWAY profile.

## Overview

Previously, when a TAOS unit lost synchronization on a T1 or E1 digital line the following events took place:

- An SS7 NLS message was sent to the signaling gateway, indicating that the line is down
- All calls on that line were dropped
- An SS7 ACR message for each call was sent to the signaling gateway, acknowledging release of the call

With this release of TAOS, when a T1 or E1 digital line is lost, the TAOS unit can be configured to maintain the connection of those calls for a certain period of time. If the line is reestablished during this time, call connections are recovered, and the calls are not dropped.

Disconnection of calls can be placed under control of either the signaling gateway or a timer in TAOS. Regardless of which option is configured, all calls that are in a transient state are released when the digital line is lost. Also, all channels in the line are set to an out-of-service state, which means that new calls requesting service on any of the channels of the failed digital line are rejected.

## Command line changes

Within the `SS7-GATEWAY` profile, a `resilience-options` subprofile has been added. This subprofile contains a parameter, named `type`, to set the type of behavior that the TAOS unit will follow when a T1 or E1 line is lost. A second parameter, named `duration`, sets the length of time that calls connections will be maintained, if they are to be disconnected after a fixed period of time. The following is an example of the new subprofile.

```
[in SS7-GATEWAY:resilience-options]
type = release-all
duration = 0
```

There are three possible settings that can be entered as the `resilience-options type`:

- `release-all`
- `maintain-active`
- `timed-release`

### *The release-all option*

When the `resilience-options type` is set to `release-all`, the following events take place when T1 or E1 line synchronization is lost:

- An SS7 NLS message is sent to the signaling gateway, indicating that the line is down
- All calls on that line are dropped
- An SS7 acknowledgement of release (ACR) message for each call is sent to the signaling gateway, acknowledging release of the call

This is the default setting shown in the previous example.

### *The maintain-active option*

When the `resilience-options type` is set to `maintain-active`, the following events take place when T1 or E1 line synchronization is lost and remains lost:

- An SS7 NLS message is sent to the signaling gateway, indicating that the line is down
- The TAOS unit maintains all call connections until it receives a request to release (RCR) message from the signaling gateway.
- Upon request to reset, the TAOS unit drops the call and returns an acknowledgement of release (ACR) message to the signaling gateway

If synchronization of the T1 or E1 line is reestablished before the signaling gateway requests a release, call connections are recovered and the calls are not dropped.

The following example shows how the `resilience-options type` is set to `maintain-active`.

```
[in SS7-GATEWAY:resilience-options]
type = release-all
duration = 0

admin> set type = maintain-active

admin> list
```

```
[in SS7-GATEWAY:resilience-options (changed)]
type = maintain-active
duration = 0

admin> write
```

### *The timed-release option*

When the `resilience-options` type is set to `timed-release`, the following events take place with T1 or E1 line synchronization is lost and remains lost:

- An SS7 NLS message is sent to the signaling gateway, indicating that the line is down
- The TAOS unit waits for the amount of time specified in the duration value
- If the T1 or E1 line reestablishes synchronization within the specified time, call connections are maintained
- If the T1 or E1 line does not reestablish synchronization, the TAOS unit initiates release of the call connections.

The valid range of numeric settings for the duration value are 0-2147483647, indicating the number of milliseconds that the call can be held, pending the restoration of the digital line, before being dropped.

The following example shows how to set the `resilience-options` type to `timed-release` and the release duration to 1000 milliseconds (1 second).

```
[in SS7-GATEWAY:resilience-options]
type = release-all
duration = 0

admin> set type = timed-release

admin> set duration = 1000

admin> list

[in SS7-GATEWAY:resilience-options (changed)]
type = timed-release
duration = 1000

admin> write
```

## ***Differentiated services code point (DSCP) support***

This release adds parameters to Connection, Filter, and VoIP profiles and a new RADIUS attribute to support the ability to mark packets for differentiated services that are compatible with RFC 2474. At this time, queuing strategies, per-hop behaviors, and other QoS schemes defined in RFC 2474 are not supported.

### **Differentiating class of service**

The second octet in the IP datagram header carries the service parameters that are associated with the packet. These parameters specify how the packet is handled by the devices within the network that are capable of recognizing and acting upon them.

Previously, TAOS used the first six bits in the second octet to indicate the precedence and type of service (TOS) of the packet in the structured manner defined in RFC 791 only. The first six bit positions represented the values of four defined parameters as shown in Table 9.

Differentiated services code point (DSCP) marking, as defined in RFC 2474, uses the same six bits to differentiate the service associated with the packet in a less structured way. The first six bits can be used to create values (00 to 3F) specifying different classes of service.

*Table 9. Second IP header octet utilization*

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

**Note:** TAOS 9.1.0 allows DSCP code information to be specified, so that it can be acted upon by other network devices. However, at this time TAOS 9.1.0 does not interpret or support queuing strategies, per-hop behaviors, or other QoS schemes defined in RFC 2474.

## Command line changes

Two parameters, shown in Table 10, have been added to Connection, Filter, and VoIP profiles.

*Table 10. New TAOS parameters for DSCP marking*

| Parameter    | Specifies which standard you want the handling of packets to follow. Set one of the following values:                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| marking-type | <ul style="list-style-type: none"><li>precedence-tos (default) - specifies RFC 791 as the standard to differentiate class of service</li></ul>                                                                                               |
| dscp         | <ul style="list-style-type: none"><li>dscp - specifies RFC 2474 as the standard to differentiate class of service. The DSCP value if DSCP is specified in the marking-type parameter. Values can range from 00 to FF (hexidecimal)</li></ul> |

**Note:** Although all eight bits of the second octet in the IP packet header can be set by entering hexadecimal values from 00 to FF, to stay compliant with RFC 2474 only the first six bits should be set, by entering values from 00 to 3F.

## Connection profiles

In a Connection profile, the new DSCP parameters are located in the `tos-options` subprofile, as shown in the following example:

```
[in CONNECTION/test-profile:ip-options:tos-options (new)]
active = no
precedence = 000
type-of-service = normal
apply-to = incoming
marking-type = precedence-tos
dscp = 00
```

## Filter profiles

In a Filter profile, the new DSCP parameters are located in the `tos-filter` subprofile of a specific input or output filter, as shown in the following example:

```
[in FILTER/test-filt:input-filters[1]:tos-filter (new)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = 0
dest-port = 0
precedence = 000
type-of-service = normal
marking-type = precedence-tos
dscp = 00
```

## VoIP profiles

In the VoIP profile, the new DSCP attributes are located in the `tos-options` subprofile, as shown in the following example:

```
[in VOIP/{ " " } :tos-options (new)]
active = no
precedence = 101
type-of-service = latency
apply-to = both
marking-type = precedence-tos
dscp = 00
```

## RADIUS support

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

|           |                |   |         |
|-----------|----------------|---|---------|
| ATTRIBUTE | Ascend-IP-DSCP | 3 | integer |
|-----------|----------------|---|---------|

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

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

To select DSCP marking over the default Precedence-TOS marking, the `Ascend-IP-TOS` RADIUS attribute must be set to `IP-TOS-Dscp`. The new `Ascend-IP-DSCP` RADIUS attribute is used to specify the DSCP value to be set in the Connection profile. The value

specified in the RADIUS profile must be the decimal equivalent of the binary bit setting desired in the second octet of the IP packet header.

Following is an example RADIUS profile, named `test`. The last two lines show how to specify the use of DSCP marking and set the DSCP value to 252.

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

## ***SS7: Command-level generation of DS0 test tones***

A new argument, `a`, for the `ss7call -m` debug-level command enables you to test DS0 channels before SS7 call establishment. New log messages report the activation of the test tones.

**Note:** Currently, the `ss7call` command can generate tones on up to 24 channels of an 8T1 card at the same time, and up to 64 channels of a CT3 card at the same time.

### **Command usage**

The `ss7call` command is available only on systems that have the Lucent Technologies SS7 software license enabled. To use the `ss7call` command, the User profile for your login must have debug permissions enabled.

The `ss7call -m` command supports a new `a` argument to generate an arbitrary test tone on a DS0 channel before SS7 call establishment. DS0-level testing is typically done before connecting the MAX TNT unit to a Softswitch. The new option uses the following syntax:

```
ss7call -m a freq1 [, freq2 [, power-level [, duration]]] logical-address
```

Brackets indicate an optional argument and are not part of the command syntax.

| <b>Argument</b>            | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>freq1, freq2</i></b> | Frequencies, in Hertz (Hz), to be mixed into the signal. The <i>freq1</i> value must be specified and has no default. The valid range is from 1 through 3999 for <i>freq1</i> . The default value for <i>freq2</i> is zero. The valid range is from 0 through 3999 for <i>freq2</i> .<br><br>When both values are specified, the system generates a dual-tone multifrequency (DTMF) signal. If only <i>freq1</i> is specified and <i>freq2</i> is zero, the system generates a single-tone signal. |



| Argument               | Description                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>power-level</i>     | Power level of the signal to be generated. The default power level is 0dBm0. If the value is from -50 through 3, it is expressed in dBm0. Lucent Technologies recommends use of values within this range (dBm0 values). If the value is from 4 through 32767, it is an absolute value. The relationship of dBm0 to the absolute values is as follows:<br>$absolute-value = 22748.4 * 10 ^ {(dBm0/20)}$ |
| <i>duration</i>        | Duration of the signal to be generated, in milliseconds. The default duration is zero, which means that the signal continues indefinitely until it is interrupted. For information about interrupting a signal, see “Events that interrupt continuous test tones” on page 39.                                                                                                                          |
| <i>logical-address</i> | Logical address of the DS0 channel on which the signal is sent. In TAOS, logical addresses use the following address format:<br>$\{ \{ shelf-N slot-N line-N \} channel-N \}$                                                                                                                                                                                                                          |

For example, the following command generates a single 1004Hz tone at -2dBm0 for 5 seconds on the fourth DS0 channel in shelf 1, slot 2, line 3:

```
admin> ss7call -m a 1004,0,-2,5000 { { 1 2 3 } 4 }
```

The following command initiates continuous generation of a 1004Hz milliwatt tone at 0dBm0 on the fourth DS0 channel in shelf 1, slot 2, line 3:

```
admin> ss7call -m a 1004 { { 1 2 3 } 4 }
```

## Events that interrupt continuous test tones

The following events cancel a test signal activated by the `ss7call -m a` command:

- You cancel the test by entering `ss7call -m i` to bring the channel into service or `ss7call -m o` to take the channel out of service.
- The MAX TNT unit receives an IPDC SCS message or an ASGCP/Q.931+ RESTART message from the Softswitch. If the Softswitch tries to restart a channel, maintenance actions on that channel are automatically canceled.
- The MAX TNT unit receives a call on the channel. If a call arrives on a channel that is generating a test tone, the test tone is canceled and the call is processed as usual.

## Related log messages

The system logs messages that indicate that a test tone has been activated by means of the `ss7call -m a` command and that reflect the status of those tones. The messages are logged according to the usual TAOS method, as specified in the Log profile, User profile, or both. You can modify the configuration in those profiles to filter unwanted messages by severity level. The log messages have the following format:

```
ADMIN ss7call DSP transaction: status for logical-address
```

| Variable               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|----------------|----------------|----------------|---------|---------|----------|---------|-----------------|-------|---------------|-------|-----------------|-------|---------|--------|-----------|--------|------------|--------|
| <i>status</i>          | Indicates the status of the tone generation. Following are the possible values: <table> <tr> <th>Message</th><th>Severity level</th></tr> <tr> <td>Request queued</td><td>Software Debug</td></tr> <tr> <td>Timeout</td><td>Warning</td></tr> <tr> <td>Canceled</td><td>Warning</td></tr> <tr> <td>Invalid request</td><td>Error</td></tr> <tr> <td>Resource busy</td><td>Error</td></tr> <tr> <td>Buffer overflow</td><td>Error</td></tr> <tr> <td>Started</td><td>Notice</td></tr> <tr> <td>Completed</td><td>Notice</td></tr> <tr> <td>Final tone</td><td>Notice</td></tr> </table> | Message | Severity level | Request queued | Software Debug | Timeout | Warning | Canceled | Warning | Invalid request | Error | Resource busy | Error | Buffer overflow | Error | Started | Notice | Completed | Notice | Final tone | Notice |
| Message                | Severity level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Request queued         | Software Debug                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Timeout                | Warning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Canceled               | Warning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Invalid request        | Error                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Resource busy          | Error                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Buffer overflow        | Error                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Started                | Notice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Completed              | Notice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| Final tone             | Notice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |
| <i>logical-address</i> | Logical address of the DS0 channel to which the DSP is connected. In TAOS, logical addresses use the following address format: <pre>{ { shelf-N slot-N line-N } channel-N }</pre>                                                                                                                                                                                                                                                                                                                                                                                                      |         |                |                |                |         |         |          |         |                 |       |               |       |                 |       |         |        |           |        |            |        |

In addition, the Line status window displays an m (for *maintenance*) for each channel on which a test tone is being generated

## Examples showing usage and log messages

The following command initiates continuous generation of a 1004Hz milliwatt tone at 0dBm0 on the fourth DS0 channel in shelf 1, slot 2, line 3:

```
admin> ss7call -m a 1004 { { 1 2 3 } 4 }
```

The system logs the following message to indicate that the test has started:

```
LOG notice, Shelf 1, Controller, Time: 19:24:19--
ADMIN ss7call DSP transaction: Started for { { 1 2 3 } 4 }
```

The following command brings the fourth DS0 channel in shelf 1, slot 2, line 3 into service, which terminates the test:

```
admin> ss7call -m i { { 1 2 3 } 4 }
```

The system logs the following message to indicate that the test was canceled:

```
LOG warning, Shelf 1, Controller, Time: 19:25:33--
ADMIN ss7call DSP transaction: Canceled for { { 1 2 3 } 4 }
```

The following command generates a single 1004Hz tone at -2dBm0 for 5 seconds on the fourth DS0 channel in shelf 1, slot 2, line 3:

```
admin> ss7call -m a 1004,0,-2,5000 { { 1 2 3 } 4 }
```

The system logs the following messages, indicating when the test started and completed:

```
LOG notice, Shelf 1, Controller, Time: 19:26:02--
ADMIN ss7call DSP transaction: Started for { { 1 2 3 } 4 }
```

```
LOG notice, Shelf 1, Controller, Time: 19:26:07--
ADMIN ss7call DSP transaction: Completed for {{1 2 3} 4}
```

## ***T1 channel idle pattern support***

A new parameter in each T1 profile defines the idle pattern for the channel that the profile configures. The idle pattern is transmitted on the configured channel when the channel is in the idle state. Channel idle-pattern transmission is currently enabled on the T1 slot card and the T3 slot card. It applies to all T1 channels except channel 24, the D channel. For all other pattern types, it applies to all T1 channels.

To define the idle pattern, set the `idle-pattern` parameter to any decimal value from 0 (all zeros) to 255 (all ones). For example, the following command specifies a pattern of alternating ones and zeros:

```
admin> set idle-pattern = 170
```

The default value is 255

The new idle pattern takes effect when the profile is saved.

## **Modem manager features in TAOS 9.1.0**

### ***Firmware versions for digital modems***

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

- Series56 Digital Modem cards (also called CSM/1, TNT-SL-48MOD-S56) support V2.0982-K56\_2M\_DLP\_CSM firmware.
- Series56 II Digital Modem cards (also called CSM/3, TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C) support V5.8177 firmware.
- Series56 III Digital Modem cards (also called CSMV/3, TNT-SL-48MODV3-S-C) support V5.8177 firmware.

### ***Firmware versions for MultiDSP cards***

This release includes the following Lucent firmware versions for MAX TNT and APX 8000 MultiDSP cards:

- 48-port MultiDSP cards (TNTP-SL-ADI-C or TNTV-SL-ADI-C) support Controller V0.1.46, Modem DSP V0.1803.0, and VoIP DSP V3.0.35 Lucent V0.1622.0 firmware.
- 96-port MultiDSP cards (APX8-SL-96DSP) support Controller V0.1.46, Modem DSP V0.1803.0, and VoIP DSP V3.0.35 Lucent firmware.

## ***Support for V.92 and V.44 modem standards***

TAOS 9.1.0 offers preliminary support for the new V.92 modem standard and complete support for the V.44 compression standard. The V.92 modem standard extends the existing V.90 standard with new capabilities that include Modem on Hold, Quick Connect, and Pulse-Code Modulation (PCM) Upstream. The V.44 compression standard improves on the previous V.42bis compression standard and allows for faster data transfer speeds.

**Note:** Because V.92 is a new standard, some V.92 client modems might not fully support the new capabilities. Lucent recommends that end users regularly check with their manufacturers for firmware updates. V.92 capabilities are only achieved when the client modems are V.92 compatible, otherwise the modems fall back to a normal V.90 connection.

### **V.92 enhancements**

This TAOS release adds the V.92 Modem on Hold and Quick Connect capabilities to the 48-port and 96-port MultiDSP slot cards. PCM Upstream will be implemented in future releases.

#### ***V.92 Modem on Hold feature***

The Modem on Hold (MoH) feature allows a user to use call waiting while engaged in a modem session. The modem connection can be put on hold without being disconnected, and can be resumed when the voice call is completed. It may take a certain amount of time (comparable to a regular modem hand-shake) before the modem is connected.

When a V.92 modem receives a call-waiting tone, it sends an MoH request to the server modem. The server modem might accept or deny this request. If the request is accepted, then the server modem sends an on hold timeout value to the client modem, and the modems will go on hold. If the client modem does not complete the voice call and resume the data call within the specified timeout duration, the server modem will drop the connection.

#### ***V.92 Quick Connect feature***

The Quick Connect feature shortens the time normally taken by V.90 modems to establish a connection by reducing the duration of phase 1 and phase 2 negotiations. Quick Connect may not function properly with the local loop if the connection changes in subsequent calls.

#### ***V.92 PCM Upstream feature***

The PCM Upstream feature increases the maximum upstream data transfer rate from V.90 33,600 bits/second (bps) to 48,000 bps. This feature is not yet available.

### *modem-on-hold-timeout parameter for V.92*

The `modem-on-hold-timeout` parameter sets the time that the server modem remains on hold after the client modem receives a call and requests that the data call be suspended. The `modem-on-hold-timeout` parameter can be set in the connection profile, or globally set in the modem-configuration subprofile of the terminal-server profile. The values for the parameter are as follows:

| Values                               | Result                                                                                                                                                             |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>moh-disabled</code>            | Disables modem on hold (default)<br>(Valid for the modem-configuration subprofile only)                                                                            |
| <code>10-sec-moh-timeout</code>      | Sets the modem on hold timeout to 10 seconds                                                                                                                       |
| <code>20-sec-moh-timeout</code>      | Sets the modem on hold timeout to 20 seconds                                                                                                                       |
| <code>30-sec-moh-timeout</code>      | Sets the modem on hold timeout to 30 seconds                                                                                                                       |
| <code>40-sec-moh-timeout</code>      | Sets the modem on hold timeout to 40 seconds                                                                                                                       |
| <code>1-min-moh-timeout</code>       | Sets the modem on hold timeout to 1 minute                                                                                                                         |
| <code>2-min-moh-timeout</code>       | Sets the modem on hold timeout to 2 minutes                                                                                                                        |
| <code>3-min-moh-timeout</code>       | Sets the modem on hold timeout to 3 minutes                                                                                                                        |
| <code>4-min-moh-timeout</code>       | Sets the modem on hold timeout to 4 minutes                                                                                                                        |
| <code>6-min-moh-timeout</code>       | Sets the modem on hold timeout to 6 minutes                                                                                                                        |
| <code>8-min-moh-timeout</code>       | Sets the modem on hold timeout to 8 minutes                                                                                                                        |
| <code>12-min-moh-timeout</code>      | Sets the modem on hold timeout to 12 minutes                                                                                                                       |
| <code>16-min-moh-timeout</code>      | Sets the modem on hold timeout to 16 minutes                                                                                                                       |
| <code>no-limit-moh-timeout</code>    | Sets the modem on hold timeout to unlimited                                                                                                                        |
| <code>conn-profile-use-global</code> | Sets the value for all the modem sessions unless specified in the respective connection profiles. The value in the connection profile overrides this global value. |

**Note:** Although V.92 allows for a maximum on hold time of 16 minutes, timeout values in higher protocol stacks may interrupt data applications before the on hold time is up. Network administrators should examine the implications of enabling modem on hold for their network applications. For example, the end-user should not expect file transfers using FTP or similar protocols to resume after the modems have reestablished connection.

**Note:** You should generally set the value of the `idle-timer` parameter of a connection profile to be at least 30 seconds longer than the value of the `modem-on-hold-timeout` parameter in order to prevent calls that have been placed on hold from being disconnected prematurely.

## Modem manager features in TAOS 9.1.0

*Support for V.92 and V.44 modem standards*

---

The following example shows how to set the modem-on-hold-timeout value for a connection profile to 2 minutes.

```
[in CONNECTION/test-profile (new)]
station* = ""
active = no
encapsulation-protocol = mpp
called-number-type = national
dial-number = ""
...
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global

admin> set modem-on-hold-timeout = 2-min-moh-timeout

admin> list

[in CONNECTION/test-profile (new)]
station* = ""
active = no
encapsulation-protocol = mpp
called-number-type = national
dial-number = ""
...
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = 2-min-moh-timeout
```

### *quick-connect-enabled parameter for V.92*

The new quick-connect-enabled parameter enables and disables the QuickConnect feature.

| Value | Result                                           |
|-------|--------------------------------------------------|
| yes   | Enable Quick-Connect feature                     |
| no    | Disable Quick-Connect feature<br>(Default value) |

## *V.92 Ascend-MOH-Timeout attribute in RADIUS*

The Ascend-MOH-Timeout RADIUS attribute has been added to the dictionary to support setting the modem-on-hold-timeout value for an individual connection.

|           |                    |     |         |
|-----------|--------------------|-----|---------|
| ATTRIBUTE | Ascend-MOH-Timeout | 261 | integer |
|-----------|--------------------|-----|---------|

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

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

The following is an example RADIUS profile. The last line shows how you would set the MoH timeout value to 16 minutes.

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

## *Disconnect-Reason-Type value in V.92 logging*

There is a new `disconnect-reason-type` that is logged to syslog and RADIUS accounting servers. This value will be logged when a modem is disconnected due to the maximum-on-hold-timeout being exceeded.

|       |                        |                             |    |
|-------|------------------------|-----------------------------|----|
| VALUE | Disconnect-Reason-Type | DIS_MODEM_MOH_TIMER_EXPIRED | 19 |
|-------|------------------------|-----------------------------|----|

## *Progress-Type value in V.92 logging*

There is a new `progress-type` that will be logged to syslog and RADIUS accounting servers when a call is in an on hold state.

|       |               |                 |    |
|-------|---------------|-----------------|----|
| VALUE | Progress-Type | PR_MODEM_ONHOLD | 34 |
|-------|---------------|-----------------|----|

## V.44 enhancements

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

### *V44-Enabled parameter*

There is a new `v44-enabled` parameter available in the `modem-configuration` subprofile of the `terminal-server` profile. This boolean parameter specifies whether the TAOS unit will negotiate V.44 compression with modems having this feature.

| Value | Result                                                  |
|-------|---------------------------------------------------------|
| yes   | Enable V.44 compression negotiation                     |
| no    | Disable V.44 compression negotiation<br>(Default value) |

The following shows a sample `modem-configuration` profile after the `v44-enabled` parameter has been enabled.

```
admin> read term
TERMINAL-SERVER read
admin> list modem
[in TERMINAL-SERVER:modem-configuration]
v42/mnp = will-v42
max-baud-rate = 33600-max-baud
modem-transmit-level = -13-db-mdm-trn-level
cell-mode-first = no
cell-level = -18-db-cell-level
7-even = no
modem-mod = v90-modulation
AT-answer-string = ""
modem-on-hold-timeout = moh-disabled
quick-connect-enabled = no
max-v92-receive-baud-rate = 48000-max-v92-baud
v44-enabled = yes
```

### *Ascend-Compression-Protocol value for V.44 logging*

There is a new V.44 Ascend-Compression-Protocol value that is logged to RADIUS accounting servers. The V.44 value is logged when a connection is made using V.44 compression.

VALUE      Ascend-Compression-Protocol v44

4



# Authentication and accounting features in TAOS 9.1.0

## ***Support for selection of authentication method for command-line-interface users***

Previously, if a command-line-interface user failed authentication by means of local User profiles, the MAX TNT unit attempted authentication by means of an external authentication server, such as a RADIUS server, if one was enabled and configured. The sequence was based on the setting of the `local-profiles-first` parameter. (For additional information about the `local-profiles-first` parameter, see the *APX 8000/MAX TNT Reference*.) Depending on the setting of the `local-profiles-first` parameter, if a command-line-interface user logged in incorrectly and an external authentication server was unavailable, the system recovery time was lengthy.

With TAOS 9.1.0, you can select the authentication method that the MAX TNT unit uses to authenticate a command-line-interface user. By setting the `cli-user-auth` parameter in the `external-auth` profile, you can specify whether the MAX TNT unit authenticates a command-line-interface user by means of local profiles or an external authentication server, and if the authentication is to be in any specific order. Specify one of the following values:

| Value                                       | Specifies                                                                                                                                                                                                  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>local-then-external</code> (default)  | The MAX TNT unit uses local User profiles for the first authentication attempt. If that attempt fails, the unit attempts authentication through an external server, if an external authentication server . |
| <code>local-only</code>                     | The MAX TNT unit uses only local User profiles.                                                                                                                                                            |
| <code>external-only</code>                  | The MAX TNT unit uses only an external authentication server and ignores local User profiles.                                                                                                              |
| <code>external-then-local</code>            | The MAX TNT unit authenticates by means of an external authentication server. If authentication fails or times out, the unit uses local User profiles to make another attempt.                             |
| <code>external-then-local-if-timeout</code> | The MAX TNT unit authenticates by means of an external authentication server. If authentication times out, the unit uses local User profiles to make another attempt.                                      |

The following example shows how to specify a value sample setting for the `cli-user-auth` parameter:

```
[in EXTERNAL-AUTH]
auth-type = RADIUS
rad-serv-enable = yes
cli-user-auth = local-then-external
```

## Support for DNIS fallback

TAOS 9.1 includes a DNIS fallback feature, which enables you to configure the MAX TNT unit to accept a call even after Dialed Number Information Service (DNIS) authentication has failed because of a time-out from the RADIUS server. A similar feature, CLID fallback, already exists for Calling-Line ID (CLID). The DNIS fallback feature does not apply to DNIS authentication using local profiles.

To support this new capability, TAOS 9.1.0 adds the `dnis-fallback` setting to the `clid-auth-mode` parameter in the `answer-defaults` profile. If the `clid-auth-mode` parameter is set to `dnis-fallback`, the MAX TNT unit requires DNIS on the line and it uses RADIUS to authenticate the call. However, if the RADIUS server does not respond, the MAX TNT unit performs password authentication instead of dropping the call.

If the `clid-auth-mode` parameter is set to `dnis-fallback`, the MAX TNT unit takes the a given action when it encounters one of the following situations:

| Situation                        | Action                                     |
|----------------------------------|--------------------------------------------|
| No DNIS is received on the line. | The MAX TNT unit drops the call.           |
| RADIUS authentication fails.     | The MAX TNT unit drops the call.           |
| RADIUS authentication passes.    | The MAX TNT unit proceeds with call setup. |
| RADIUS authentication times out. | The MAX TNT unit proceeds with call setup. |

For information about the other settings for a `clid-auth-mode` parameter, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Guide* and the *APX 8000/MAX TNT Reference*.

The following example shows how to configure the MAX TNT unit for DNIS fallback:

```
[in ANSWER-DEFAULTS]
Admin> set clid-auth-mode = dnis-fallback
Admin> write
ANSWER-DEFAULTS written
```

## Maximum accounting checkpoint interval increased

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

## Command-line interface changes

You can now specify a value from 0 through 1440 for the `Acct-Checkpoint` parameter in the `External-Auth > Rad-Acct-Client` profile.

### *Acct-Checkpoint*

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

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

**Example:** `set acct-checkpoint = 120`

**Location:** External-Auth > Rad-Acct-Client

**See Also:** Acct-Host

## ***Support for selecting PAP authentication before CHAP***

With TAOS 9.1, you can configure a MAX TNT unit to offer authentication protocols in the following order during link control protocol (LCP) negotiations:

- 1 Password Authentication Protocol (PAP)
- 2 Challenge Handshake Authentication Protocol (CHAP)
- 3 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

If a client refuses to accept PAP authentication (for example, a Microsoft Windows client that is configured to accept only encrypted authentication), the MAX TNT unit then offers CHAP or MS-CHAP authentication.

TAOS 9.1.0 supports one-way authentication of a dial-in client, but not authentication for bidirectional CHAP or MS-CHAP Connection profiles.

## **Command-line interface support**

TAOS 9.1 adds the `pap-preferred` setting for the `receive-auth-mode` parameter of the `ANSWER PROFILE:PPP-answer` subprofile. The following example configures the MAX TNT unit to offer PAP before CHAP or MS-CHAP authentication:

```
[in ANSWER-DEFAULTS:ppp-answer]
admin> set receive-auth-mode = pap-preferred
admin> write
```

## **RADIUS support**

The RADIUS dictionary now includes the following values for the `PppAuthType` attribute:

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

## ***RADIUS session-based checkpoint accounting***

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

### **Command-line interface changes**

You can specify per-session checkpoint accounting by setting a new parameter, `Acct-Checkpoint-Timer`, in the `External-Auth > Rad-Acct-Client` subprofile.

#### *Acct-Checkpoint-Timer*

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

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

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

**Example:** `set acct-checkpoint-timer = per-session`

**Dependencies:** For the `Acct-Checkpoint-Timer` parameter to apply, RADIUS accounting must be enabled.

**Location:** `External-Auth > Rad-Acct-Client`

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

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

## ***Call logging support for DS3, DS3/ATM2, and OC3 slot cards***

TAOS 9.1.0 adds call logging support for unchannelized DS3, DS3/ATM2, and OC3 TAOS unit slot cards. Unchannelized DS3, DS3/ATM2, and OC3 slot cards now log `START`, `STOP`, and `STREAMING` call logging packets. Whenever the line comes up, a `START` packet with the appropriate call logging parameters is transmitted to the call logging server. Similarly, when the line goes down, a `STOP` packet with appropriate parameters is sent to the call logging server. In addition, `STREAMING` call logging packets are logged at intervals specified by the `call-log-stream-period` parameter.

To use this feature, `call-log-enable` must be set to `yes` in the `CALL-LOGGING` profile.

An example of a call logging configuration:

```
[in CALL-LOGGING]
call-log-enable = yes
call-log-host-1 = 192.168.1.1
call-log-port = 1646
call-log-key = Ascend
call-log-stream-period = 2
call-log-radius-compat = 16-bit-vendor-specific
call-log-stream-period=3
```

A slot card specific configuration is not necessary to support this feature. If call logging is enabled as shown above, then the START, STOP, and STREAMING packets will be logged to the logging server.

## ***New attributes for progress call logging packet***

Two new attributes are introduced for progress call logging packets to inform the call logging server when a VoIP call is changed to a real-time fax call. These attributes are vendor-specific for Ascend and Lucent, and enable the call logging server to change VoIP packets to real-time fax calls.

Following are the new attributes for the progress call logging packet:

```
Ascend-Xmit-Rate
Ascend-Modulation
```

**Note:** `Ascend-Xmit-Rate` is vendor-specific to Ascend, and `Ascend-Modulation` is vendor-specific to Lucent.

## ***Support for limiting the number of simultaneous users of a shared profile***

A new `max-shared-users` parameter has been added to the Connection profile that limits the number of users that can be simultaneously connected using a shared profile.

In previous releases of TAOS, there was no way to limit the number of users that could be connected using a given shared profile. In this release of TAOS, the `max-shared-users` parameter allows you to optionally limit the number of simultaneous users of a shared connection profile.

The default value for the `max-shared-users` is zero which does not limit the number of users that can connect using that profile. This attribute can be set to any value between zero and the maximum number of calls that can be handled by the TAOS unit, which varies depending on the number and type of slot cards that are installed in the unit.

When this parameter has been specified for a profile, a new call is dropped if the total active `mp-bundles` and `ppp-sessions` for the user is greater than the value of `max-shared-users` for that profile.

# Routing features in TAOS 9.1.0

## ***BGP routing support***

In this release, you can configure IP routing using version 4 of the Border Gateway Protocol (BGP).

**Note:** BGP is supported on both the MAX TNT and APX 8000 platforms, even though the following feature description highlights APX platform specific examples.

### **Overview**

The Border Gateway Protocol (BGP) is an exterior routing protocol. BGP version 4, described in RFC 1771, and further defined in version 5 of the BGP-4 Internet Draft RFC of January 1997, was designed for routing between autonomous systems. To use BGP, each autonomous system must have an autonomous system identifier. You obtain autonomous system identifiers from the Internet Network Information Center (InterNIC).

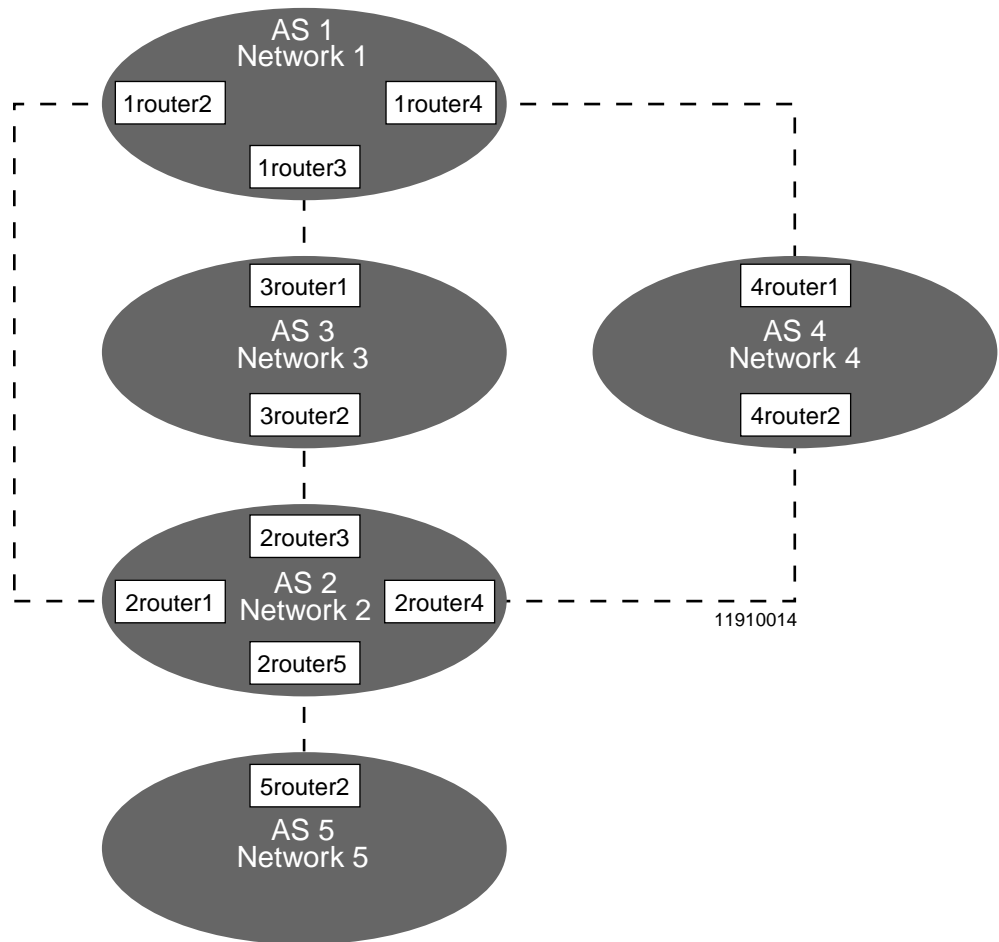
BGP can be thought of as the “glue” that holds the Internet together. Consequently, BGP routing tables can contain tens of thousands of routes. This number is increasingly rapidly as the Internet expands.

The primary purpose of BGP is to allow different autonomous systems to share routes and to connect in redundant ways, controlled by policy and protocol design, so that routing loops are not formed.

### ***Routing with BGP***

Figure 1 illustrates companies in five autonomous systems that use BGP as an exterior routing protocol.

Figure 1. Example of Linked Multiple Autonomous Systems



Autonomous system AS 1 advertises Network 1; autonomous system AS 2 advertises Network 2, and so on. A pair of BGP routers is located between each pair of autonomous systems. For example, *1router4* and *4router1* are located between AS1 and AS4.

### Policies for best-path selection

BGP does not advertise a simple metric representing cumulative link bandwidth costs, as do protocols such as OSPF. Instead, BGP advertises only a path through zero or more autonomous systems, the attributes of the path, and sets of destinations reachable at the end of the path. Sets of destinations are called the network layer reachability information (NLRI). The combined bundle of the path, attributes, and NLRI is called a BGP route. Based on BGP route information, each BGP router executes policy decisions to choose the best route to a final destination.

AS 1 has the following information about paths to Network 5:

- Via *4router1*, along path AS 4 -> AS 2 -> AS 5
- Via *3router1*, along path AS 3 -> AS 2 -> AS 5
- Via *2router1*, along path AS 2 -> AS 5

Although the third path is shortest, it might not be the best path for your purposes. You can create BGP policies to determine the best path according to your own preferences. For example, you can configure policies that implement path preferences such as the following:

- Paths going through the *3router1* peer are preferred over all others.
- Paths going through AS 2 are used only as a last resort.

### *BGP peers*

BGP does not broadcast route information to all listeners as do RIP and OSPF. Instead, each router running BGP must be configured for every other BGP router with which it needs to communicate. Routers that send BGP messages to each other are called BGP speakers, and each pair of BGP speakers that communicate with each other are called peers. Peers are explicitly configured by the administrator.

Peers are called internal when they belong to the same autonomous system. When peers belong to other autonomous systems, they are referred to as external peers. BGP treats internal and external peers differently in many details. In particular, unless either route reflection or BGP confederations are configured, all internal peers in a single autonomous system must be fully meshed (directly peered) with each other. For example, if AS 25 has four internal peers (A, B, C, D), then it has six pairs of internal peers (AB, AC, AD, BC, BD, CD). If you are using route reflection or confederations, the routers are partially meshed.

### *Confederations*

BGP requires that all BGP peers within an autonomous system be linked to each other—or fully meshed. As a result, when a BGP peer learns an internal route—path attributes and destination—it does not forward this route to the other BGP peers because they already have it. As the number of peers increases in an autonomous system, the number of required links can become large. For example, an autonomous system with 20 peers requires 190 links.

You can reduce the number of BGP peer links by dividing the autonomous system into smaller autonomous systems called confederation member autonomous systems (CMASs). RFC 1965 describes CMASs. If the 20-peer autonomous system is subdivided into a confederation with five CMASs of four peers each, the total number of links is reduced from 190 to 40. This reduction simplifies management of the autonomous system, and reduces message traffic.

### *Route reflection*

Like BGP autonomous system confederations, route reflection (described in RFC 1966) allows the clustering of peers and reduces the number of links that are otherwise required for a fully meshed autonomous system. Although route reflector clusters are configured differently from CMASs, the functional difference between the two is that route reflectors in each cluster maintain path and attribute information across the entire autonomous system. In this way, the autonomous system still functions like a fully meshed autonomous system.

Route reflection is useful when you want to reduce the traffic and CPU overhead of a fully meshed system. However, confederations allow for policy changes and control across the confederation boundaries within an autonomous system, while route reflection requires the use of identical policies on all internal peers. Therefore, if you want to fine-tune routing within the autonomous system, confederations offer a better solution.



## Route Summarization

A BGP speaker can forward to its peers information learned from other peers, as well as originate information into the BGP Internet. BGP originates to its peers only routing information explicitly indicated and supported by the interior routing protocols in use—OSPF, RIP, static routes, or directly attached routes. These special advertisements are called summarizations, and must be explicitly configured.

A summarization is advertised only when an explicit route in that summary is supported through a non-BGP source such as OSPF, RIP, a static route, or a directly attached route—Ethernet, Frame Relay, T1, and so on. The supported route must be more specific than or as specific as the route in the summary. For example, a default route to 0.0.0.0/0 cannot support a summary.

On the TAOS unit, all static routes, either configured or learned via RADIUS, can be summarized automatically through a redistribution policy. You can define a rule for propagating—translating and advertising—all static routes into BGP.

**Note:** In the route summarization implemented in TAOS, route aggregation of BGP learned routes is not currently supported.

## Command-line interface (CLI) changes

Changes to the CLI include the introduction of the following BGP profiles, commands, and additions to the routing table flags:

- BGP profiles
- BGP show commands
- BGP restart command
- BGP debug command
- Routing table flags

## The BGP profiles

The following BGP profiles have been added:

- BGP-global
- BGP-peer
- BGP-summarization
- BGP-policy

### BGP-Global profile

The BGP-global profile defines global parameters. There is only one BGP Global profile per TAOS unit. The following example shows a new BGP Global profile with default values:

```
admin> new bgp-global
BGP-GLOBAL read
admin> list
[in BGP-GLOBAL (new)]
enable = no
autonomous-system = 65534
```

```
id = 0.0.0.0
connect-retry-interval = 120
keepalive-time = 30
hold-time = 90
confed-member-sub-as = 0
cluster-id = 0.0.0.0
igp-lockstep = no
static-route-redist-policy = ""
conn-route-redist-policy = ""
local-pref-default = 100
```

Use the set command to obtain help on configuring a particular parameter. For example:

```
admin> set parameter_name ?
```

### *BGP-Peer profile*

The BGP-peer profile defines a relationship with a BGP peer. You must define one BGP Peer profile for each peer relationship. The following example shows a new BGP Peer profile with default values:

```
admin> new bgp-peer
BGP-PEER/" read
admin> list
[in BGP-PEER/" (new)]
peer-name* = ""
enable = no
peer-ip-address = 0.0.0.0
my-ip-address = 0.0.0.0
autonomous-system = 65534
always-next-hop = no
route-reflector-client = no
confederation-member = no
default-gateway-metric = 0
accept-policy = ""
inject-policy = ""
advertise-policy = ""
```

Use the set command to obtain help on configuring a particular parameter. For example:

```
admin> set parameter_name ?
```

### *BGP-Policy profile*

The BGP-policy profile allows you to define acceptance, injection, advertisement, and redistribution policies. You can fine-tune the routes accepted, injected and advertised to and from other peers, and specify which static and connected routes to redistribute into BGP. The following example shows a new BGP policy:

```
admin> new bgp-policy
BGP-POLICY/" read
admin> list
[in BGP-POLICY/" (new)]
name* = ""
next-policy = ""
rule = [""]
```

See “Creating BGP policies” on page 61 for examples on how to define the rules.

Use the `set` command to obtain help on configuring a particular parameter. For example:

```
admin> set parameter_name ?
```

### BGP-Summarization profile

The BGP-summarization profile allows you to define which route summarizations to advertise to other peers, with the local TAOS unit as the origin. The following example shows a new BGP summarization with default values:

```
admin> new bgp-summarization
BGP-SUMMARIZATION/{ 0.0.0.0/0 } read
admin> list
[in BGP-SUMMARIZATION/{ 0.0.0.0/0 } (new)]
prefix* = { 0.0.0.0/0 }
enable = no
multi-exit-disc-enable = no
multi-exit-disc = 0
local-pref-enable = no
local-pref = 0
community = ""
autonomous-system = [0 +
confed-member-as = [0 +
```

Use the set command to obtain help on configuring a particular parameter. For example:

```
admin> set parameter_name ?
```

## The BGP Show commands

The following show commands have been added:

- `bgp show global`
- `bgp show next-hop`
- `bgp show paths`
- `bgp show peers`
- `bgp show policy`
- `bgp show summarization`

### BGP Show Global command

The `bgp show global` command displays configured information about BGP at the highest level. For example:

```
admin> bgp show global
BGP :enabled
BGP ID[AS]:192.1168.30.10[60001]
BGP timers:Connect 120 Keepalive 30 Hold 90
BGP IGP Lockstep:off
BGP Max multipath 0
```

#### *BGP Show Next-Hop command*

The `bgp show next-hop` command displays the known BGP next hop addresses and the gateways to them. This command provides a convenient way to determine where packets go when forwarded. The information displayed is based on entries in the BGP routing table that are used to forward packets to their destinations.

The following example shows the next-hop count for two interfaces (172.16.95.1 and 172.16.96.1) on the TAOS unit:

```
admin> bgp show next-hop
```

| Next Hop      | Gateway       | Src Addr<br>to it | Source | Metric | Interface<br>----- |
|---------------|---------------|-------------------|--------|--------|--------------------|
| 192.168.1.2   | 172.16.96.2   | 172.16.95.1       |        | 1      | ie0                |
| 172.16.96.129 | 172.16.96.129 | 172.16.96.1       |        | 1      | ie0                |
| 172.16.96.133 | 172.16.96.129 | 172.16.96.1       |        | 1      | ie0                |

**Note:** If the next-hop address and the gateway address are the same, the next hop router is directly adjacent to the TAOS unit interface.

#### *BGP Show Paths command*

The `bgp show paths` command displays BGP path information (also referred to as the BGP routing table) learned by the TAOS unit.

```
admin> bgp show paths [Prefix/NM [verbose]]
```

|         |                                                                                                                                                      |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prefix  | IP prefix address, specified in dotted decimal notation.                                                                                             |
| /NM     | Netmask that indicates the number of high-order bits in the IP prefix. This value is a number from 0 to 32, preceded by a slash (/)—for example /24. |
| verbose | Displays all the network layer reachability information (NLRI) associated with the paths that the specified prefix address is on.                    |

The following example shows output for one entry in the BGP routing table:

```
admin> bgp show paths
```

```
O: INC AAS: 12345 AIP: 1.2.3.4 OID: 192.168.1.130
Cluster List: 192.168.135.1
Sequence: 60149 1 2 3
NH: 172.16.96.76 LP: 100 MED Learned/Used: 100/200
Metrics to NH: 3/2/0/2/0 Gateway to NH: 192.168.10.1
Communities info: 129/129/8454273
NLRI: +10.24.0.0/16/8/7
```

#### *BGP Show Peers command*

The `bgp show peers` command displays a list of BGP peers and, optionally, a summary of packets sent to and received from the peers. Using the command without either optional keyword provides summary information. This is the default.

```
admin> bgp show peers [verbose|packets]
```

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| <i>verbose</i> | Provides detailed information about BGP peers.                     |
| <i>packets</i> | Provides a summary of packets sent to and received from the peers. |

In the following example, BGP peer 192.168.1.2 is a member of autonomous system 2 and is a route-reflector client of the TAOS unit. It is configured to accept and inject BGP policy “only207” and to advertise all routes. For example:

```
Command> bgp show peers
```

| Remote IP   | AS | Flg | DM | Up | Accept  | Inject  | Advertise |
|-------------|----|-----|----|----|---------|---------|-----------|
| -----       |    |     |    |    |         |         |           |
| 192.168.1.2 | 2  | RN  | -- | Up | only207 | only207 | all       |

The R flag in this example identifies this peer as a route-reflector client to the TAOS unit. The N flag indicates that this peer is configured to always consider the TAOS unit as the next hop for any update packet sent by the TAOS unit.

### *BGP Show Policy command*

The `bgp show policy` command lists policy names and definitions. Use the keyword *Policyname* to get information about a specific policy. Without this option only the names of existing BGP policies are displayed.

```
admin> bgp show policy [Policyname]
```

In the following example, the policies on the TAOS unit (add401 and add402) are listed and then information about add401 is displayed:

```
Command> bgp show policy
add401 add402
Command> bgp show policy add401
1 permit
 if prefix 10.0.0.0/8
 then community add 401
```

### *BGP Show Summarization command*

The `bgp show summarization` command shows the route summaries that were manually configured with the `bgp-summary` command. It also shows the static and connected route summaries that are automatically created when you configure the `static-route-redirect-policy` and `conn-route-redirect-policy` parameters in the BGP Global profile.

```
admin> bgp show summarization
```

The following example shows a summary configured for a route to an IP address with a prefix of 10.0.0.0, a netmask of /8, and a multiexit discriminator of 5. The summary is being forwarded to autonomous systems 1, 2, and 3.

```
admin> bgp show summarization
10.0.0.0/8/C Count of Supporting Routes: 53
LP: 0 MED: 5 CAS: no-advertise
```

## Routing features in TAOS 9.1.0

### BGP routing support

---

```
Export to AS: 1 2 3
Export to CMA: 4
```

### The BGP Restart command

The `bgp restart` command allows you to shut down and restart all BGP sessions, or a session with a specified peer.

```
admin> bgp restart [peer [peername / Ipaddress]]
```

When used with no parameters, this command causes the TAOS unit to lose all currently known BGP information, except configuration information. The TAOS unit then rereads configuration information for BGP and re-establishes sessions with peers. This process can take some time to complete.

**Note:** After you use this command, BGP is in a transient state during which the `show` commands are inoperative. The message `bgp restart complete` is reported on the console when you execute the restart process manually.

The following example shows how to restart the BGP session with peer 192.168.1.2:

```
admin> bgp restart peer 192.168.1.2
```

When making changes to the BGP profiles, keep the following in mind:

- When you make changes to a BGP-peer profile and write them, BGP automatically restarts the peer session.
- When you make changes to a BGP-policy profile and write them, you must manually restart the peers that are using this policy.
- When you make changes to the BGP-global profile, it's a good idea to always restart BGP manually.

### The BGP Debug command

The following `bgp debug` command has been added:

```
admin> bgp debug fsm|decision-process|opens|keep-alives|updates|notifications|errors|packets|on|off
```

**Note:** The `bgp debug on` command enables the maximum level of BGP debugging. And, as with other TAOS commands, be sure also to turn debug on.

### Routing table flags

The `Be` flag in the routing table identifies BGP routes learned from an external peer. The `Bi` flag in the routing table identifies BGP routes learned from an internal peer. In the following example, the route 100.1.0.1/32 is a BGP route learned from an external BGP peer.

```
APX201> netstat -rn
```

| Destination  | Gateway      | IF      | Flg | Pref | Met | Use | Age |
|--------------|--------------|---------|-----|------|-----|-----|-----|
| 100.1.0.1/32 | 192.168.10.1 | ie1-4-4 | Be  | 5    | 1   | 0   | 470 |
| 100.3.0.3/32 | 192.168.20.3 | ie1-4-2 | Bi  | 180  | 1   | 0   | 194 |

## Creating BGP policies

You use the new `bgp policy` command to create a policy. After you create a policy, you define it as an acceptance policy, and injection policy, or an advertisement policy. For example, to create a policy called `first_policy`, use the following command:

```
admin> new bgp-policy first_policy
```

List the policy you just created, and then list the rules as follows:

```
admin> list
[in BGP-POLICY/first_policy (new)]
name* = first_policy
next-policy = ""
rule = [""]

admin> list rule
[in BGP-POLICY/first_policy:rule (new)]
rule[1] = ""
rule[2] = ""
rule[3] = ""
rule[4] = ""
. . .
```

The name parameter shows the name of the policy you created. The rule parameters are empty because policies are created without rules. You set rules to define a policy as an acceptance policy, an injection policy, and an advertisement policy as follows:

- You configure an **acceptance policy** with the following rules:

```
set rule RuleNumber permit|deny|include Policyname
[if
[prefix [exactly] Prefix/NM]
[prefix-longer-than NM]
[as-path String|empty]
[community Tag]]
[then
[input-multi-exit-disc Number|strip]
[degree-of-preference Number]]
```

- You configure an **injection policy** with the following rules:

```
set rule RuleNumber permit|deny|include Policyname
[if
[prefix [exactly] Prefix/NM]
[as-path String|empty]
[community Tag]]
```

- You configure an **advertisement policy** with the following rules:

```
set rule RuleNumber permit|deny|include Policyname
[if
[prefix [exactly] Prefix/NM]
[as-path String|empty]
[community Tag]]
[then
[local-pref Number]
[output-multi-exit-disc Number|strip]
[next-hop Ipaddress]
[community add|replace|strip Tag]
[ignore-community-restrictions]]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RuleNumber                         | <p>Number value from 1 to 20.</p> <ul style="list-style-type: none"> <li>• Use the <i>RuleNumber</i> of an existing rule to replace that rule.</li> <li>• Add this rule to the end of the list of rules by using a <i>RuleNumber</i> value that is 1 greater than the current largest rule number.</li> <li>• A maximum of 20 rules is permitted in a policy. If more rules are needed, they can be added with the <b>include</b> <i>Policyname</i> option.</li> </ul>                                                                                                                              |
| permit                             | Allows the IP prefix into the BGP routing table if the criteria in the rule are met.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| deny                               | Prohibits the IP prefix from the BGP routing table if the criteria in the rule are met.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| include<br>Policyname              | <p>Inserts an existing policy <i>Policyname</i> into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| if                                 | <p>Compares the prospective IP prefix against corresponding elements specified after <b>if</b> in this rule. Specifying no <b>if</b> elements causes all prefixes to match the current rule.</p> <ul style="list-style-type: none"> <li>• If all elements of the IP prefix match these <b>if</b> criteria, this rule is applied to the prefix and the prefix is either permitted or denied.</li> <li>• If the elements do not match, the list of policy rules is further scanned for a matching rule.</li> <li>• If no matches are found, the IP prefix is denied from the BGP database.</li> </ul> |
| prefix<br>Prefix/subnet<br>mask    | <p>IP prefix <i>Prefix</i> and netmask <i>subnet mask</i> to compare the prospective IP prefix against. The netmask indicates the number of high-order bits in the IP prefix.</p> <ul style="list-style-type: none"> <li>• Specify <i>Prefix</i> in dotted decimal notation.</li> <li>• Specify <i>subnet mask</i> as number from 1 to 32, preceded by a slash (/)—for example, /24.</li> </ul> <p>By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.</p>                                                           |
| exactly                            | Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| prefix-longer-<br>than subnet mask | When used with the <b>deny</b> keyword, prohibits from the BGP routing table any prospective IP address with a prefix containing more high-order bits than are specified by the netmask <i>subnet mask</i> .                                                                                                                                                                                                                                                                                                                                                                                        |



|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-path String | <p>Autonomous system path <i>String</i> to compare the prospective IP prefix against.</p> <p><i>String</i> is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.</p> <p>When <i>String</i> is compared to an autonomous system path <b>sequence</b>, the order of the sequence must match the order of <i>String</i>. When <i>String</i> is compared to an autonomous system path <b>set</b>, the <b>set</b> is put in ascending numerical order, and then matched against <i>String</i>. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to <i>String</i>.</p> <p>The following special characters have the following meaning in the expression:</p> <ul style="list-style-type: none"><li>• An asterisk (*) matches one or more entries in the autonomous system sequence.</li><li>• A question mark (?) matches any single item in the autonomous system sequence.</li></ul>                                                                                                                                                                                                                                                   |
| empty          | <p>Value for <i>String</i> that matches only paths containing no autonomous system path information.</p> <p>Use <b>as-path empty</b> only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the TAOS unit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| community      | <p>Identifier <i>Tag</i> that categorizes a group of destinations to compare the prospective IP prefix against.</p> <p>See RFC 1997 for more information on a BGP community.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Tag            | <p>Thirty-two-bit number that indicates a destination category in one of the following forms:</p> <ul style="list-style-type: none"><li>• One 32-bit value identifying the autonomous system of the destination</li><li>• Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community <i>Tag</i>, replace the second 16-bit value with the keyword <b>any</b>.</li><li>• One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:<ul style="list-style-type: none"><li>– <b>no-export—Destinations only within a confederation.</b> Advertise the route only to BGP peers within your confederation or autonomous system.</li><li>– <b>no-advertise—No destinations.</b> Do not advertise this route.</li><li>– <b>no-export-subconfed—Internal destinations only.</b> Advertise this route only to internal BGP peers.</li></ul></li></ul> <p>The restrictions imposed by these reserved community keywords do not apply to the TAOS unit originating this information.</p> |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| then                                   | Assigns the following metric or metrics to any IP prefix selected for acceptance by the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| input-multi-exit-disc<br>Number strip  | <p>Assigns an arbitrary <i>Number</i> for the learned multiexit discriminator, overriding any that is learned from the peer. <i>Number</i> is a 32-bit integer. The <b>strip</b> keyword causes any multiexit discriminator information learned from a peer to be ignored.</p> <p><b>input-multi-exit-disc</b> can be abbreviated as <b>imed</b> in this command.</p> <p><b>Lower</b> numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.</p>                                                                                                                                                                                                                                                                                                                     |
| degree-of-preference<br>Number         | <p>Assigns a degree-of-preference <i>Number</i> to a route. <i>Number</i> is a 32-bit integer.</p> <p><b>degree-of-preference</b> can be abbreviated as <b>dop</b> in this command</p> <p><b>Higher</b> numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example.</p> <p>If you do not assign a degree of preference to the IP prefix, one of the following values is assigned by default:</p> <ul style="list-style-type: none"> <li>• If the route comes from an internal peer, the learned local preference number is assigned.</li> <li>• If the route comes from an external peer, <i>Number</i> is based on the autonomous system path length, with a shorter path being preferred.</li> </ul>                                                                  |
| local-pref<br>Number                   | <p>Assigns an arbitrary rating <i>Number</i> to an external route for advertisement to internal or confederation-member peers only. <i>Number</i> is a 32-bit integer.</p> <p><b>local-pref</b> can be abbreviated as <b>lp</b> in this command.</p> <p><b>Higher</b> numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example.</p> <p>If you do not assign a local preference rating to the IP prefix, one of the following values is assigned by default:</p> <ul style="list-style-type: none"> <li>• If the route comes from an internal peer, the learned local preference number is assigned.</li> <li>• If the route comes from an external peer, <i>Number</i> is based on the autonomous system path length, with a shorter path being preferred.</li> </ul> |
| output-multi-exit-disc<br>Number strip | <p>Assigns an arbitrary rating <i>Number</i> for the multiexit discriminator to an external route for advertisement to external or confederation member peers only. <i>Number</i> is a 32-bit integer.</p> <p>A multiexit discriminator configured in a policy takes precedence over one configured in a route summarization.</p> <p><b>output-multi-exit-disc</b> can be abbreviated as <b>omed</b> in this command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Lower** numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.

If you do not assign a multiexit discriminator, no value is sent unless the TAOS unit is advertising one of its own summarizations that specifies a multiexit discriminator. In this case, the value specified in the BGP Summarization profile is used if none is present in the policy.

To avoid advertising any multiexit discriminator, use the **strip** keyword.

|                                       |                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| next-hop<br>Ipaddress                 | Assigns the IP address to advertise as the next hop. If you do not assign a value, a value is computed automatically for the best possible next hop to reach this route. Note that setting this parameter in a policy takes precedence over over setting the <code>always-next-hop</code> parameter in the BGP-peer profile |
| add                                   | Adds the community categories identified in <i>Tag</i> to the IP prefix to be advertised.                                                                                                                                                                                                                                   |
| replace                               | Replaces the community categories identified in the community <i>Tag</i> of the IP prefix to be advertised with new <i>Tag</i> values.                                                                                                                                                                                      |
| strip                                 | Removes existing community categories from the IP prefix to be advertised.                                                                                                                                                                                                                                                  |
| ignore-<br>community-<br>restrictions | Instructs the TAOS unit to ignore the restrictive keywords <b>no-advertise</b> , <b>no-export</b> , and <b>no-export-subconfed</b> when advertising this route to a peer. Use this keyword in the rule to override these restrictions received from other peers.                                                            |

## Configuring a simple BGP policy

This section shows how to create a BGP policy with multiple rules that accepts routing information from just one peer. Before creating the policy, it is helpful to gather some information about the BGP configuration on the TAOS unit. Use the `bgp show peer` command to display BGP peer information. In the following example, the peers has been configured to accept, inject and advertise all routes:

```
admin> bgp show peer
```

| Remote Peer          | AS Flg | DM | Up | Accept | Inject | Advertise |
|----------------------|--------|----|----|--------|--------|-----------|
| apx1 (200.200.200.1) | 2      |    | -- | Up     | all    | all       |

The output shows that just one BGP peer, apx1, is configured to accept, inject, and advertise all routes.

Use the `bgp show path` command to display all the paths in the BGP routing table. For example:

```
admin> bgp show path
```

```
O:IGP
Sequence: 3
NH:200.200.200.3 LP: 100 MED Learned/Used: 0/0
```

## Routing features in TAOS 9.1.0

### BGP routing support

---

```
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.3
NLRI:+220.220.220.3/32/1/0
O:IGP
NH:200.200.200.1 LP: 8 MED Learned/Used: 8/
8
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+1.1.1.0/24/1/0 +134.112.30.254/32/1/0
NH:200.200.200.1 LP: 9 MED Learned/Used: 7/
7
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+12.12.12.0/24/1/0 +12.12.12.2/32/1/0
NH:200.200.200.1 LP: 16 MED Learned/Used: 0/
0
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+12.12.12.1/32/1/0 +131.108.0.0/24/1/0
134.112.30.0/24/1/0 +194.194.194.0/24/1/0
200.200.200.0/24/1/0 +202.202.202.0/24/1/0
+220.220.220.1/32/1/0 +221.221.221.1/32/1/0
NH:Self-generated LP: 16 MED Learned/Used: 0/
0
Metrics to NH:60/2/1/4 Gateway to NH:134.112.30.1
NLRI:+220.220.220.9/32/4000/0 +200.200.200.0/24/4000/0
+199.199.199.0/24/4000/0 +134.112.30.0/24/4000/0
```

The network layer reachability information (NLRI) in the output shows all routes that are accepted from the peer.

The following procedure shows how to create a policy (called `two_networks`) to permit two network routes (194.194.194.0/24 and 1.1.1.0/24):

#### 1 Create the policy.

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

#### 2 List the policy.

```
admin> list
[in BGP-POLICY/two_networks (new)]
name* = two_networks
next-policy = ""
rule = [""]
```

#### 3 List the rule.

```
admin> list rule
[in BGP-POLICY/two_networks:rule (new)]
rule[1] = ""
rule[2] = ""
rule[3] = ""
rule[4] = ""
rule[5] = ""
rule[6] = ""
rule[7] = ""
rule[8] = ""
rule[9] = ""
rule[10] = ""
rule[11] = ""
rule[12] = ""
rule[13] = ""
```

---

```
rule[14] = ""
rule[15] = ""
rule[16] = ""
rule[17] = ""
rule[18] = ""
rule[19] = ""
rule[20] = ""
```

As the output shows, the policy is created with no rules.

- 4 Apply rules to the policy to permit routes from two networks and set the input multiexit discriminator and save your changes.

```
admin> set 1 = permit if prefix 194.194.194.0/24 then imed 5
admin> set 2 = permit if prefix 1.1.1.0/24 then imed 5
admin> write
BGP-POLICY/two_networks written
```

- 5 List the policy.

```
admin> list
[in BGP-POLICY/two_networks:rule]
rule[1] = "permit if prefix 194.194.194.0/24 then imed 5"
rule[2] = "permit if prefix 1.1.1.0/24 then imed 5"
rule[3] = ""
rule[4] = ""
. . .
```

- 6 Apply the policy as an acceptance policy to peer apx1.

```
apx1-admin> read bgp-peer apx1
BGP-PEER/apx1 read
apx1-admin> list
[in BGP-PEER/apx1]
peer-name* = apx1
enable = yes
peer-ip-address = 200.200.200.1
my-ip-address = 200.200.200.9
autonomous-system = 2
always-next-hop = no
route-reflector-client = no
confederation-member = no
default-gateway-metric = 0
accept-policy = all
inject-policy = all
advertise-policy = all
```

```
admin> set accept-policy = two_networks
admin> write
BGP-PEER/apx1 written
```

- 7 Use the `bgp show peer` command to display information about the peer.

```
admin> bgp show peer
Remote Peer AS Flg DM Up Accept Inject Advertise

apx1 (200.200.200.1) 2 -- Up two_networks all all
```

The `two_networks` policy is listed under the `Accept` column.

- 8 Use the `bgp show path` command to display all the paths in the BGP routing table.

```
admin> bgp show path
```

```
O:IGP
NH:200.200.200.1 LP: 8 MED Learned/Used: 8/ 5
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+1.1.1.0/24/1/0
NH:200.200.200.1 LP: 16 MED Learned/Used: 0/ 5
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+194.194.194.0/24/1/0
```

Note that only the 194.194.194.0/24 and the 1.1.1.0/24 networks are listed in the NLRI fields in the output to the `show peer` command. This is because we set the `two_networks` policy (in Step 4) to accept routes only from those two networks. Also, note that the MED used was set to 5.

## Examples

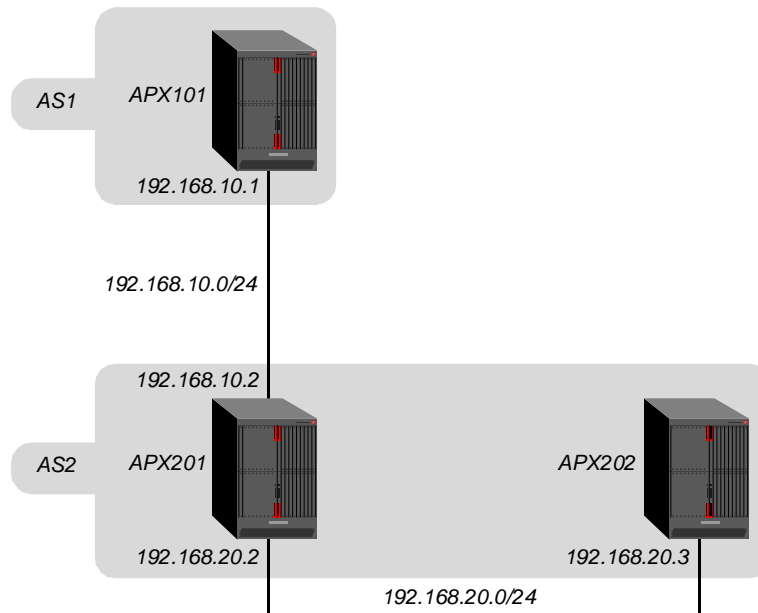
Except for the first example, all samples in this section are designed so that you can mix and match depending on what your objective is, you can combine them.

- “Simple iBGP-to-eBGP configuration” on page 68
- “Default route examples” on page 71
- “Advertise IP address pools to an eBGP peer” on page 77
- “Accepting/injecting BGP routes from an eBGP peer” on page 81
- “Route reflector example” on page 84
- “Confederations example” on page 90

### *Simple iBGP-to-eBGP configuration*

Configure the TAOS unit with an iBGP and eBGP peer. This is not a typical configuration; the objective is to show how to configure a simple iBGP and eBGP peer and accept all routes advertised from the peers.

Figure 2. Simple iBGP-to-eBGP



Assumptions:

- APX101 is in autonomous system 1.
- APX101 has soft IP address 100.1.0.1, APX201 has soft IP address 100.2.0.2, APX202 has soft IP address 100.3.0.3.
- APX201 and APX202 are in autonomous system 2.

Goals:

- Establish external BGP peer relationships between APX101 and APX201.
- Establish internal BGP peer relationships between APX201 and APX202.
- Each TAOS unit will accept and inject all the routes from each peer.

**Note:** It is not recommended to configure a TAOS unit to accept all routes from a peer that is advertising a full Internet routing table.

### APX101 configuration

1 Configure the BGP Global parameters as follows:

```
APX101> new bgp-global
APX101> set enable = yes
APX101> set autonomous-system = 1
APX101> set id = 100.1.0.1
APX101> set static-route-redist-policy = all
APX101> set conn-route-redist-policy = all
APX101> write
```

The `static-route-redistribution-policy` and `connected-routes-redistribution-policy` parameters control redistribution of static and connected routes to BGP. See “Advertise IP address pools to an eBGP peer” on page 77 for an example of the connected routes redistribution policy parameter.

2 Configure the external peer to APX201 as follows:

```
APX101> new bgp-peer
APX101> set peer-name = apx201
APX101> set enable = yes
APX101> set peer-ip-address = 192.168.10.2
APX101> set my-ip-address = 192.168.10.1
APX101> set autonomous-system = 2
APX101> set accept-policy = all
APX101> set inject-policy = all
APX101> set advertise-policy = all
APX101> write
```

### *APX201 configuration*

3 Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> set static-route-redirect-policy = all
APX201> set conn-route-redirect-policy = all
APX201> write
```

4 Configure the external peer to APX101 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = apx101
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set accept-policy = all
APX201> set inject-policy = all
APX201> set advertise-policy = all
APX201> write
```

5 Configure the internal peer to APX202 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = apx202
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.20.3
APX201> set my-ip-address = 192.168.20.2
APX201> set autonomous-system = 2
APX201> set accept-policy = all
APX201> set inject-policy = all
APX201> set advertise-policy = all
APX201> write
```

### *APX202 configuration*

6 Configure the BGP Global parameters as follows:

```
APX202> new bgp-global
APX202> set enable = yes
APX202> set autonomous-system = 2
APX202> set id = 100.3.0.3
APX202> set static-route-redirect-policy = all
APX202> set conn-route-redirect-policy = all
APX202> write
```



7 Configure the internal peer to APX201 as follows:

```
APX202> new bgp-peer
APX202> set peer-name = apx201
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.20.2
APX202> set my-ip-address = 192.168.20.3
APX202> set autonomous-system = 2
APX202> set accept-policy = all
APX202> set inject-policy = all
APX202> set advertise-policy = all
APX202> write
```

8 Verify that the peers are active as follows:

```
APX201> bgp show peer
```

| Remote Peer           | AS | Flg | DM | Up | Accept | Inject | Advertise |
|-----------------------|----|-----|----|----|--------|--------|-----------|
| px101 (192.168.10.1)  | 1  | --  |    | Up | all    | all    | all       |
| apx202 (192.168.20.3) | 2  | --  |    | Up | all    | all    | all       |

9 Display the entries in the BGP routing table as follows to see the routes in the BGP routing table:

```
APX201> bgp show path
```

```
O: IGP
Sequence: 1
NH: 192.168.10.1 LP: not present MED Learned/Used: 0/ 0
Metrics to NH: 0/32/0/3 Gateway to NH: 192.168.10.1
NLRI: +100.1.0.1/32/2/4

O: IGP
NH: 192.168.20.3 LP: 16 MED Learned/Used: 0/ 0
Metrics to NH: 0/32/0/3 Gateway to NH: 192.168.20.3
NLRI: +100.3.0.3/32/1/0
```

10 Display the entries in the routing table as follows:

```
APX201> netstat -rn
```

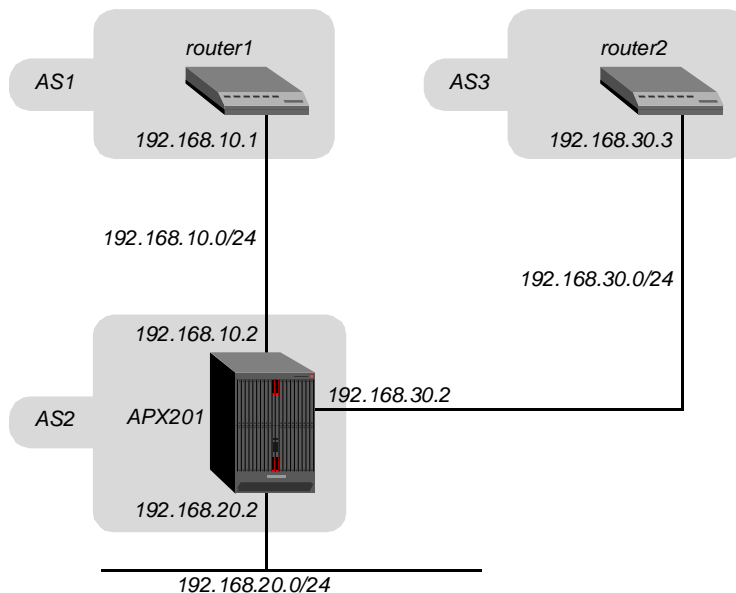
| Destination  | Gateway      | IF      | Flg | Pref | Met | Use | Age |
|--------------|--------------|---------|-----|------|-----|-----|-----|
| 100.1.0.1/32 | 192.168.10.1 | ie1-4-4 | Be  | 5    | 1   | 0   | 470 |
| 100.3.0.3/32 | 192.168.20.3 | ie1-4-2 | Bi  | 180  | 1   | 0   | 194 |

## Default route examples

If the TAOS unit's external BGP (eBGP) peer is to be its default gateway, it can be configured in any of the following ways described in this section:

- “A: Creating a default route using the IP-Route profile” on page 72
- “B: Creating a dynamic BGP default route with the Default-Gateway-Metric parameter” on page 73
- “C: Learning the default route from external BGP peer through eBGP” on page 75

Figure 3. Default route



With examples A and B, the administrator of the TAOS unit has control and can specify the default route. With example C, the default route is learned from the remote eBGP peer, which requires coordination with the administrator of the remote eBGP peer.

If the remote peer is not advertising a default route to itself and you still want to make it the default gateway on your system, example A or example B are better choices.

The difference between A and B becomes clear in the examples.

### *A: Creating a default route using the IP-Route profile*

Assumptions:

- router1 is in autonomous system 1.
- APX201 is in autonomous system 2.
- router2 is in autonomous system 3.

Scenario:

The TAOS unit will have a primary default route to router1.

**Note:** In this example, the default route is not a BGP route. It is not dynamic route, it is a static route. If the link to the gateway is broken, the route remains in the routing table.

### *APX201 configuration*

**1** Read and configure the IP Route profile as follows:

```
APX201> read IP-ROUTE
APX201> set name = default
APX201> set dest-address = 0.0.0.0/0
APX201> set gateway-address = 192.168.10.1
APX201> set metric = 1
```

```
APX201> set private-route = yes
APX201> set active-route = yes
APX201> write -f
```

2 Display the routing table. Note the S flag is set for a static route.

```
APX201> netstat -rn
```

| Destination | Gateway      | IF      | Flg | Pref | Met | Use | Age |
|-------------|--------------|---------|-----|------|-----|-----|-----|
| 0.0.0.0/0   | 192.168.10.1 | ie1-4-4 | SGP | 60   | 1   | 1   | 36  |

Another way to use a static default route is as a backup default route. You can then create your primary default route through the methods explained in “B: Creating a dynamic BGP default route with the Default-Gateway-Metric parameter” on page 73 and “C: Learning the default route from external BGP peer through eBGP” on page 75. You create the backup default route as indicated in the steps above, except that you assign the metric parameter to a higher value than the metric of the primary default route. For example, if your primary default route has a metric of 1, you can set the metric of your backup static default route to 5. Then if the primary default route is removed, the static default route will be used.

```
APX201> new IP-ROUTE
APX201> set name = backup_def_route
APX201> set dest-address = 0.0.0.0/0
APX201> set gateway-address = 192.168.10.1
APX201> set metric = 5
APX201> set private-route = yes
APX201> set active-route = yes
APX201> write -f
```

### *B: Creating a dynamic BGP default route with the Default-Gateway-Metric parameter*

Scenario:

The TAOS unit is configured with two eBGP peers, each in a different autonomous system.

The TAOS unit will have a primary default route through router1 and a backup default route through router2.

In this scenario, both the primary and backup default route will be accomplished with the default-gateway-metric parameter.

Assumptions:

- router1 is in autonomous system 1
- router2 is in autonomous system 3
- apx201 is in autonomous system 2

Goals:

- Establish external BGP peer relationships with router1 and router2
- APX201 will have a primary default gateway to router1 (metric 1) and a backup default gateway to router2 (metric 5)

### APX201 configuration

**1** Configure the BGP Global parameters:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> write
```

**2** Configure the IP Global parameters:

```
APX201> read ip-global
APX201> set ignore-def-route = no
APX201> write
```

**Note:** Setting the `ignore-def-route` parameter to `no` is required when you use the `default-gateway-metric` parameter in a BGP peer profile.

**3** Configure the external peer to router1 and set the `default-gateway-metric` parameter to 1:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set default-gateway-metric = 1 (preferred default route is through router1)
APX201> write
```

Setting the `default-gateway-metric` parameter indicates that a default route to this external peer is created if the peer is up. The value of the `default-gateway-metric` parameter is the metric it uses when injecting this peer as a gateway to the default route. You must assign a value to the default routes of different peers to specify a preferred default gateway.

When multiple peers are configured with the `default-gateway-metric`, the one with the lowest metric is the preferred router for default-route forwarding. Number is a value from 1 to 15. If the metric is set to 0, the default route is not created.

**4** Configure the external peer to router2:

```
APX201> new bgp-peer
APX201> set peer-name = router2
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.30.3
APX201> set my-ip-address = 192.168.30.2
APX201> set autonomous-system = 3
APX201> set default-gateway-metric = 5 (a backup default route)
APX201> write
```

**5** Verify that the peers are up and view the DM field:

```
APX201> bgp show peer
```

| Remote Peer            | AS | Flg | DM | Up | Accept | Inject | Advertise |
|------------------------|----|-----|----|----|--------|--------|-----------|
| -----                  |    |     |    |    |        |        |           |
| router1 (192.168.10.1) | 1  |     |    | 1  | Up     |        |           |
| router2 (192.168.30.3) | 3  |     |    | 5  | Up     |        |           |

The DM column contains the values of the default-gateway-metric specified for each peer.

**6** Display the routing table as follows.

```
APX201> netstat -rn
```

| Destination | Gateway     | IF      | Flg | Pref | Met | Use | Age |
|-------------|-------------|---------|-----|------|-----|-----|-----|
| 0.0.0.0/0   | 92.168.10.1 | ie1-4-4 | Bd  | 5    | 1   | 0   | 31  |

Note that the route with the lowest metric is inserted into the table. The Flg column shows that it is a BGP, dynamic route. If the peer to router1 is disconnected, then the default route for router2 will be inserted into the table and it will become the default route.

The advantage of using the default-gateway-metric parameter over creating a static route (in Example A) is that the default route created with the default-gateway metric is dynamic. If the peer with the default-gateway-metric goes down, then the default route is removed from the table. When you create the default route with the IP-ROUTE profile, the route always exists in the table.

### *C: Learning the default route from external BGP peer through eBGP*

Scenario:

A TAOS unit is configured with two EBGP peers, each in a different autonomous system.

The TAOS unit is configured to have a primary default route through router1 and a backup default route through router2.

Both the primary default route and the backup default route are accomplished through external BGP and a policy that uses a input multiexit discriminator (IMED).

Assumptions:

- router1 is in autonomous system 1 and will advertise a default route to APX201.
- APX201 is in autonomous system 2 and has soft IP address 100.2.0.2.
- router2 is in autonomous system 3 and will advertise a default route to APX201.

Goals:

- Establish external BGP peer relationships between router1 and router2.
- APX201 will receive a default route advertised from router1 and router2.
- Through policies created on APX201, APX201 will configure router1 to be the primary default route by setting the IMED to 1, and will configure router2 as the backup default route by setting the IMED to 4.

### *APX201 configuration*

**1** Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> set ignore-def-route = no
APX201> write
```

**Note:** Setting the `ignore-def-route` parameter to `no` is required when you use the `default-gateway-metric` parameter in a BGP peer profile.

**2** Configure the external peer to router1 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set accept-policy = router1_routes
APX201> set inject-policy = router1_routes
APX201> set advertise-policy =
APX201> set default-gateway-metric =
APX201> write
```

**Note:** If router1 is advertising just a default route and you don't need to set any parameters (like the `IMED`, for example), it is sufficient to set the `accept-policy` parameter to `all`. In this way you avoid the need to create the policy `router1_routes` in Step 4.

**Note:** In this example, APX201 is not advertising any routes to its peer. Refer to "Advertise IP address pools to an eBGP peer" on page 77 for an example of advertising routes to a peer.

**3** Configure the external peer to router2 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router2
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.30.3
APX201> set my-ip-address = 192.168.30.2
APX201> set autonomous-system = 3
APX201> set accept-policy = router2_routes
APX201> set inject-policy = router2_routes
APX201> set advertise-policy =
APX201> set default-gateway-metric =
APX201> write
```

**4** For the primary default route, create the policy `router1_routes`, and set the `input-multi-exit-discriminator` to 1, as follows:

```
APX201> new bgp-policy
APX201> set name = router1_routes
APX201> set rule 1 = "permit if prefix exactly 0.0.0.0/0 then imed 1"
APX201> write -f
```

**Note:** The keyword **exactly** is needed in the rule, in Step 4 and Step 5, for them to match on the default route. If you don't include the keyword **exactly**, that is, if you specify **permit if prefix 0.0.0.0/0**, the rule permits all routes.

**5** For the backup default route, create the policy `router2_routes`, and set the `input-multi-exit-discriminator` to 4, as follows:

```
APX201> new bgp-policy
APX201> set name = router2_routes
APX201> set rule 1 = "permit if prefix exactly 0.0.0.0/0 then imed 4"
APX201> write -f
```

---

## 6 Restart BGP:

```
APX201> bgp restart
or
APX201> bgp restart peer peer_name | peer_ip_address
```

When you make configuration changes to a peer, Lucent recommends that you restart BGP.

## 7 Verify the peers are up as follows:

```
APX201> bgp show peer
```

| Remote Peer            | AS | Flg | DM | Up | Accept       | Inject       | Advertise |
|------------------------|----|-----|----|----|--------------|--------------|-----------|
| router1 (192.168.10.1) | 1  | --  | Up |    | router1_rout | router1_rout |           |
| router2 (192.168.30.3) | 3  | --  | Up |    | router2_rout | router2_rout |           |

Note that the names of the policies are specified in the Accept and Inject columns:

## 8 Display the BGP routing table as follows:

```
APX201> bgp show summary
```

|                                                     |                 |                                  |
|-----------------------------------------------------|-----------------|----------------------------------|
| NH: 192.168.30.3                                    | LP: not present | MED Learned/Used: not present/ 4 |
| Metrics to NH: 0/32/0/3 Gateway to NH: 192.168.30.3 |                 |                                  |
| NLRI: 0.0.0.0/0/2/0                                 |                 |                                  |
| NH: 192.168.10.1                                    | LP: not present | MED Learned/Used: not present/ 1 |
| Metrics to NH: 0/32/0/3 Gateway to NH: 192.168.10.1 |                 |                                  |
| NLRI: +0.0.0.0/0/1/0                                |                 |                                  |

You can see an update received for the default route (NLRI 0.0.0.0/0) from router1 (192.168.10.1) and router2 (192.168.30.3). The IMED specified in the policies is indicated in the MED Used column—4 in this example. There was no MED present on the routes it learned from router1 and router2.

## 9 View the routing table as follows:

```
APX201> netstat -rn
```

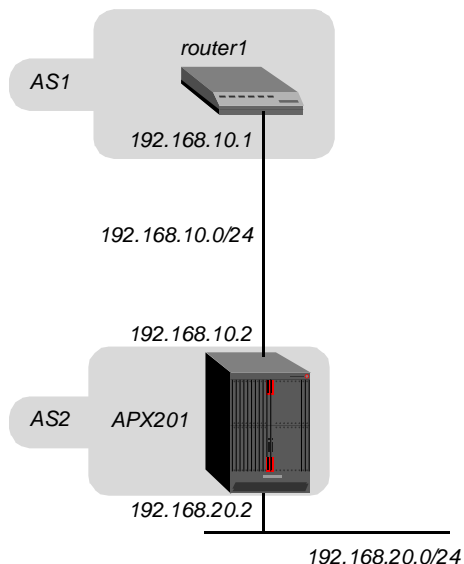
| Destination | Gateway      | IF      | Flg | Pref | Met | Use | Age    |
|-------------|--------------|---------|-----|------|-----|-----|--------|
| 0.0.0.0/0   | 192.168.10.1 | ie1-4-4 | Be  | 5    | 1   | 0   | 521016 |

Note that the route with the lowest metric is inserted into the table. The Flg column shows that it is a external BGP route. If the peer to router1 is disconnected, the default route for router2 will be inserted into the table and it will become the default route after the hold-time parameter setting is met.

## Advertise IP address pools to an eBGP peer

This example shows how to configure a TAOS unit with an eBGP peer, and how to configure the TAOS unit to advertise it's IP address pools.

Figure 4. Advertise IP address pools to eBGP peers



Assumptions:

- router1 is any router in autonomous system 1.
- APX201 is a TAOS unit in autonomous system 2 and has soft IP address 100.2.0.2.

Goals:

- Establish external BGP peer relationships between router1 and APX201.
- APX201 will advertise its IP address pools to router1.

This example uses the following address blocks for the IP pools on APX201:

192.168.77.0/24  
192.168.78.0/24  
192.168.79.0/24  
192.168.80.0/24  
192.168.81.0/24

### *APX201 configuration*

- 1 In the IP-Global profile, configure the IP address pools that will be advertised to router1 as follows:

```
APX201> new IP-global
APX201> set pool-summary = yes
APX201> set pool-base-address 1 = 192.168.77.1
APX201> set pool-base-address 2 = 192.168.78.1
APX201> set pool-base-address 3 = 192.168.79.1
APX201> set pool-base-address 4 = 192.168.80.1
APX201> set pool-base-address 5 = 192.168.81.1
APX201> set assign-count 1 = 254
APX201> set assign-count 2 = 254
APX201> set assign-count 3 = 254
APX201> set assign-count 4 = 254
```



```
APX201> set assign-count 5 = 254
APX201> write -f
```

2 View the IP pools as follows:

```
APX201> netstat -rn
```

| Destination     | Gateway | IF  | Flg | Pref | Met | Use | Age  |
|-----------------|---------|-----|-----|------|-----|-----|------|
| 192.168.77.0/24 | -       | rj0 | C   | 0    | 0   | 0   | 6219 |
| 192.168.78.0/24 | -       | rj0 | C   | 0    | 0   | 0   | 6219 |
| 192.168.79.0/24 | -       | rj0 | C   | 0    | 0   | 0   | 6219 |
| 192.168.80.0/24 | -       | rj0 | C   | 0    | 0   | 0   | 6219 |
| 192.168.81.0/24 | -       | rj0 | C   | 0    | 0   | 0   | 6219 |

**Note:** When the IP pools are created as in Step 1, they are created as connected routes in the IP routing table. The C in the Flg column represents connected routes:

3 Create a BGP policy that will match the IP address pools as follows:

```
APX201> new bgp-policy
PX201> set name = apx201_pools
APX201> set rule 1 = "permit if prefix 192.168.77.0/24"
APX201> set rule 2 = "permit if prefix 192.168.78.0/24"
APX201> set rule 3 = "permit if prefix 192.168.79.0/24"
APX201> set rule 4 = "permit if prefix 192.168.80.0/24"
APX201> set rule 5 = "permit if prefix 192.168.81.0/24"
APX201> write -f
```

4 Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> set conn-route-redirect-policy = apx201_pools
APX201> write
```

When you set the `conn-route-redirect-policy` in the `bgp-global` profile, it causes the TAOS unit to automatically create BGP summarizations for the routes matched in the policy specified.

`conn-route-redirect-policy = policy name | all`

BGP summarizations indicate how routing information from connected and static routes are forwarded to BGP for advertisement to other BGP peers. When you display the routing table with the `netstat -rn` command, connected routes are identified by the C in the Flg column, and static routes are identified by an S in the Flg column. Those summarizations can be advertised if specified (see Step 4). If you want all of the TAOS unit's connected routes to be advertised, you set `conn-route-redirect-policy = all`.

5 Configure the external peer to router1 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set advertise-policy = apx201_pools
APX201> write
```

## Routing features in TAOS 9.1.0

### BGP routing support

The advertise policy must be set to a policy or it must be set to the keyword `all` for the summarizations that are created in Step 4 to be advertised.

**6** Confirm that the peer is up as follows:

```
APX201> bgp show peer
```

| Remote Peer            | AS | Flg | DM | Up | Accept | Inject | Advertise    |
|------------------------|----|-----|----|----|--------|--------|--------------|
| -----                  |    |     |    |    |        |        |              |
| router1 (192.168.10.1) | 1  |     | -- | Up |        |        | apx201_pools |

**7** Display the summarizations automatically created for the IP address pools (as a result of Step 4) as follows:

```
APX201> bgp show summarization
```

|                   |               |                             |                       |
|-------------------|---------------|-----------------------------|-----------------------|
| 192.168.81.0/24/A | The same      | Count of supporting routes: | 0                     |
| LP:               | 16            | MED:                        | 0 CAS: not applicable |
| Export to AS:     | All           |                             |                       |
| Export to CMA:    | All           |                             |                       |
| 192.168.80.0/24/A | The same      | Count of supporting routes: | 0                     |
| LP:               | 16            | MED:                        | 0 CAS: not applicable |
| Export to AS:     | All           |                             |                       |
| Export to CMA:    | All           |                             |                       |
| 192.168.79.0/24/A | The same      | Count of supporting routes: | 0                     |
| LP:               | 16            | MED:                        | 0 CAS: not applicable |
| Export to AS:     | All           |                             |                       |
| Export to CMA:    | All           |                             |                       |
| 192.168.78.0/24/A | The same      | Count of supporting routes: | 0                     |
| LP:               | 16            | MED:                        | 0 CAS: not applicable |
| Export to AS:     | All           |                             |                       |
| Export to CMA:    | All           |                             |                       |
| 192.168.77.0/24/C | Init          | Count of supporting routes: | 0                     |
| LP: none set      | MED: none set | CAS: not set                |                       |
| Export to AS:     | 1             |                             |                       |
| Export to CMA:    |               |                             |                       |

**8** Display the corresponding routes in the BGP routing table as follows:

```
APX201> bgp show path
```

```
NH: Self-generated LP: 16 MED Learned/Used: 0/ 0
Metrics to NH: 60/2/1/4 Gateway to NH: 172.20.3.3
NLRI: +192.168.81.0/24/4000/1 +192.168.80.0/24/4000/1
 +192.168.79.0/24/4000/1 +192.168.78.0/24/4000/1
 +192.168.77.0/24/4000/1
```

- 9 From router1, display the BGP and routing table to confirm that it received the routes that correspond to the APX's IP address pools.

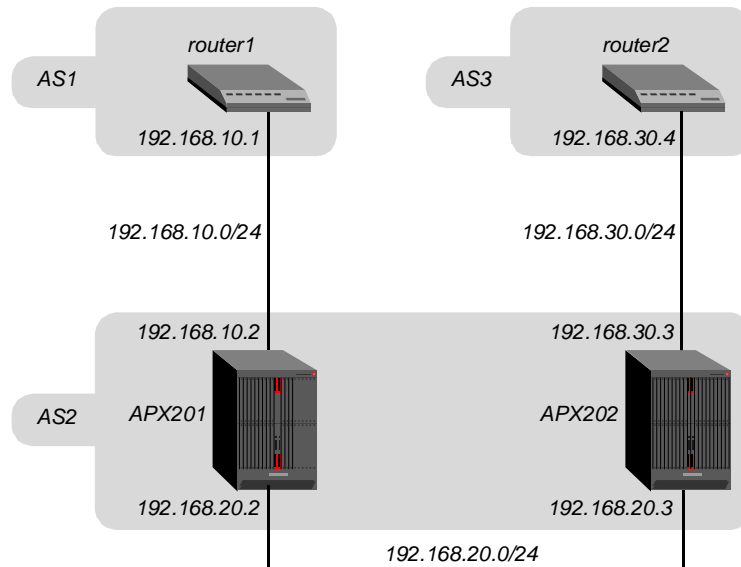
### *Accepting/injecting BGP routes from an eBGP peer*

Configure two TAOS units as IBGP peers, and configure each TAOS unit with an EBGP peer to a different autonomous system.

The TAOS units are configured to accept routes from the upstream ISP's autonomous system.

It is not advisable to accept and inject the full Internet routing table into the TAOS unit. Lucent recommends that you create a policy that accepts and injects only the routes that you need. The following simple example shows how to configure TAOS unit to accept and inject routes from an upstream autonomous system number.

Figure 5. Accepting and injection routes from an upstream ISP



Assumptions:

- router1—an external BGP peer in autonomous system 1—advertises routes to APX201 in AS 2.
- router2—an external BGP peer in autonomous system 3—advertises routes to APX202 in AS 2.
- APX201 and APX202 are internal BGP peers in autonomous system 2.
- APX201 has soft IP address 100.2.0.2.

Goals:

- Establish external BGP peer relationships between router1 and APX201, and between router2 and APX202.
- Create a policy called `isp_routes_as1` that accepts routes in autonomous system 1, and create a policy called `isp_routes_as3` that accepts routes in autonomous system 3.
- Configure APX201 to accept and inject the routes from router1 that match the `isp_routes_as1` policy, and configure APX202 to accept and inject the routes from router2 that match the `isp_routes_as3` policy.

- Establish internal BGP peer relationships between APX201 and APX202.

Refer to “Default route examples” on page 71 for examples of configuring default routes. Refer to “Advertise IP address pools to an eBGP peer” on page 77 for an example of advertising the IP address pools.

### *APX201 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> write
```

- 2 Create a BGP policy, called `isp_routes_as1`, that accepts routes that are in autonomous system 1 as follows:

```
APX201> new bgp-policy
APX201> set name = isp_routes_as1
APX201> set rule 1 = "permit if as-path 1"
APX201> write
```

**Note:** If you plan to combine this example with the default route example C, you must add the rule in example C to this policy. For example:

```
set rule 2 = "permit if prefix exactly 0.0.0.0/0 then imed 1"
```

- 3 Configure the external peer to `router1` as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set accept-policy = isp_routes_as1
APX201> set inject-policy = isp_routes_as1
APX201> set advertise-policy = all
APX201> write
```

**Note:** The `advertise policy` parameter is set to `all` in this example. If you do not want to advertise all the routes, a policy can be created and applied here too. Refer to “Advertise IP address pools to an eBGP peer” on page 77 for an example of advertising the IP address pools.

- 4 Configure the internal peer to APX202 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = apx202
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.20.3
APX201> set my-ip-address = 192.168.20.2
APX201> set autonomous-system = 2
APX201> set accept-policy = all
APX201> set inject-policy = all
APX201> set advertise-policy = all
APX201> write
```

## APX202 configuration

- 1 Configure the BGP Global parameters as follows:

```
APX202> new bgp-global
APX202> set enable = yes
APX202> set autonomous-system = 2
APX202> set id = 100.3.0.3
APX202> write
```

- 2 Create a BGP policy, called `isp_routes_as3`, that will accept routes that are in autonomous system 3 as follows:

```
APX202> new bgp-policy
APX202> set name = isp_routes_as3
APX202> set rule 1 = "permit if as-path 3"
APX202> write
```

**Note:** If you plan to combine this example with the default route example C, you must add the rule in example C to this policy. For example:

```
set rule 2 = "permit if prefix exactly 0.0.0.0/0 then imed 4"
```

- 3 Configure the external peer to router2 as follows:

```
APX202> new bgp-peer
APX202> set peer-name = router2
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.30.4
APX202> set my-ip-address = 192.168.30.3
APX202> set autonomous-system = 3
APX202> set accept-policy = isp_routes_as3
APX202> set inject-policy = isp_routes_as3
APX202> set advertise-policy = all
APX202> write
```

**Note:** The `advertise policy` parameter is set to `all` in this example. If you do not want to advertise all the routes, you can create and apply a policy here, too. Refer to “Advertise IP address pools to an eBGP peer” on page 77 for an example of advertising the IP address pools.

- 4 Configure the internal peer to APX201 as follows:

```
APX202> new bgp-peer
APX202> set peer-name = apx201
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.20.2
APX202> set my-ip-address = 192.168.20.3
APX202> set autonomous-system = 2
APX202> set accept-policy = all
APX202> set inject-policy = all
APX202> set advertise-policy = all
APX202> write
```

To display a list of the routes accepted into the BGP table, enter the `bgp show path` command.

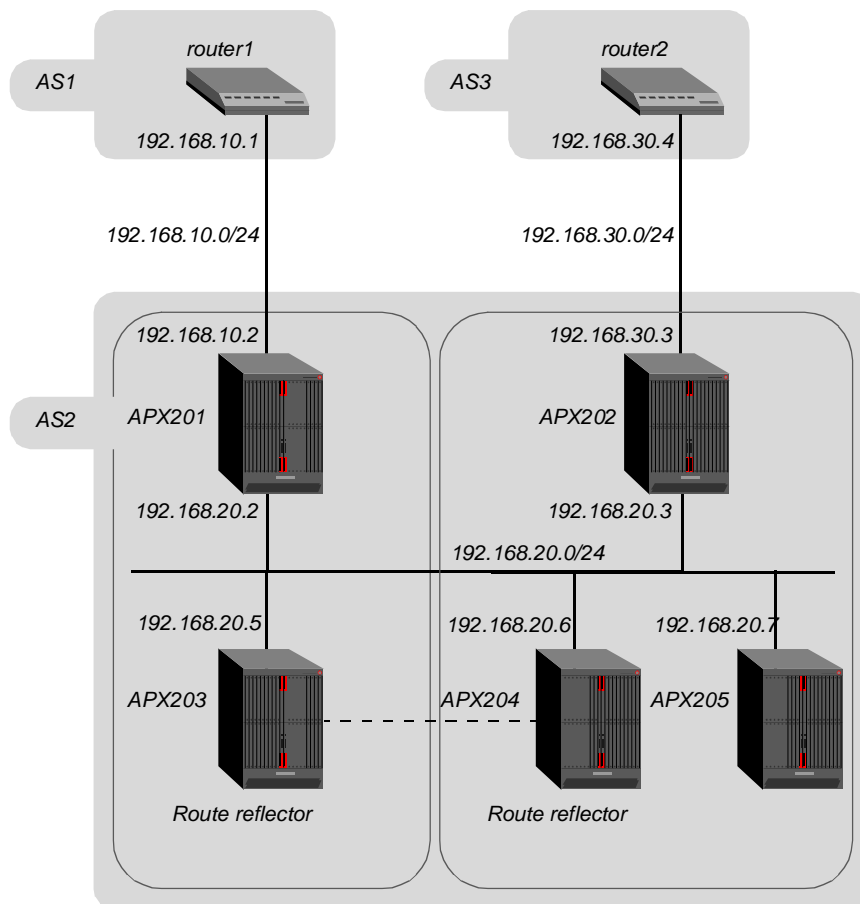
To display a list of the routes injected into the routing table, enter the `netstat -rn` command.

#### Route reflector example

This example shows the parameters needed to configure route reflectors and route reflector clients. For more information about BGP route reflection, refer to RFC 1966, *BGP Route Reflection*.

In Autonomous System 2, APX201 and APX203 form one cluster; APX203 is the route reflector. APX202, APX204, and APX205 form another cluster; APX204 is the route reflector.

Figure 6. Route reflector



Assumptions:

- router1—an external BGP peer in autonomous system 1—advertises routes to APX201 in AS 2.
- router2—an external BGP peer in autonomous system 3—advertises routes to APX202 in AS 2.
- APX201, APX202, APX203, APX204, and APX205 are in Autonomous System 2.
- APX201 and APX203 form a route reflector cluster in which APX203 is the route reflector.
- APX202, APX204, and APX205 form another route reflector cluster in which APX204 is the route reflector.
- APX201 has soft IP address 100.2.0.2, APX202 has soft IP address 100.3.0.3.

Goals:

- Establish external BGP peer relationships between router1 and APX201, and between router2 and APX202.
- Configure APX203 as a route reflector and configure APX201 as a route reflector client.
- Configure APX204 as a route reflector and configure APX202 and APX205 as route reflector clients.
- Establish internal BGP peer relationships between route reflectors APX203 and APX204.

### *APX201 configuration—a route reflector client*

- 1 Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set id = 100.2.0.2
APX201> write
```

- 2 Configure the external peer to router1 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set accept-policy = isp_routes_as1
APX201> set inject-policy = isp_routes_as1
APX201> set advertise-policy = apx201_pools
APX201> write
```

The accept, inject, and advertise policies can be set to policies that reflect what you want to accomplish in your network. Refer to “Accepting/injecting BGP routes from an eBGP peer” on page 81 for the contents of the `isp_routes_as1`, and refer to “Advertise IP address pools to an eBGP peer” on page 77 for the contents of `apx201_pools`.

- 3 Configure the internal peer to APX203, the route reflector in APX201's cluster, as follows:

```
APX201> new bgp-peer
APX201> set peer-name = apx203
APX201> set enable = yes
```

```
APX201> set peer-ip-address = 192.168.20.5
APX201> set my-ip-address = 192.168.20.2
APX201> set autonomous-system = 2
APX201> set accept-policy = all
APX201> set inject-policy = all
APX201> set advertise-policy = all
APX201> write
```

**Note:** On the route reflector client, you do not set any specific route reflector parameter on the peer to the route reflector. This is a normal IBGP configuration.

### *APX203 configuration—a route reflector*

- 1 Configure the BGP Global parameters as follows:

```
APX203> new bgp-global
APX203> set enable = yes
APX203> set autonomous-system = 2
APX203> set id = 100.5.0.5
APX203> set cluster-id = 100.5.0.5
APX203> write
```

- 2 Configure the internal peer to APX201, the route reflector client in its cluster as follows:

```
APX203> new bgp-peer
APX203> set peer-name = apx201
APX203> set enable = yes
APX203> set peer-ip-address = 192.168.20.2
APX203> set my-ip-address = 192.168.20.5
APX203> set autonomous-system = 2
APX203> set accept-policy = all
APX203> set inject-policy = all
APX203> set advertise-policy = all
APX203> set route-reflector-client = yes
APX203> write
```

**Note:** Setting the route-reflector-client parameter to yes in this example automatically configures APX203 as a route reflector and APX201 as a route reflector client.

- 3 Configure the internal peer to APX204, which is the route reflector for the other cluster in AS 2, as follows:

```
APX203> new bgp-peer
APX203> set peer-name = apx204
APX203> set enable = yes
APX203> set peer-ip-address = 192.168.20.6
APX203> set my-ip-address = 192.168.20.5
APX203> set autonomous-system = 2
APX203> set accept-policy = all
APX203> set inject-policy = all
APX203> set advertise-policy = all
APX203> write
```

### *APX202 configuration—a route reflector client*

- 1 Configure the BGP Global parameters as follows:

```
APX202> new bgp-global
APX202> set enable = yes
APX202> set autonomous-system = 2
```

---



```
APX202> set id = 100.3.0.3
APX202> write
```

2 Configure the external peer to router2 as follows:

```
APX202> new bgp-peer
APX202> set peer-name = router2
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.30.4
APX202> set my-ip-address = 192.168.30.3
APX202> set autonomous-system = 3
APX202> set accept-policy = isp_routes_as3
APX202> set inject-policy = isp_routes_as3
APX202> set advertise-policy = apx202_pools
APX202> write
```

The accept, inject, and advertise policies can be set to policies that reflect what you want to accomplish in your network. Refer to “Accepting/injecting BGP routes from an eBGP peer” on page 81 for the contents of the `isp_routes_as3`, and refer to “Advertise IP address pools to an eBGP peer” on page 77 for an example similar to the contents of `apx202_pools`.

3 Configure the internal peer to APX204, the route reflector in APX202’s cluster, as follows:

```
APX202> new bgp-peer
APX202> set peer-name = apx204
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.20.6
APX202> set my-ip-address = 192.168.20.3
APX202> set autonomous-system = 2
APX202> set accept-policy = all
APX202> set inject-policy = all
APX202> set advertise-policy = all
APX202> write
```

**Note:** On the route reflector client, you do not set any specific parameter on the peer to the route reflector. This is a normal IBGP configuration.

### *APX204 configuration—a route reflector*

1 Configure the BGP Global parameters as follows:

```
APX204> new bgp-global
APX204> set enable = yes
APX204> set autonomous-system = 2
APX204> set id = 100.6.0.6
APX204> set cluster-id = 100.6.0.6
APX204> write
```

2 Configure the internal peer to APX202, the route reflector client in its cluster, as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx202
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.3
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 2
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
```

```
APX204> set route-reflector-client = yes
APX204> write
```

**Note:** Setting the `route-reflector-client` parameter to `yes` in this example automatically configures APX204 as a route reflector and APX202 as a route reflector client.

**3** Configure the internal peer to APX203 as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx203
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.5
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 2
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
APX204> write
```

**4** Configure the internal peer to APX205 (the other route reflector client in its cluster) as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx205
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.7
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 2
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
APX204> set route-reflector-client = yes
APX204> write
```

**Note:** Setting the `route-reflector-client` parameter to `yes` in this example automatically configures APX204 as a route reflector and APX205 as a route reflector client.

### *APX205 configuration—a route reflector client*

**1** Configure the BGP Global parameters as follows:

```
APX205> new bgp-global
APX205> set enable = yes
APX205> set autonomous-system = 2
APX205> set id = 100.7.0.7
APX205> write
```

**2** Configure the internal peer to APX204, the route reflector in APX205's cluster, as follows:

```
APX205> new bgp-peer
APX205> set peer-name = apx204
APX205> set enable = yes
APX205> set peer-ip-address = 192.168.20.6
APX205> set my-ip-address = 192.168.20.7
APX205> set autonomous-system = 2
APX205> set accept-policy = all
APX205> set inject-policy = all
APX205> set advertise-policy = all
APX205> write
```

---

**Note:** On the route reflector client, you do not set any specific parameter on the peer to the route reflector. This is a normal IBGP configuration.

### Viewing BGP peer information

To display route reflector information about apx204 peers, enter the following command on the route reflector:

```
APX204> bgp show peer
```

| Remote Peer          | AS | Flg | DM | Up | Accept | Inject | Advertise |
|----------------------|----|-----|----|----|--------|--------|-----------|
| apx203(192.168.20.5) | 2  |     | -- | Up | all    | all    | all       |
| apx202(192.168.20.3) | 2  | R   | -- | Up | all    | all    | all       |
| apx205(192.168.20.7) | 2  | R   | -- | Up | all    | all    | all       |

The R in the Flg column identifies this peer as a route reflector client.

Enter the following command on route reflector client APX205 in this example to display information about the peer:

```
APX205> bgp show peer
```

| Remote Peer           | AS | Flg | DM | Up | Accept | Inject | Advertise |
|-----------------------|----|-----|----|----|--------|--------|-----------|
| apx204 (192.168.20.6) | 2  |     | -- | Up | all    | all    | all       |

Note that there is only one peer, which is a peer to the route reflector, and that no flags are set on the route reflector client.

### Configurations with more than one route reflector in a cluster

If you configure more than one route reflector in a cluster, you must set the `cluster-id` in the BGP Global profile to the same value on each router reflector in the cluster. The `cluster-id` must be unique to a cluster. The BGP Global profile with sample setting is as follows:

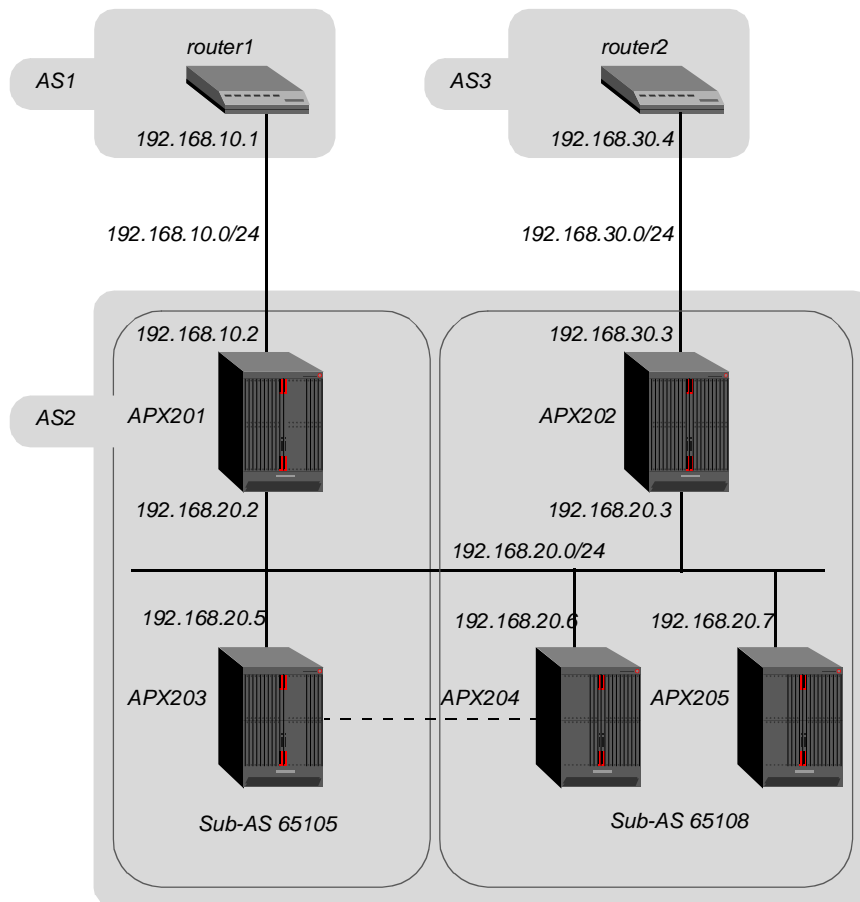
```
[in BGP-GLOBAL]
enable = yes
autonomous-system = 2
id = 100.6.0.6
connect-retry-interval = 120
keepalive-time = 30
hold-time = 90
sub-as = 0
cluster-id = 100.6.0.6
igp-lockstep = no
static-route-redist-policy = all
conn-route-redist-policy = all
```

The `cluster-id` can be any IP address but is typically the BGP id of one of the route reflectors.

### Confederations example

This example shows the parameters needed to configure the TAOS units in AS 2 into sub-autonomous systems (sub-ASs). In autonomous system 2, APX201 and APX203 form one sub-autonomous system. APX202, APX204, and APX205 form another sub-autonomous system.

Figure 7. Confederations



#### Assumptions:

- router1—an external BGP peer in autonomous system 1—advertises routes to APX201 in AS 2.
- router2—an external BGP peer in autonomous system 3—advertises routes to APX202 in AS 2.
- APX201, APX202, APX203, APX204, and APX205 are in AS 2.
- APX201 and APX203 form sub-AS 65105.
- APX202, APX204, and APX205 form sub-AS 65108.
- APX202 has soft IP address 100.3.0.3.

Goals:

- Establish external BGP peer relationships between router1 and APX201 and between router2 and APX202.
- Configure APX201 and APX203 in sub-AS 65105.
- Configure APX202, APX204, and APX205 as fully meshed peers in sub-AS 65108.
- Establish external BGP peer relationships between the sub-ASs with APX203 and APX204.

### *APX201 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX201> new bgp-global
APX201> set enable = yes
APX201> set autonomous-system = 2
APX201> set sub-as = 65105
APX201> set id = 100.2.0.2
APX201> write
```

- 2 Configure the external peer to router1 as follows:

```
APX201> new bgp-peer
APX201> set peer-name = router1
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.10.1
APX201> set my-ip-address = 192.168.10.2
APX201> set autonomous-system = 1
APX201> set accept-policy = isp_routes_as1
APX201> set inject-policy = isp_routes_as1
APX201> set advertise-policy = apx201_pools
APX201> write
```

**Note:** The accept, inject, and advertise policies can be set to policies that reflect what you want to accomplish in your network. Refer to “Accepting/injecting BGP routes from an eBGP peer” on page 81 for the contents of the `isp_routes_as1`, and refer to “Advertise IP address pools to an eBGP peer” on page 77 for the contents of `apx201_pools`.

- 3 Configure the internal peer to APX203, the other internal BGP peer in sub-AS 65105, as follows:

```
APX201> new bgp-peer
APX201> set peer-name = apx203
APX201> set enable = yes
APX201> set peer-ip-address = 192.168.20.5
APX201> set my-ip-address = 192.168.20.2
APX201> set autonomous-system = 65105
APX201> set accept-policy = all
APX201> set inject-policy = all
APX201> set advertise-policy = all
APX201> write
```

### *APX203 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX203> new bgp-global
APX203> set enable = yes
APX203> set autonomous-system = 2
APX203> set sub-as = 65105
APX203> set id = 100.5.0.5
APX203> write
```

- 2 Configure the internal peer to APX201, the other internal BGP peer in sub-AS 65105, as follows:

```
APX203> new bgp-peer
APX203> set peer-name = apx201
APX203> set enable = yes
APX203> set peer-ip-address = 192.168.20.2
APX203> set my-ip-address = 192.168.20.5
APX203> set autonomous-system = 65105
APX203> set accept-policy = all
APX203> set inject-policy = all
APX203> set advertise-policy = all
APX203> write
```

- 3 Configure the peer to APX204, which is an external BGP peer in sub-AS 65108, as follows:

```
APX203> new bgp-peer
APX203> set peer-name = apx204
APX203> set enable = yes
APX203> set peer-ip-address = 192.168.20.6
APX203> set my-ip-address = 192.168.20.5
APX203> set autonomous-system = 65108
APX203> set accept-policy = all
APX203> set inject-policy = all
APX203> set advertise-policy = all
APX203> write
```

### *APX202 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX202> new bgp-global
APX202> set enable = yes
APX202> set autonomous-system = 2
APX202> set id = 100.3.0.3
APX202> set sub-as = 65108
APX202> write
```

- 2 Configure the external peer to router2 as follows:

```
APX202> new bgp-peer
APX202> set peer-name = router2
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.30.4
APX202> set my-ip-address = 192.168.30.3
APX202> set autonomous-system = 3
APX202> set accept-policy = isp_routes_as3
APX202> set inject-policy = isp_routes_as3
APX202> set advertise-policy = apx202_pools
APX202> write
```

---

**Note:** The accept, inject, and advertise policies can be set to policies that reflect what you want to accomplish in your network. Refer to “Accepting/injecting BGP routes from an eBGP peer” on page 81 for the contents of the `isp_routes_as3`, and refer to “Advertise IP address pools to an eBGP peer” on page 77 for an example similar to the contents of `apx202_pools`.

- 3 Configure the internal peer to APX204, an internal BGP peer in sub-AS 65108, as follows:

```
APX202> new bgp-peer
APX202> set peer-name = apx204
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.20.6
APX202> set my-ip-address = 192.168.20.3
APX202> set autonomous-system = 65108
APX202> set accept-policy = all
APX202> set inject-policy = all
APX202> set advertise-policy = all
APX202> write
```

- 4 Configure the internal peer to APX205, the other internal BGP peer in sub-AS 65108, as follows:

```
APX202> new bgp-peer
APX202> set peer-name = apx205
APX202> set enable = yes
APX202> set peer-ip-address = 192.168.20.7
APX202> set my-ip-address = 192.168.20.3
APX202> set autonomous-system = 65108
APX202> set accept-policy = all
APX202> set inject-policy = all
APX202> set advertise-policy = all
APX202> write
```

### *APX204 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX204> new bgp-global
APX204> set enable = yes
APX204> set autonomous-system = 2
APX204> set sub-as = 65108
APX204> set id = 100.6.0.6
APX204> write
```

- 2 Configure the internal peer to APX202, an internal BGP peer in sub-AS 65108, as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx202
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.3
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 65108
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
APX204> write
```

- 3 Configure the internal peer to APX205, an internal BGP peer in sub-AS 65108, as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx205
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.7
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 65108
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
APX204> write
```

- 4 Configure the peer to APX203, which is an external BGP peer in sub-AS 65105, as follows:

```
APX204> new bgp-peer
APX204> set peer-name = apx203
APX204> set enable = yes
APX204> set peer-ip-address = 192.168.20.5
APX204> set my-ip-address = 192.168.20.6
APX204> set autonomous-system = 65105
APX204> set accept-policy = all
APX204> set inject-policy = all
APX204> set advertise-policy = all
APX204> write
```

### *APX205 configuration*

- 1 Configure the BGP Global parameters as follows:

```
APX205> new bgp-global
APX205> set enable = yes
APX205> set autonomous-system = 2
APX205> set sub-as = 65108
APX205> set id = 100.7.0.7
APX205> write
```

- 2 Configure the internal peer to APX204, an internal BGP peer in sub-AS 65108, as follows:

```
APX205> new bgp-peer
APX205> set peer-name = apx204
APX205> set enable = yes
APX205> set peer-ip-address = 192.168.20.6
APX205> set my-ip-address = 192.168.20.7
APX205> set autonomous-system = 65108
APX205> set accept-policy = all
APX205> set inject-policy = all
APX205> set advertise-policy = all
APX205> write
```

- 3 Configure the internal peer to APX202, an internal BGP peer in sub-AS 65108, as follows:

```
APX205> new bgp-peer
APX205> set peer-name = apx202
APX205> set enable = yes
APX205> set peer-ip-address = 192.168.20.3
APX205> set my-ip-address = 192.168.20.7
APX205> set autonomous-system = 65108
APX205> set accept-policy = all
APX205> set inject-policy = all
```



```
APX205> set advertise-policy = all
APX205> write
```

### Viewing BGP peer information

To display confederation information about APX204 peers, enter the following command on APX 204:

```
APX204> bgp show peer
```

| Remote Peer           | AS    | Flg | DM | Up | Accept | Inject | Advertise |
|-----------------------|-------|-----|----|----|--------|--------|-----------|
| apx203 (192.168.20.5) | 65105 | C N | -- | Up | all    | all    | all       |
| apx202 (192.168.20.3) | 65108 | C   | -- | Up | all    | all    | all       |
| apx205 (192.168.20.7) | 65108 | C   | -- | Up | all    | all    | all       |

Note that the C in the Flg column identifies this peer as member of the confederation. The N in the Flg column indicates that any update packets sent from this peer will have a next-hop with APX204's IP address.

Display confederation information on APX202 as follows:

```
APX202> bgp show peer
```

| Remote Peer            | AS    | Flg | DM | Up | Accept | Inject | Advertise |
|------------------------|-------|-----|----|----|--------|--------|-----------|
| apx204 (192.168.20.6)  | 65108 | C   | -- | Up | all    | all    | all       |
| router2 (192.168.30.4) | 3     |     | -- | Up | all    | all    | all       |
| apx205 (192.168.20.7)  | 65108 | C   | -- | Up | all    | all    | all       |

Use the following command on APX202 to display information in the BGP routing table about a path received from router1:

```
APX202> bgp show path 100.1.0.1/32
```

Best match for 100.1.0.1/32 is NLRI 100.1.0.1/32. Details are:

O: IGP

Confederation Set: 65105

Sequence: 1

NH: 192.168.20.5 LP: 100 MED Learned/Used: 0/ 0

Metrics to NH: 0/32/0/3 Gateway to NH: 192.168.20.5

NLRI: +100.1.0.1/32/1/0

## **Support for network routes for multiple customer premises equipment (CPEs)**

TAOS 9.1.0 introduces support for network routes for multiple hosts or customer premises equipment (CPE).

Network routes are an extension of the existing RADIUS dial-out routes. While a dial-out route represents only a single RADIUS profile, a network route can represent multiple RADIUS dial-out profiles.

This feature requires the following nonstandard extensions of the RADIUS server:

- The RADIUS server must be able to process multiple profiles with the same user name.
- The RADIUS server must be able to use the Framed-IP-Address attribute to select the matching profile. Standard RADIUS servers ignore the Framed-IP-Address attribute and only use User-Name attribute as a key.

## **Overview of network routing**

After you restart a MAX TNT unit or issue the `refresh` command, a MAX TNT unit downloads RADIUS dial-out routes from the RADIUS server and adds them to its routing table. Initially, the downloaded dial-out routes are linked to the `wanabe` interface. The `wanabe` interface is an inactive interface. If outbound traffic is destined to a dial-out route, the MAX TNT unit attempts to bring up a new interface by retrieving the associated profile from the RADIUS server. After the TAOS unit has retrieved the Connection profile, it creates a new interface and links the dial-out route to that new interface.

The network routes feature extends the dial-out functionality as follows:

- When the MAX TNT unit requests the profile from the RADIUS server, it adds the `Framed-IP-Address` attribute to the RADIUS request message. This attribute contains the destination IP address of the packet that triggered the route. The RADIUS server uses this additional information to choose the appropriate profile.
- After the MAX TNT unit retrieves the profile from the RADIUS server, it brings up a new interface. However, the original network route that is attached to `wanabe` interface in the routing table is not linked to this new interface—it remains as a `wanabe` interface in the routing table. Instead, the MAX TNT unit adds a new route using the information from the profile provided by the RADIUS server and links this route to the new interface.

**Note:** For a MAX TNT unit to forward packets using a network route, the dial-out profile that is returned by the RADIUS server after a network-route lookup must be a subnet of the network route. For example, if the network route is 10.0.0.0/8, then the dial-out profile must have an IP address that is a subnet, for example, 10.3.0.0/16. However, a RADIUS server can possibly return a dial-out profile that is not a subnet of a network route. For example, for a network route of 10.0.0.0/8, RADIUS might return a Connection profile with a route of 10.0.0.0/4. In such a situation, the MAX TNT unit is unable to forward the IP packets to their final destination.

## Enabling support for network routes

To support network routes for multiple CPEs, TAOS 9.1 adds the `auth-network-route-server` parameter to the `rad-auth-client` subprofile of the `external-auth` profile:

```
[in EXTERNAL-AUTH:rad-auth-client]
auth-network-route-server = yes
```

| Parameter                              | Specifies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>auth-network-route-server</code> | Whether the MAX TNT unit adds the <code>Framed-IP-Address</code> attribute to the RADIUS request message or if the TAOS unit appends the destination IP address to the <code>User-Name</code> for a connection profile lookup. Specify one of the following values: <ul style="list-style-type: none"> <li><code>yes</code> (the default)—The MAX TNT unit adds the <code>Framed-IP-Address</code> attribute to the RADIUS request message. This setting requires a nonstandard RADIUS server that can use the <code>Framed-IP-address</code> attribute to select a valid connection profile from multiple profiles with the same user name.</li> <li><code>no</code>—The MAX TNT unit appends the destination IP address to the <code>User-Name</code> attribute in the RADIUS request message. A standard RADIUS server uses the <code>User-Name</code> attribute and the destination IP address to reply with the appropriate connection profile.</li> </ul> |

### Sample configuration

The following sample settings show the network route feature on the MAX TNT unit. By default, the network route feature is enabled.

```
[in EXTERNAL-AUTH]
auth-type = RADIUS

[in EXTERNAL-AUTH:rad-auth-client]
auth-network-route-server = yes
```

The following sample RADIUS entry configures the network route feature on the RADIUS server:

```
network-route-TNTbox1-1 Password = "ascend", User-Service =Dialout-
Framed-User
 Framed-Route = "10.0.0.0/0 0.0.0.0 1 n CorpA-all-sites"
```

The following are sample user profiles on a RADIUS server that supports multiple profiles with the same user name:

```
CorpA-all-sites Password = "ascend", User-Service = Dialout-Framed-
User,
 Framed-Address = 10.1.*.*
 Ascend-Dial-Number = "1234567890",
 Framed-Protocol = PPP,
 Framed-Address = 10.1.0.1,
 Framed-Netmask = 255.255.0.0,
 Ascend-Send-Auth = Send-Auth-CHAP,
 Ascend-Send-Secret = "TopSecretPassword"

CorpA-all-sites Password = "ascend", User-Service = Dialout-Framed-
User,
```

## Routing features in TAOS 9.1.0

Support for network routes for multiple customer premises equipment (CPEs)

---

```
Framed-Address = 10.2.*.*
Ascend-Dial-Number = "1234123412",
Framed-Protocol = MPP,
Framed-Address = 10.2.0.10,
Framed-Netmask = 255.255.0.0,
Ascend-Send-Auth = Send-Auth-CHAP,
Ascend-Send-Secret = "AnotherPassword"

CorpA-all-sites Password = "ascend", User-Service = Dialout-Framed-
User,
 Framed-Address = 10.3.*.*
 Ascend-Dial-Number = "6789012345",
 Framed-Protocol = PPP,
 Framed-Address = 10.3.0.1,
 Framed-Netmask = 255.255.0.0,
 Ascend-Send-Auth = Send-Auth-CHAP,
 Ascend-Send-Secret = "APassword"

CorpA-all-sites Password = "ascend", User-Service = Dialout-Framed-
User,
 Framed-Address = 10.76.5.*
 Ascend-Dial-Number = "6789012345",
 Framed-Protocol = PPP,
 Framed-Address = 10.76.5.1,
 Framed-Netmask = 255.255.255.0,
 Ascend-Send-Auth = Send-Auth-CHAP,
 Ascend-Send-Secret = "Password"
```

### Setting the network-route preference

To avoid having network route conflicts with newly created routes, set the preference for the network route to a value greater than 120.

For additional information about setting the preference for a route, see the `preference` and `static-pref` parameters in the *APX 8000/MAX TNT Reference*.

## How network routes affect the routing table

Suppose a company CorpA has multiple remote sites, all are subnets of the 10.0.0.0 network:

| Remote Site    | Destination address |
|----------------|---------------------|
| CorpA-site-001 | 10.1.0.0/16         |
| CorpA-site-002 | 10.2.0.0/16         |
| .              | .                   |
| .              | .                   |
| .              | .                   |
| CorpA-site-255 | 10.255.0.0/16       |

To reach each remote site, the RADIUS server must be configured with 255 dial-out routes.

---

admin> **netstat -r:**

| Destination   | Gateway    | IF     | Flg | Pref | Met | Use | Age   |
|---------------|------------|--------|-----|------|-----|-----|-------|
| 10.1.0.0/16   | 10.1.0.1   | wanabe | SG  | 120  | 1   | 0   | 68019 |
| 10.2.0.0/16   | 10.2.0.1   | wanabe | SG  | 120  | 1   | 0   | 68019 |
| .             | .          | .      | .   | .    | .   | .   | .     |
| .             | .          | .      | .   | .    | .   | .   | .     |
| .             | .          | .      | .   | .    | .   | .   | .     |
| 10.255.0.0/16 | 10.255.0.1 | wanabe | SG  | 120  | 1   | 0   | 68019 |

Using the network-route feature, the dial-out routes for all the remote sites for Corp-A are represented by a single dial-out route in the routing table. The plus (+) sign flags a network route in the output of the netstat -r command.

admin> **netstat -r:**

| Destination | Gateway | IF     | Flg | Pref | Met | Use | Age   |
|-------------|---------|--------|-----|------|-----|-----|-------|
| 10.0.0.0/8  | -       | wanabe | SG+ | 121  | 1   | 0   | 68019 |

Suppose that an outbound IP packet with a destination address of 10.3.27.6 reaches the MAX TNT unit. The TAOS unit sends a request to the RADIUS server, with the Framed-IP-Address attribute set to 10.3.27.6. The RADIUS server processes that request and replies with the matching dial-out profile. Note that the original network-route, 10.0.0.0 remains unchanged—it is still associated with the wanabe interface so that any other IP packet destined for the 10.0.0.0/8 network is always represented by an entry in the routing table. The TAOS unit adds a new route for 10.3.27.6, as shown when you issue the netstat -r command:

admin> **netstat -r**

| Destination | Gateway  | IF     | Flg | Pref | Met | Use | Age   |
|-------------|----------|--------|-----|------|-----|-----|-------|
| 10.0.0.0/8  | -        | wanabe | SG+ | 121  | 1   | 0   | 68019 |
| 10.3.0.0/16 | 10.3.0.1 | wan58  | rGT | 60   | 1   | 25  | 890   |

Suppose that the TAOS unit receives an IP packet 10.76.5.2. The netstat -r command now generates the following routing table:

admin> **netstat -r**

| Destination  | Gateway   | IF     | Flg | Pref | Met | Use | Age   |
|--------------|-----------|--------|-----|------|-----|-----|-------|
| 10.0.0.0/8   | -         | wanabe | SG+ | 121  | 1   | 0   | 68519 |
| 10.3.0.0/16  | 10.3.0.1  | wan58  | rGT | 60   | 1   | 77  | 1390  |
| 10.76.5.0/24 | 10.76.5.1 | wan94  | rGT | 60   | 1   | 13  | 240   |

## ***Using pseudogateways with Ascend-Private-Route (104)***

You can now use the RADIUS `Ascend-Private-Route (104)` attribute to create one or more pseudogateways. Using the RADIUS `Ascend-Private-Route` attribute, you can define a route with a pseudogateway. You specify the pseudogateway as an IP address that cannot be reached from any of the MAX TNT unit's configured interfaces. This pseudogateway specification is resolved to the actual gateway's IP address when the unit routes packets to a specified destination. Using pseudogateways requires you to configure a static route on the MAX TNT unit, specifying the destination as the pseudogateway IP address and the gateway as the actual interface IP address through which the packets have to be routed.

The pseudogateway feature primarily targets roaming users who can dial in to any MAX TNT unit to connect to the networks specified by the `Ascend-Private-Route` attribute. By using a pseudogateway, you need only configure a single RADIUS users file for all MAX TNT units.

### **Configuring a pseudogateway**

To configure a pseudogateway, you must perform the following tasks:

- Specify one or more values for `Ascend-Private-Route` in a RADIUS user profile.
- Configure a static route on each of the MAX TNT units that use the pseudogateway feature.

#### ***Specifying values for the Ascend-Private-Route attribute***

In a RADIUS user profile, use the following format to specify one or more values for `Ascend-Private-Route`:

```
Ascend-Private-Route="dest_addr/netmask next_hop/netmask"
```

Replace `dest_addr/netmask` with the destination IP address of the route, and `next_hop/netmask` with the IP address of the pseudogateway.

#### ***Configuring a static route on a MAX TNT unit***

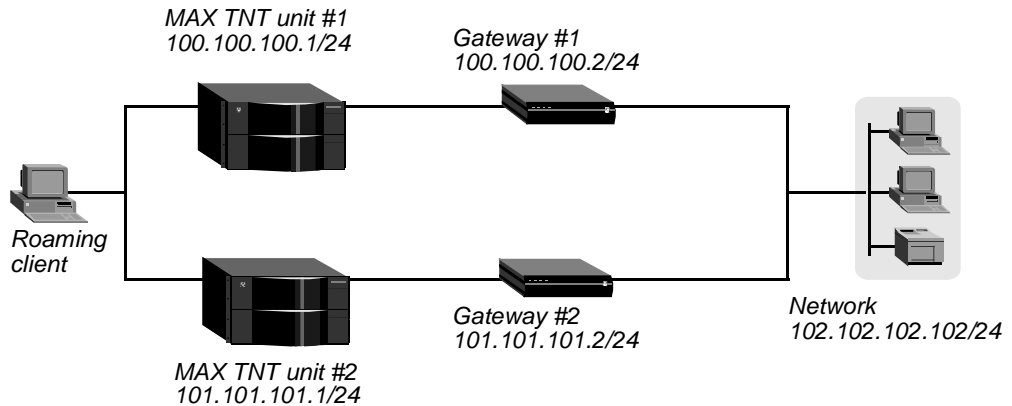
To configure a static route on a MAX TNT unit that uses the pseudogateway feature, proceed as follows:

- 1 Make the working profile an IP-Route profile.
- 2 Set the `Dest-Address` parameter to the IP address of the pseudogateway. Specify any IP address that cannot be reached from any of the MAX TNT unit's interfaces.
- 3 Set the `Gateway-Address` parameter to the IP address of the gateway to the destination.
- 4 Write the profile.

## Sample pseudogateway configuration

In this example, a roaming user can connect to MAX TNT unit #1 at IP address 100.100.100.1/24 or to MAX TNT unit #2 at IP address 101.101.101.1/24. MAX TNT unit #1 can reach the network at IP address 102.102.102.102/24 by means of Gateway #1. MAX TNT unit #2 can reach the same network by means of Gateway #2. Figure 8 illustrates the configuration.

Figure 8. Using a pseudogateway



Assuming that the IP address 10.10.10.10/24 is not reachable by either of the MAX TNT units, you specify the Ascend-Private-Route value in the RADIUS profile in the following way:

```
Ascend-Private-Routes = "102.102.102.102/24 10.10.10.10/24"
```

MAX TNT unit #1 and MAX TNT unit #2 use the common RADIUS profile to authenticate the roaming user and connect him or her to the network at 102.102.102.102/24.

For the static route on MAX TNT unit #1, you set Dest-Address to the pseudogateway's IP address (10.10.10.10/24) and Gateway-Address to the IP address of Gateway #1 (100.100.100.2/24):

```
admin> new ip-route pseudol
IP-ROUTE/pseudol read

admin> list
[in IP-ROUTE/pseudol (new)]
name* = pseudol
dest-address = 0.0.0.0/0
gateway-address = 0.0.0.0
metric = 1
cost = 1
preference = 100
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = yes
active-route = no

admin> set dest-address = 10.10.10.10/24
admin> set gateway-address = 100.100.100.2/24
```

## Tunneling features in TAOS 9.1.0

*L2TP command that displays domain, tunnel, and call statistics*

---

```
admin> write
IP-ROUTE/pseudo1 written
```

Likewise, for the static route on MAX TNT unit #2, you set Dest-Address to the pseudogateway's IP address (10.10.10.10/24) and Gateway-Address to the IP address of Gateway #2 (101.101.101.2/24):

```
admin> new ip-route pseudo2
IP-ROUTE/pseudo2 read
admin> list
[in IP-ROUTE/pseudo2 (new)]
name* = pseudo2
dest-address = 0.0.0.0/0
gateway-address = 0.0.0.0
metric = 1
cost = 1
preference = 100
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = yes
active-route = no
admin> set dest-address = 10.10.10.10/24
admin> set gateway-address = 101.101.101.2/24
admin> write
IP-ROUTE/pseudo2 written
```

On each MAX TNT unit, the pseudogateway address resolves to the IP address specified by the Gateway-Address setting.

## Tunneling features in TAOS 9.1.0

### ***L2TP command that displays domain, tunnel, and call statistics***

This release adds a new TAOS command to display L2TP domain, tunnel and call statistic information on the console. Previously this information was only available from an external SNMP management station.



## Command line changes

The new **l2tp** command may be used to display a variety of different information about the L2TP configuration of the TAOS unit.

| <code>l2tp -[a v d t[srcct] c[isnm]]</code> | Option | Displays                                                                                                                                                                                                                                                |
|---------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a: L2TP administrative status              | a      | L2TP administrative status                                                                                                                                                                                                                              |
| -v: L2TP version information                | v      | L2TP version information                                                                                                                                                                                                                                |
| -d: L2TP domain statistics table            | d      | L2TP domain statistics table                                                                                                                                                                                                                            |
| -t: L2TP tunnel statistics table            | t      | Additional modifiers: <ul style="list-style-type: none"><li>• s:display tunnel states</li><li>• r:display remote information</li><li>• c:display capability information</li><li>• t:display totals/active session</li></ul>                             |
| -c: L2TP call statistics table              | c      | Additional modifiers: <ul style="list-style-type: none"><li>• i: display user name and call serial number</li><li>• s: display call state, connection speed, and capability</li><li>• m: display proxy LCP, auth method, and sequencing state</li></ul> |

## Verifying Peer Host Name In L2TP Authentication

This release introduces RADIUS tunnel accounting support for Layer 2 Forwarding (L2F) in accordance with RFC 2867. It is now possible to verify the peer Host Name during L2TP Tunnel authentication on the tunnel initiator side.

If tunnel authentication is enabled and the Tunnel-Server-Auth-ID RADIUS attribute is present, it is now possible to ensure that the host name of the remote tunnel end point matches the name we expect.

On the tunnel initiator side, the host name AVP from the L2TP Start-Control-Connection-Reply (SCCRP) is compared to the RADIUS Tunnel-Server-Auth-ID attribute if one is present. A mismatch will prevent the tunnel from establishing.

This additional validation can be enabled by a configuration option in the L2-tunnel-global profile. By default, it is turned off to preserve current behavior.

No check is performed on the tunnel server side because the lookup of the tunnel profile (for retrieving the tunnel-password) is keyed with the host name AVP. Therefore, specifying a different Tunnel-Client-Auth-ID value to compare against the host name in the profile does not make much sense.

## Command-line interface changes

The new `verify-remote-host` parameter has been added to the `L2TP-config` subprofile under the `l2-tunnel-global` profile:

```
super> list l2tp-config
[in L2-TUNNEL-GLOBAL:l2tp-config]
first-retry-timer = 1000
retry-count = 6
hello-timer = 60
control-connect-establish-timer = 60
lac-incoming-call-timer = 60
base-udp-port = 0
dialout-auth-lns = no
dialout-send-profile-name = no
verify-remote-host-name = no
```

Using the command line help for the `verify-remote-host-name` parameter:

```
super> set verify-remote-host-name ?
verify-remote-host-name: If Tunnel Authentication is enabled,
also verify the remote peer HostName AVP.
Boolean field, 'no' or 'yes'
```

This parameter controls whether or not to verify the remote peer host name against the corresponding radius attribute, if present. The default value is no.

## External-interface changes

If peer-host name verification fails, a disconnect cause code of `DIS_L2TUNNEL_SERVER_AUTH_FAILED` is reported.

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

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

## Command-Line Interface (CLI) changes

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

- Connection *station* > Tunnel-Options > Primary-Tunnel-Server
- Connection *station* > Tunnel-Options > Secondary-Tunnel-Server
- Tunnel-Server > Server-Endpoint

## RADIUS changes

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

---

---

## RFC 2867 RADIUS tunnel accounting support for L2TP

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

### Command-line interface changes

The new `Acct-Tunnel-Connection-Encoding` parameter has been added to the L2TP-Config subprofile of the L2-Tunnel-Global profile.

#### *Acct-Tunnel-Connection-Encoding*

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

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

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

**Example:** `set acct-tunnel-connection-encoding = decimal-call-serial-number`

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

## **RADIUS changes**

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

| <b>Value</b>            | <b>Indicates</b>                                                                                                                                                                                                                                                                                                                               |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel-Start (9)        | A tunnel has been established.<br><br>The value specified by the <code>user-name</code> attribute indicates the name of the dial-in user that initiated the tunnel, if the name is available. The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Stop (10)        | A tunnel has been deactivated.<br><br>The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                                         |
| Tunnel-Reject (11)      | A tunnel could not be established.<br><br>The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel. The <code>ascend-disconnect-cause</code> and <code>ascend-connect-progress</code> values indicate the reason for the failure.                       |
| Tunnel-Link-Start (12)  | A client connection using the tunnel has been established.<br><br>The value specified by the <code>acct-session-id</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                    |
| Tunnel-Link-Stop (13)   | A client connection using the tunnel has been deactivated.<br><br>The value specified by the <code>acct-session-id</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                    |
| Tunnel-Link-Reject (14) | A client connection using the tunnel could not be established.<br><br>The value specified by the <code>acct-session-id</code> attribute is identical in all link and session accounting records for the tunnel. The <code>ascend-disconnect-cause</code> and <code>ascend-connect-progress</code> values indicate the reason for the failure.  |

---

## RFC 2867 RADIUS tunnel accounting support for L2F

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

### RADIUS changes

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

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

### New Acct-Status-Type values

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

| Value                  | Indicates                                                                                                                                                                                                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel-Start (9)       | A tunnel has been established.<br><br>The value specified by the <code>user-name</code> attribute indicates the name of the dial-in user that initiated the tunnel, if the name is available. The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel. |
| Tunnel-Stop (10)       | A tunnel has been deactivated.<br><br>The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                                         |
| Tunnel-Reject (11)     | A tunnel could not be established.<br><br>The value specified by the <code>acct-tunnel-connection</code> attribute is identical in all link and session accounting records for the tunnel. The <code>ascend-disconnect-cause</code> and <code>ascend-connect-progress</code> values indicate the reason for the failure.                       |
| Tunnel-Link-Start (12) | A client connection using the tunnel has been established.<br><br>The value specified by the <code>acct-session-id</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                    |
| Tunnel-Link-Stop (13)  | A client connection using the tunnel has been deactivated.<br><br>The value specified by the <code>acct-session-id</code> attribute is identical in all link and session accounting records for the tunnel.                                                                                                                                    |

| Value                   | Indicates                                                                                                                                                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel-Link-Reject (14) | A client connection using the tunnel could not be established.<br><br>The value specified by the acct-session-id attribute is identical in all link and session accounting records for the tunnel. The ascend-disconnect-cause and ascend-connect-progress values indicate the reason for the failure. |

### *Sample accounting records for an L2F connection*

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

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

Tue Aug 29 11:42:32 2000
 User-Name = "PIPELINE"
 NAS-IP-Address = 10.6.0.3
 Ascend-Owner-IP-Addr = 0.0.0.0
 Acct-Status-Type = Tunnel-Start
 Acct-Delay-Time = 0
 Acct-Session-Id = "335985247"
```

---

```
Acct-Authentic = Local
Vendor-Specific = vAscend-1c0600000000
Tunnel-Type = L2F : 0
Tunnel-Server-Endpoint = "10.1.1.2" : 0
Tunnel-Client-Auth-ID = "NAS_NAME" : 0
Tunnel-Server-Auth-ID = "HGW_NAME" : 0
Tunnel-ID = "1406ba5f" : 0
Tue Aug 29 11:42:33 2000
User-Name = "PIPELINE"
NAS-IP-Address = 10.6.0.3
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 30
Ascend-NAS-Port-Format = 2
NAS-Port-Type = Sync
Service-Type = Framed
Acct-Status-Type = Tunnel-Link-Start
Acct-Delay-Time = 0
Acct-Session-Id = "335985246"
Acct-Authentic = RADIUS
Vendor-Specific = vAscend-1c0600000000a
Ascend-Modem-PortNo = 19
Ascend-Modem-SlotNo = 8
Ascend-Modem-ShelfNo = 1
Tunnel-Type = L2F : 0
Tunnel-Server-Endpoint = "10.1.1.2" : 0
Tunnel-Client-Auth-ID = "NAS_NAME" : 0
Tunnel-Server-Auth-ID = "HGW_NAME" : 0
Tunnel-ID = "1406ba5f" : 0

Tue Aug 29 11:44:33 2000
User-Name = "PIPELINE"
NAS-IP-Address = 10.6.0.3
Ascend-Owner-IP-Addr = 0.0.0.0
Acct-Status-Type = Tunnel-Stop
Acct-Delay-Time = 0
Acct-Session-Id = "335985247"
Acct-Authentic = Local
Vendor-Specific = vAscend-1c0600000000
```

---

## Tunneling features in TAOS 9.1.0

### *RFC 2867 RADIUS tunnel accounting support for L2F*

---

```
Tunnel-Type = L2F : 0
Tunnel-Server-Endpoint = "10.1.1.2" : 0
Tunnel-Client-Auth-ID = "NAS_NAME" : 0
Tunnel-Server-Auth-ID = "HGW_NAME" : 0
Tunnel-ID = "1406ba5f" : 0
Ascend-Disconnect-Cause = 736
Ascend-Connect-Progress = 244
```

Tue Aug 29 11:44:33 2000

```
User-Name = "PIPELINE"
NAS-IP-Address = 10.6.0.3
Ascend-Owner-IP-Addr = 0.0.0.0
NAS-Port = 30
Ascend-NAS-Port-Format = 2
NAS-Port-Type = Sync
Service-Type = Framed
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "335985246"
Acct-Authentic = RADIUS
Vendor-Specific = vAscend-1c060000000a
Acct-Session-Time = 121
Acct-Input-Octets = 203
Acct-Output-Octets = 176
Acct-Input-Packets = 5
Acct-Output-Packets = 6
Ascend-Disconnect-Cause = 100
Ascend-Connect-Progress = 244
Ascend-Xmit-Rate = 64000
Ascend-Data-Rate = 64000
Ascend-PreSession-Time = 1
Ascend-Pre-Input-Octets = 100
Ascend-Pre-Output-Octets = 122
Ascend-Pre-Input-Packets = 4
Ascend-Pre-Output-Packets = 4
Ascend-Modem-PortNo = 19
Ascend-Modem-SlotNo = 8
Ascend-Modem-ShelfNo = 1
```

---



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

## Command-line changes

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

```
admin> l2f accounting
```

# Management agent features in TAOS 9.1.0

## ***SNMP: Flash MIB supported***

The `flash` MIB provides an interface to various aspects of the system configuration and the images stored on the internal and external flash cards.

This release includes the following enhancements:

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

## Changes to MIB objects

The following objects have been changed in the `flash` MIB:

| Object                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>flashDeviceWriteProtect</code> | Enables write-protect detection of active PCMCIA devices in the <code>flashDeviceTable</code> . If the value of the object is <code>true</code> , the write protection of the flash card is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>flashDeviceType</code>         | Identifies the type of flash card in use.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>flashFileAttributes</code>     | <p>Renamed from <code>flashFileAccess</code>, which always returned <code>read_write(2)</code>, to more accurately refer to a file attribute object like those used on file systems. The new implementation provides special file attribute values that indicate, for example, that the entry is a directory. This information was not available in the previous implementation. The values are returned in a bitmask and can be one of the following:</p> <p><code>readOnly(1)</code>—Indicates a read-only file entry.</p> <p><code>hidden(2)</code>—Indicates a file marked as hidden.</p> <p><code>system(4)</code>—Indicates a system file.</p> <p><code>volumeLabel(8)</code>—Indicates the volume label.</p> <p><code>subDirectory(16)</code>—Indicates a subdirectory.</p> <p><code>archived(32)</code>—Indicates that the file has been archived.</p> <p>A normal file has an attribute value of 0 (zero).</p> |

---

| Object                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flashFileLoadName      | Identifies the TAOS load name of the file listed in the entry. The FAT file system can have multiple loads and versions of the system software stored on the flash card. For this reason, the filename of a particular load might not reflect the version and load name information for a particular file. Because the information is stored in the file itself, retrieving the information is rather costly and might take several seconds. |
| flashOperationStatus   | Provides operational status and additional error codes for all types of flash operations and all TFTP operation errors. Almost all possible error conditions can be uniquely identified by this code. For new operations, active codes enable you to follow the progress of the current operation.                                                                                                                                           |
| fileTable<br>cardTable | Provides additional details about the files and cards present in the system.                                                                                                                                                                                                                                                                                                                                                                 |

## Added MIB objects

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

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

## New MIB group

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

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

## New commands

The `flashOperationCommand` object includes the following new commands:

| Command                                 | Description                                                                                                                                                                                                                        |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>format-card-fat(6)</code>         | Specify FAT format.                                                                                                                                                                                                                |
| <code>format-card-fat-no-mbr(7)</code>  | Specify FAT format without Master Boot Record (MBR). This command is valid only for an ATA flash memory device.                                                                                                                    |
| <code>format-card-fat-boot(8)</code>    | Specify FAT format with boot section.                                                                                                                                                                                              |
| <code>format-card-erase(9)</code>       | Erase card without formatting.                                                                                                                                                                                                     |
| <code>format-card-erase-boot(10)</code> | Erase boot region only.                                                                                                                                                                                                            |
| <code>move-file(11)</code>              | Move file on flash card. This command requires the source ( <code>flashOperationSrcFileName</code> ) and destination ( <code>flashOperationDestFileName</code> ) to be set.                                                        |
| <code>remove-file(12)</code>            | Remove file from flash card. This command requires the source ( <code>flashOperationSrcFileName</code> ) to be specified.                                                                                                          |
| <code>make-directory(13)</code>         | Create directory on flash card. This command requires the source ( <code>flashOperationSrcFileName</code> ) to be specified.                                                                                                       |
| <code>reset-attributes(15)</code>       | Reset <code>flashOperationGroup</code> to its defaults.                                                                                                                                                                            |
| <code>tftp-download(16)</code>          | Download file from flash card. This command requires the host ( <code>flashOperationHost</code> ), source ( <code>flashOperationSrcFileName</code> ), and destination ( <code>flashOperationDestFileName</code> ) to be specified. |
| <code>restore-config(17)</code>         | Restore saved configuration from internal flash memory or a PCMCIA flashcard.                                                                                                                                                      |
| <code>backup-config(18)</code>          | Locally save current configuration.                                                                                                                                                                                                |
| <code>load-mate (19)</code>             | Transfer files to a peer controller in a dual-controller system.                                                                                                                                                                   |

## SNMP: Support for virtual routers (VRouters)

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

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

### Using context names

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

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

Consider the following:

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

### Interface changes

Following are the SNMP changes made for VRouter support:

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

## ***SNMP: View-based access control implementation***

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

### **Overview**

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

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

### **Command-line interface configuration**

You configure VACM at the command-line interface by carrying out the following steps:

- 1 Enable VACM by setting Enable-VACM to Yes in the SNMP profile.
- 2 Map a security name and security model in an incoming or outgoing message to a security group by setting the parameters in the VACM-Security-Group profile.
- 3 Specify view names for different kinds of access (read, write, notify) by setting parameters in the VACM-Access profile. A view specifies whether a given OID is accessible.
- 4 Define views by setting parameters in the VACM-View-Tree profile.

### ***Enabling VACM***

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

The default value of No disables VACM, allowing access to all objects in the system. However, security based on SNMPv1 community strings and the SNMP version 3 user-based security model (SNMPv3 USM) is still used to determine access.

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

To map a security name and security model to a security group, you must set parameters in the VACM-Security-Group profile. Following is a listing of the profile's default values:

```
admin> list vacm-security-group { v1 "" }
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""

admin> list security-properties
[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new) (changed)]
security-model = v1
security-name = ""
```

To map a security name and security model to a security group, set the following parameters:

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

For example, to specify SNMPv3 USM for a USM user called joe and a group called groupNY, enter the following commands:

```
admin> new vacm-security-group
VACM-SECURITY-GROUP/{ v1 "" } read

admin> list
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""

admin> set active = yes

admin> set group-name = groupNY

admin> list security-properties
[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new) (changed)]
security-model = v1
security-name = ""

admin> set security-model = v3-usm

admin> set security-name = joe
(New index value; will save as new profile VACM-SECURITY-GROUP/{ v3-
usm joe }.)

admin> write
VACM-SECURITY-GROUP/{ v3-usm joe } written
```

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

To map a group name, context prefix, context name, security model, and security level to a view name, you must set parameters in the VACM-Access profile. Following is a listing of the profile's default values:

```
admin> list vacm-access {"" "" v1 none }
[in VACM-ACCESS/{"" "" v1 none }]
access-properties* = { {"" "" v1 none } }
active = no
match-method = exact-match
read-view-name = ""
write-view-name = ""
notify-view-name = FullView

admin> list access-properties
group-name = ""
context-prefix = ""
security-model = v1
security-level = none
```

To specify view names for different types of access, set the following parameters:

| Parameter        | Description                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active           | Enables or disables the view. Specify Yes to enable the view or No to disable it. The default is No.                                                                                                            |
| Group-Name       | Specifies a group name. The default is null.                                                                                                                                                                    |
| Context-Prefix   | Specifies a prefix for a given context. The default is null. The Match-Method value determines whether the context name is matched exactly or the prefix alone is matched.                                      |
| Security-Model   | Specifies the security model in use. V1 (the default) specifies the SNMPv1 security model. V3-USM specifies SNMPv3 USM. For VACM support, specify V3-USM.                                                       |
| Security-Level   | Specifies the security level. None (the default) specifies that there is no authentication and no privacy. Auth-Priv specifies authentication and privacy. Auth-Nopriv specifies authentication and no privacy. |
| Match-Method     | Specifies the context-match method. Exact-Match (the default) specifies that the entire context name must be matched. Prefix-Match specifies that only the prefix specified by Context-Prefix must be matched.  |
| Read-View-Name   | Specifies the name of the view for read access. The default is null.                                                                                                                                            |
| Write-View-Name  | Specifies the name of the view for write access. The default is null.                                                                                                                                           |
| Notify-View-Name | Specifies the name of the view for notify access. The default is null.                                                                                                                                          |

For example, to specify a view for read access for a group called `groupSF` with SNMPv3 USM, authentication, and privacy enabled, enter the following commands:

```
admin> new vacm-access
VACM-ACCESS/{ "" "" v1 no+ } read

admin> list
[in VACM-ACCESS/{ "" "" v1 no+ } (new)]
```



```
access-properties* = { "" "" v1 no+ }
active = no
match-method = exact-match
read-view-name = ""
write-view-name = ""
notify-view-name = ""

admin> set active = yes
admin> set read-view-name = view1
admin> list access-properties
[in VACM-ACCESS/{ "" "" v1 no+ }:access-properties (new) (changed)]
group-name = ""
context-prefix = ""
security-model = v1
security-level = none

admin> set group-name = groupSF
admin> set security-model = v3-usm
admin> set security-level = auth-priv
admin> write
VACM-ACCESS/{ groupSF "" v3-usm auth-priv } written
```

## Defining views

To define a view, you must set parameters in the VACM-View-Tree profile. Following is a listing of the profile's default values:

```
admin> list vacm-view-tree { "" 0.0.0.0 }
[in VACM-VIEW-TREE/{ "" "" }]
tree-properties* = { "" "" }
active = no
tree-mask = ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff
tree-type = included

admin> list tree-properties
view-name = ""
view-tree-oid = ""
```

To define a view, set the following parameters:

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

For example, to define a view called `view1` with an OID of 1.3.6.1.4.1.529, enter the following commands:

```
admin> new vacm-view-tree
VACM-VIEW-TREE/{ "" "" } read

admin> list
[in VACM-VIEW-TREE/{ "" "" } (new)]
tree-properties* = { "" "" }
active = no
tree-oid-mask = ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff
tree-type = included

admin> set active = yes

admin> list tree-properties
[in VACM-VIEW-TREE/{ "" "" }:tree-properties (new) (changed)]
view-name = ""
view-tree-oid = ""

admin> set view-name = view1

admin> set view-tree-oid = 1.3.6.1.4.1.529
(New index value; will save as new profile VACM-VIEW-TREE/{
view1 1.3.6.1.4.1.529 }.)

admin> write
VACM-VIEW-TREE/{ view1 1.3.6.1.4.1.529 } written
```

## MIB definitions

To configure VACM via SNMP, proceed as follows:

- 1 Map USM user names to security groups by setting the parameters in the MIB table `VacmSecurityToGroupTable`.
- 2 Specify view names for different kinds of access (read, write, notify) by setting parameters in the MIB table `VacmAccessTable`.
- 3 Define views by setting parameters in the MIB table `VacmViewTreeFamilyTable`.

Following is the new MIB definition:

```
SNMP-VIEW-BASED-ACM-MIB
snmpVacmMIB MODULE-IDENTITY
 DESCRIPTION "The management information definitions for the
 View-based Access Control Model for SNMP."
 OID :1.3.6.1.6.3.16.1
 x vacmContextTable (OID: 1.3.6.1.6.3.16.1.1)
 DESCRIPTION
 This table provides information to SNMP Command
 Generator applications so that they can properly
 configure the vacmAccessTable to control access to
```

```
all contexts at the SNMP entity.

INDEX
{
 vacmContextName
}

CONTAINS
{
 vacmContextName
}

x vacmSecurityToGroupTable (OID: 1.3.6.1.6.3.16.1.2)

DESCRIPTION
 This table maps a combination of securityModel and
 securityName into a groupName which is used to define
 an access control policy for a group of principals.

INDEX
{
 vacmSecurityModel,
 vacmSecurityName
}

CONTAINS
{
 vacmSecurityModel,
 vacmSecurityName,
 vacmGroupName ,
 vacmSecurityToGroupStorageType,
 vacmSecurityToGroupStatus
}

x vacmAccessTable (OID: 1.3.6.1.6.3.16.1.3)

DESCRIPTION
 The table of access rights for groups.
 Each entry is indexed by a groupName, a contextPrefix,
 a securityModel and a securityLevel. To determine
 whether access is allowed, one entry from this table
 needs to be selected and the proper viewName from that
 entry must be used for access control checking.

INDEX
{
 vacmGroupName,
 vacmAccessContextPrefix,
 vacmAccessSecurityModel,
```

---

```
 vacmAccessSecurityLevel
 }
CONTAINS
 {
 vacmAccessContextPrefix,
 vacmAccessSecurityModel,
 vacmAccessSecurityLevel,
 vacmAccessContextMatch,
 vacmAccessReadViewName,
 vacmAccessWriteViewName,
 vacmAccessNotifyViewName,
 vacmAccessStorageType,
 vacmAccessStatus
 }
x vacmMIBViews (OID: 1.3.6.1.6.3.16.1.4)
(Contains a vacmViewSpinLock and vacmViewTreeFamilyTable)
DESCRIPTION
 Locally held information about families of subtrees
 within MIB views.
 Each MIB view is defined by two sets of view subtrees:
 - the included view subtrees, and
 - the excluded view subtrees.
 Every such view subtree, both the included and the
 excluded ones, is defined in this table.
INDEX
 {
 vacmViewTreeFamilyViewName,
 vacmViewTreeFamilySubtree
 }
CONTAINS
 {
 vacmViewTreeFamilyViewName,
 vacmViewTreeFamilySubtree,
 vacmViewTreeFamilyMask,
 vacmViewTreeFamilyType,
 vacmViewTreeFamilyStorageType,
 vacmViewTreeFamilyStatus
 }
```

---

## ***SNMP: Support for displaying and modifying profiles***

You can now display and modify the contents of all profiles by means of SNMP MIBs.

Following are the new MIBs that contain profile information:

- mibalarm.mib
- mibansplan.mib
- mibataalk.mib
- mibatmaddralias.mib
- mibatmatom.mib
- mibatmif.mib
- mibatmnbase.mib
- mibatmp.mib
- mibatmpnni.mib
- mibatmport.mib
- mibatmsig.mib
- mibatmspvc.mib
- mibatmsvcroute.mib
- mibb52test.mib
- mibbgp.mib
- mibbill.mib
- mibbrint.mib
- mibbrite.mib
- mibcallsw.mib
- mibcltm.mib
- mibcltmaccess.mib
- mibcltmrslt.mib
- mibcons.mib
- mibcrap.mib
- mibdba.mib
- mibdebug.mib
- mibdest.mib
- mibdialmod.mib
- mibdslthresh.mib
- mibether.mib
- mibfiltr.mib
- mibfwall.mib
- mibglitenet.mib
- mibintegrity.mib
- mibip.mib
- mibipfax.mib

## Management agent features in TAOS 9.1.0

*SNMP: Support for displaying and modifying profiles*

---

- mibipsec.mib
- mibipx.mib
- mibipxfl.mib
- mibipxrt.mib
- mibl2tunnel.mib
- mibloadselect.mib
- miblog.mib
- mibmaxpots.mib
- mibnat.mib
- mibnumplan.mib
- mibospfinr.mib
- mibospfnbma.mib
- mibospfvlnk.mib
- mibperdnis.mib
- mibplan.mib
- mibport1.mib
- mibprroute.mib
- mibroute.mib
- mibs56.mib
- mibscrty.mib
- mibshash.mib
- mibslot.mib
- mibsnmp.mib
- mibss7nmi.mib
- mibstack.mib
- mibstmnet.mib
- mibswannet.mib
- mibsys1.mib
- mibt1net.mib
- mibtacl.mib
- mibthermal.mib
- mibtime.mib
- mibtransaction.mib
- mibtrap.mib
- mibts.mib
- mibuser.mib
- mibvacm.mib
- mibvoip.mib
- mibvrtr.mib
- mibx25.mib

- `mibxauth.mib`

## ***SNMP: Sending coldstart traps over a slot-card interface***

In this release, a MAX TNT unit can now send coldstart traps over a slot card interface. Previously, these traps could be sent over the shelf controller only.

The `ascend.trp` file has been modified. Following is the new trap definition:

```
ascendColdStart TRAP-TYPE
 ENTERPRISE ascend
 VARIABLES { sysAbsoluteCurrentTime }
 DESCRIPTION "This enterprise trap is generated along with
 RFC1215 coldStart trap,
 this may contain additional variables."

 ::= 48
```

## ***SNMP: Link-status trap enhancements***

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

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

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

## **Command-line interface changes**

The Trap profile contains the following new parameters:

- `Ascend-Link-Down-Trap-Enabled`
- `Ascend-Link-Up-Trap-Enabled`

### ***Ascend-Link-Down-Trap-Enabled parameter***

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

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

- **Yes** (the default) specifies that the MAX TNT unit generates an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the SNMP manager.

- No specifies that the MAX TNT unit does not generate an ascendLinkDown trap when a failure occurs in a communication link between the unit and the SNMP manager.

**Example:** `set ascend-link-down-trap-enabled = no`

**Dependencies:** You can set Ascend-Link-Down-Trap-Enabled to Yes only if LinkDown-Enabled is set to Yes.

**Location:** Trap *host-name*

### *Ascend-Link-Up-Trap-Enabled parameter*

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

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

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

**Example:** `set ascend-link-up-trap-enabled = no`

**Dependencies:** You can set Ascend-Link-Up-Trap-Enabled to Yes only if LinkUp-Enabled is set to Yes.

**Location:** Trap *host-name*

## SNMP changes

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

```
ascendVrouterName OBJECT-TYPE
 SYNTAX DisplayString
 MAX-ACCESS not-accessible
 STATUS mandatory
 DESCRIPTION
 "The Name of the vrouter. The Empty string is the global vrouter."
```

Two new traps have been added to ascend.mib:

```
ascendLinkDown TRAP-TYPE
 ENTERPRISE ascend
 VARIABLES { ifIndex, ifAdminStatus, ifOperStatus, ifType,
 ifName, slotIfSlotIndex, slotIfItemIndex,
 ascendVrouterName }
 DESCRIPTION "This trap is in addition to the generic
 linkDown trap defined in RFC1215. This trap
 provides additional information such as
 ifOperStatus, ifName, slotIfSlotIndex,
```

---



```
slotIfItemIndex. This is an Alarm class
trap and it can be enabled/disabled via
alarmEnabled and/or ascendLinkDownTrapEnabled
in trap profile."

::= 50

ascendLinkUp TRAP-TYPE
 ENTERPRISE ascend
 VARIABLES { ifIndex, ifAdminStatus, ifOperStatus, ifType,
 ifName, slotIfSlotIndex, slotIfItemIndex,
 ascendVrouterName }
```

## SNMP: DOT3 MIB implemented

This release implements the DOT3 MIB for MAX TNT units. Formerly, only the MAX platform supported the DOT3 MIB.

### New objects

Following are the DOT3 statistics that are collected for MAX TNT units, along with their associated objects:

| Data                         | MIB object                         |
|------------------------------|------------------------------------|
| Single Collision Frames      | dot3StatsSingleCollisionFrames     |
| Multiple Collision Frames    | dot3StatsMultipleCollisionFrames   |
| Alignment Errors             | dot3StatsAlignmentErrors           |
| FCS Errors                   | dot3StatsFCSErrors                 |
| Deferred Transmissions       | dot3StatsDeferredTransmissions     |
| Late Collisions              | dot3StatsLateCollisions            |
| Excessive Collisions         | dot3StatsExcessiveCollisions       |
| Internal MAC Transmit Errors | dot3StatsInternalMacTransmitErrors |
| Internal MAC Receive Errors  | dot3StatsInternalMacReceiveErrors  |
| Carrier Sense Errors         | dot3StatsCarrierSenseErrors        |
| Frame Too Long Errors        | dot3StatsFrameTooLongs             |

This implementation collects statistics from Ethernet interfaces, including those on slot cards as well as those on the shelf controller, and records them in the DOT3 MIB on the shelf controller. Some DOT3 statistics are not available on some slot cards. Unavailable statistics

are reported as 0 (zero). The DOT3 statistics supported on Ethernet-2 and Ethernet-3 slot cards are:

| Slot card  | Supported statistics                                                                                                                                                                                                                                                       |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ethernet-2 | 10 Base T interfaces (PCNET Chip)—Single Collision Frames, FCS Errors, Late Collisions, Carrier Sense Errors<br><br>100 Base T interfaces (Feast Chip)—Single Collision Frames, FCS Errors, Late Collisions, Carrier Sense Errors, Alignment Errors, Frame Too Long Errors |
| Ethernet-3 | FCS Errors                                                                                                                                                                                                                                                                 |

## ***Maximum number of SNMP host entries increased***

In the SNMP profile, up to 10 IP addresses of SNMP managers that have read permission and up to 10 IP address of SNMP managers that have write permission are available. Formerly, the limit was eight IP addresses for each type of permission.

**Note:** Be aware that these parameters are deprecated. Although they might appear under certain circumstances, they should not be used. To assign read-only and/or read-write access to SNMP hosts, you must set parameters in the new `SNMP-Manager` profile. For information on this new profile, see “SNMP: Enhancements provide SNMPv3 support and remove host list limitation” on page 128.

On a MAX TNT unit, the `Read-Access-Hosts` parameter in the SNMP profile now consists of an array of 10 IP addresses. Following is a listing of the array:

```
admin> list read-access-hosts
[in SNMP:read-access-hosts]
read-access-hosts[1] = 0.0.0.0
read-access-hosts[2] = 0.0.0.0
read-access-hosts[3] = 0.0.0.0
read-access-hosts[4] = 0.0.0.0
read-access-hosts[5] = 0.0.0.0
read-access-hosts[6] = 0.0.0.0
read-access-hosts[7] = 0.0.0.0
read-access-hosts[8] = 0.0.0.0
read-access-hosts[9] = 0.0.0.0
read-access-hosts[10] = 0.0.0.0
```

Likewise, the `Write-Access-Hosts` parameter in the SNMP profile now consists of an array of 10 IP addresses. Following is a listing of the array:

```
admin> list write-access-hosts
[in SNMP:write-access-hosts]
write-access-hosts[1] = 0.0.0.0
write-access-hosts[2] = 0.0.0.0
write-access-hosts[3] = 0.0.0.0
write-access-hosts[4] = 0.0.0.0
write-access-hosts[5] = 0.0.0.0
write-access-hosts[6] = 0.0.0.0
write-access-hosts[7] = 0.0.0.0
```

```
write-access-hosts[8] = 0.0.0.0
write-access-hosts[9] = 0.0.0.0
write-access-hosts[10] = 0.0.0.0
```

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

In this release, you can specify read and write access for managers that use either SNMPv1 or SNMPv3. In previous releases, you could specify read and write access for up to 10 SNMPv1 managers. Now, when you use the command-line interface, you can specify read and write access for an unlimited number of managers that use either SNMPv1 or SNMPv3.

### **Command-line interface changes**

The new SNMP-Manager profile contains the following parameters:

- Name
- Active
- Write-Access
- SNMP-Message-Type

Following is a listing of an unconfigured SNMP-Manager profile, showing the default settings:

```
admin> list
[in SNMP-MANAGER/" " (new)]
name* = " "
active= no
write-access = no
snmp-message-type = v1-and-v3
```

## Configuring host security

To enforce host authentication, proceed as follows:

- 1 Create a new `SNMP-Manager` profile.
- 2 For the `Name` parameter, specify the DNS hostname or IP address of an SNMP manager that will have access to the unit. If you specify a DNS hostname, you must enable DNS. If DNS is not enabled, `Name` will be set to 0.0.0.0 and the manager will not be authenticated.
- 3 To enable the profile, set `Active` to `Yes`.
- 4 To enable read-only access, accept the `Write-Access` default of `No`. To enable read and write access, set the `Write-Access` parameter to `Yes`.
- 5 To specify SNMPv1 access only, set the `SNMP-Message-Type` parameter to `V1-Only`. To specify SNMPv3 access only, specify `V3-Only`. To specify both SNMPv1 and SNMPv3 access, accept the `SNMP-Message-Type` default of `V1-and-V3`.
- 6 Write the `SNMP-Manager` profile.
- 7 Read the `SNMP` profile.
- 8 Set `Enforce-Address-Security` to `Yes`.
- 9 Write the `SNMP` profile.

For example, to specify that a host called Tom has read and write access to the unit by means of SNMPv3 only, proceed as follows:

```
admin> new snmp-manager
SNMP-MANAGER/ " " read
admin> set name = tom
admin> set active = yes
admin> set snmp-message-type = v3-only
admin> set write-access = yes
admin> write
SNMP-MANAGER/tom written
```

## Parameter reference

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

### *SNMP-Message-Type*

**Description:** Specifies whether the unit accepts SNMPv1 messages only, SNMPv3 messages only, or both SNMPv1 and SNMPv3 messages.

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

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

**Example:** `set snmp-message-type = v1-only`

---

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

**Location:** SNMP-Manager

## Write-Access

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

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

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

**Example:** `set write-access = yes`

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

**Location:** SNMP-Manager

## Discontinued parameters

The Read-Access-Hosts and Write-Access-Hosts arrays in the SNMP profile are no longer available. These arrays have been replaced by the Name and Write-Access settings in the new SNMP-Manager profiles. Following is the modified SNMP profile, without the discontinued parameters:

```
admin> list
[in SNMP]
enabled = yes
read-community = public
read-write-enabled = no
read-write-community = write
enforce-address-security = yes
contact = ""
location = ""
queue-depth = 0
csm-modem-diag = no
snmp-message-type = v1-and-v3
security-level = none
enable-vacm = no
```

---

## SNMP: New trap for unauthorized access

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

The new `ascendSecurityAlert` trap contains the following information:

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

### New Ascend Security Alert trap

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

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

::= 49
```

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

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

::= { ascendNotificationObjects 2 }
```

### New syslog messages

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

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

The following `syslog` format is used for SNMPv3:

```
LOG alert, Shelf 1, Controller, Time: hour:minute:second--
```

---

SNMPV3 Security Alert: attempt to query system from Host *ipaddress*

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

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

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

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

These attributes apply only to 16-bit VSAs.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## MultiVoice features in TAOS 9.1.0

### SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x

This release supports two-stage dialing in SS7 Voice over IP. Support for two-stage dialing in SS7 VOIP involves performing iterative dual-tone multifrequency (DTMF) detection and voice announcement payout by the MAX TNT prior to the setup of the actual packet or time-division multiplexing (TDM) call.

#### VoIP call-persistence

The MAX TNT already provides support for playing a voice announcement. To do this, for each announcement request, the MAX TNT sets up a VoIP call route, plays the announcement, then tears down the VoIP call route when the announcement is over.

However, to minimize the impact on the shelf controller, we do not want to take the same approach for each request for DTMF detection and voice announcement that might be received for a given call while two-stage dialing is in progress. Therefore, this enhancement changes the MAX TNT such that a VoIP call route from a MultiDSP slot card DSP to a line card DS0 is created for a call and maintained across the VoIP-related IPDC requests (that is, DTMF detection and voice announcements) associated with the call, prior to the actual setup of the packet or TDM call.

Since the new way introduces some nonstandard behavior into the interaction between the MAX TNT and a Lucent Softswitch (discussed below), we also maintain the existing functionality, for those deployments that need not use the new capability.

To differentiate between the existing and new ways of handling VoIP requests over IPDC, we introduce the term *VoIP call persistence*. The new way sets up and maintains a VoIP call route before the actual packet or TDM call is set up so that the VoIP call route persists across the VoIP-related IPDC requests for a given call. VoIP call persistence is enabled.

The existing way means that the VoIP call route exists for a single VoIP-related IPDC request. VoIP call persistence is disabled. This enhancement introduces a third way, which is a hybrid of existing and new and is an optimization of the former: When VoIP call persistence is disabled, if a request to play an announcement is received while DTMF detection is in progress for a given call (or vice-versa), the MAX TNT uses the VoIP call route that was set up for DTMF detection (or voice announcement). The VoIP call route is torn down after the announcement or after the DTMF detection has been completed, whichever occurs last.

VoIP call persistence is a Lucent-proprietary extension of IPDC. It is desirable for the default behavior of the MAX TNT to be compliant with standard implementations of IPDC. Therefore, VoIP call persistence is set to disabled by default.

#### User Interface Changes

The `Ss7voip-Call-Persistence` parameter is added to the Voip profile as illustrated by the following example. Also, two new timers have been added to the SS7 NMI Layer 3 NLCB maintained for each call and the `ss7voip` and `ss7nmi` commands have been enhanced.



---

### *ss7voip-call-persistence parameter*

**Description:** If the ss7voip-call-persistence parameter is enabled (that is, set to “yes”), a VoIP call route persists across IPDC requests for a given call, until the call is released. This enhancement will go into effect starting with the next SS7 VoIP call.

**Usage:** Values assigned to this parameter cause MultiVoice to do the following:

| Parameter value | Specifies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| yes             | VoIP call route persists across VoIP-related IPDC requests for a given call (e.g., LTN, STN, RCCP and RMCP) until the call is released (via RCR). If disabled, the VoIP call route exists only for the life of the single IPDC request, or in the case where an announcement (STN) and DTMF detection (LTN) are overlapping, after the announcement or the DTMF detection has completed, whichever occurs last. Enabling VoIP call persistence results in faster call setup and call processing times for SS7 VoIP calls initiated through IPDC. |
| no              | VoIP call persistence is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### *SS7 VoIP call persistence timer*

The new SS7 VoIP call-persistence timer applies only when VoIP call persistence mode is enabled in the Voip profile. This is the number of milliseconds to wait after the completion of the last LTN or STN request for a call (that is, after the last ALTN or ASTN was sent). If another LTN, STN or RCCP is not received for the call, then upon timer expiration the VoIP call route will be torn down, and the MAX TNT sends an RCR message.

The default value for this timer is 60000 milliseconds. Currently, this is the only permissible value.

### *Interdigit DTMF timer*

The interdigit DTMF timer specifies the number of milliseconds to wait between entry of consecutive DTMF digits. Upon timer expiration, the MAX TNT sends an ALTN message with Tag 0x35 set to value 0x00 (Timeout).

The default value for this timer is 6000 milliseconds. This value is overridden on a per-call basis by the value specified in Tag 0x31 (Interdigit Timeout) in the LTN message.

### *SS7VOIP command enhancements*

The `ss7voip -s` command has been enhanced to display details of an active SS7 VoIP call. The new details are as follows:

- The address of the DSP used in the call
- SS7 VoIP call-persistence mode for the call
- Whether or not DTMF detection is in progress for the call
- VoIP port mode of the call

```
admin> ss7voip -s
```

```
SS7VOIP Session 14532490
```

## MultiVoice features in TAOS 9.1.0

SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x

---

```
=====
ss7CallRef(4): 0
routeID: 2
dsp: {{ 1 4 3 } 0}
VOIP call persistence mode: Disabled
DTMF detection: In Progress
voipPortMode: 3
listenIp: 0.0.0.0
listenRtpPort: 0
sendIp: 0.0.0.0
sendRtpPort: 0
packetAudioMode: 0
framesPerPacket: 8
rtpSocket: -1
portReady: TRUE
sessName: VA:SS7:0
sessUp: FALSE
```

### SS7NMI command enhancements

The `ss7nmi -n` command has been enhanced to display detail associated with active IPDC calls. The new details are as follows:

- The address of the DSP used in the call, SS7 VoIP calls only (Addr B). This field used to be displayed as `{{ 0 0 0 } 0}` for SS7 VoIP calls
- The interdigit DTMF timer (Tdig)
- The SS7 VoIP call-persistence timer (Tcal)

```
admin> ss7nmi -n
```

```
SS7NMI Active Network Layer Control Blocks:
```

```
0x14534380: Type=11 (VOIP SETUP), State=4 (CALL ACTIVE)
```

```
TransId (4): 0x00000000 RouteID: 3, CallID: 1/1:3
```

```
Addr A: {{1 1 1} 1} Addr B: {{ 1 4 5 } 0}
```

```
Timer T301: 18000 ticks - idle
```

```
Timer T303: 400 ticks - idle
```

```
Timer T308: 400 ticks - idle
```

```
Timer T341: 150 ticks - idle
```

```
Timer T351: 300 ticks - idle
```

```
Timer Tsta: 400 ticks - idle
```

```
Timer Tdig: 6000 ticks - running
```

```
Timer Tcal: 6000 ticks - idle
```

```
Total number of NLCB: 1.
```

```
SS7NMI End of NLCB list.
```

---

## *Supported Messages and Tags (for IPDC, version 0.15.1)*

This section describes the impact of the changes made by this feature on the MAX TNT implementation of IPDC. Unless otherwise noted, the changes are based on the version of IPDC as given in the document *IPDC Revision 0.15.1* (April 8, 1999).

### *IPDC Packet*

The same Transaction ID must be used for all IPDC messages associated with a call (for example, LTN, STN, RCCP, RMCP, RCR).

### *LTN message*

The following table shows tags from IPDC 0.15.1 that are currently supported by the MAX TNT and describes how Lucent interprets those tags.

| <b>Tag</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x46       | Maximum Total Time Allowed For Digit Collection. Not currently supported.                                                                                                                                                                                                                                                                                                                                                                                    |
| 0x49       | Tone Type. Only value 0x01 (DTMF) is supported at this time.                                                                                                                                                                                                                                                                                                                                                                                                 |
| 0x4A       | Apply/Listen or Cancel Tone — Apply Tone.<br>An LTN received with Tag 0x4A set to value 0x00 (Apply Tone) indicates that DTMF detection must be initiated for this call. Upon successful initiation of DTMF detection for the call, the MAX TNT sends an ALTN message with Tag 0x35 set to value 0x06 (Operation Started).                                                                                                                                   |
| 0x4A       | Apply/Listen or Cancel Tone — Cancel Tone.<br>The MAX TNT supports an LTN-cancel operation as defined in <i>IPDC Revision 0.17</i> (February 9, 2000). An LTN received with Tag 0x4A set to value 0x01 (Cancel Tone) indicates that DTMF detection must be terminated for this call. Upon successful termination of DTMF detection for the call, the MAX TNT sends an ALTN message with Tag 0x35 set to value 0x02 (Operation Terminated By The Softswitch). |

### *ALTN message*

The following table shows tags from IPDC 0.15.1 that are currently supported by the MAX TNT, and describes how Lucent interprets those tags.

| Tag  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x35 | <p>Tone Listen Completion Status</p> <p>The MAX TNT will send an ALTN message with Tag 0x35 set to value 0x06 "Operation Started" upon successfully enabling DTMF detection in response to an LTN request.</p> <p><b>Note:</b> This new use of the ALTN message and new value for Tag 0x35 are not part of the IPDC standard. However, the use of ALTN as an "Operation Started" acknowledgment to an LTN request is conceptually consistent with the use of ASTN as an "Operation Started" acknowledgment to an STN request, which <i>is</i> part of the standard.</p> |

### *ALTN as a response to LTN*

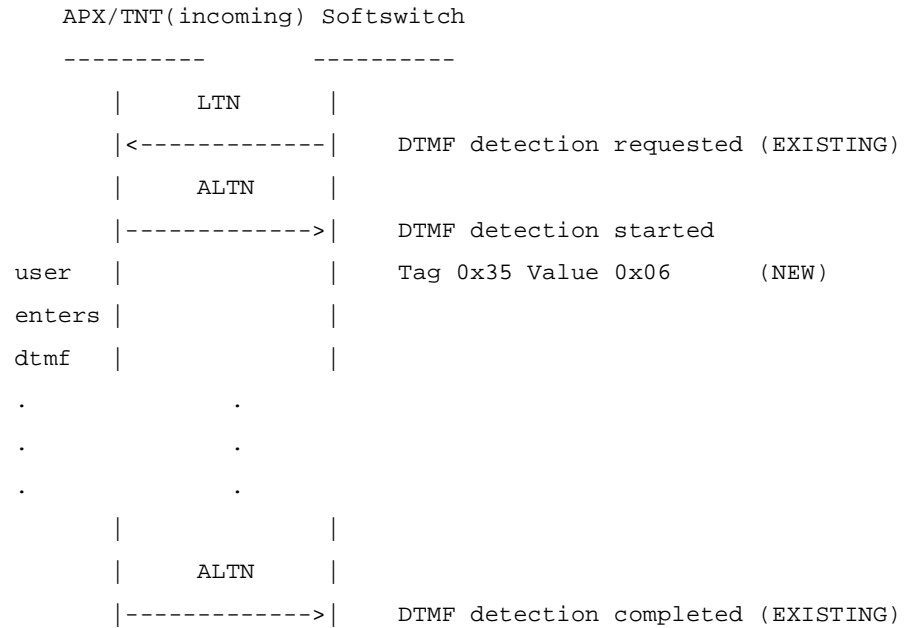
All required tags are included in the ALTN message used as an "Operation Started" acknowledgment to an LTN request. In particular, the ALTN will contain the following tags and values:

- Tag 0x07 ("Module Number") the value received in the LTN
- Tag 0x0D ("Line Number") the value received in the LTN
- Tag 0x15 ("Channel Number") the value received in the LTN
- Tag 0x49 ("Tone Type") the value received in the LTN
- Tag 0x35 ("Tone Listen Completion Status") set to the value 0x06 ("Operation Started")
- Tag 0x32 ("Tone String Length") set to 0
- Tag 0x33 ("Tone String") set to the null string

### *Sample call flow*

The following shows an example call flow using LTN and ALTN between a MAX TNT and a Softswitch for DTMF collection.

The use of ALTN as both an "Operation Started" and "Operation Stopped" message for an LTN request is directly analogous to the way that the ASTN message is used for an STN request.



### *ALTN as a response to LTN-cancel*

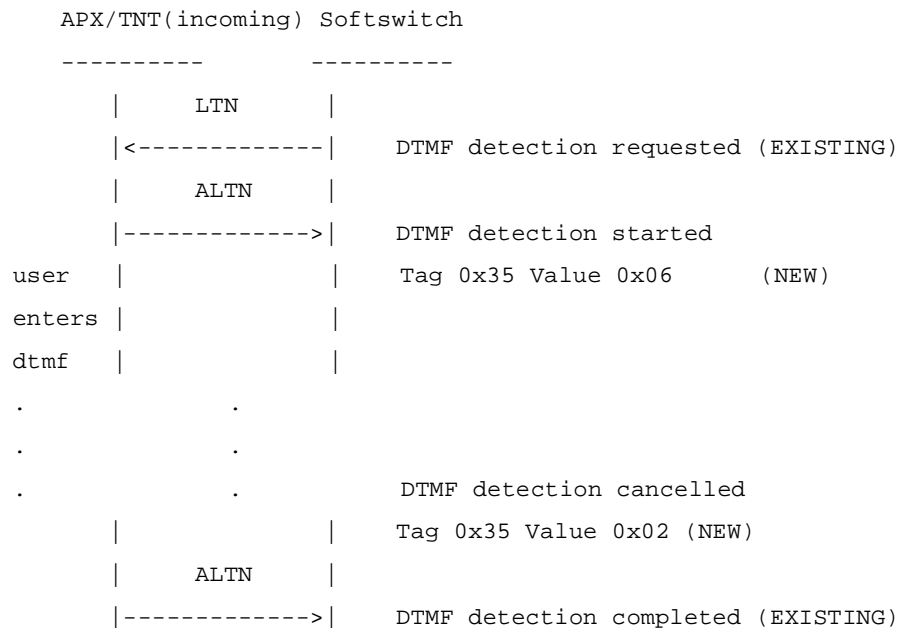
When an ALTN message is used as an acknowledgment to an LTN-cancel request, all required tags are included. In particular, the ALTN contains the following tags and values:

- Tag 0x07 ("Module Number") the value received in the LTN
- Tag 0x0D ("Line Number") the value received in the LTN
- Tag 0x15 ("Channel Number") the value received in the LTN
- Tag 0x49 ("Tone Type") the value received in the LTN
- Tag 0x35 ("Tone Listen Completion Status") set to the value 0x02 ("Operation Terminated By The Softswitch")
- Tag 0x32 ("Tone String Length") set to the number of DTMF digits collected so far
- Tag 0x33 ("Tone String") set to the string of DTMF digits collected so far

The Softswitch must not send a request to cancel DTMF collection until it has first received a DTMF collection "Operation Started" acknowledgment (ALTN with "Operation Started") from the MAX TNT.

### *Sample Call Flow*

The following shows an example call flow using LTN and ALTN between a MAX TNT and a Softswitch for DTMF collection and cancellation.



## STN message

The following changes have been made:

| Tag  | Description                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x86 | Announcement Treatment<br>The value 0x00 (Continuous Play) is not currently supported .<br>The maximum value allowed in tag 0x86 remains 0xFF. |

## ASTN message

The following changes have been made:

| Tag  | Description                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------|
| 0xFE | Cause Code<br>The inclusion of this tag in the ASTN message is a non-standard extension of IPDC. It has been removed. |

## Notes on using LTN/STN messages

When an LTN and STN are both run during a call, the LTN can be sent before the STN, or vice-versa.

The first DTMF entered while an announcement is playing stops the announcement. An ASTN is sent and DTMF collection continues. When DTMF collection completes, an ALTN is sent. If only one DTMF digit is requested by an LTN message, then the ASTN message is sent first,

followed by the ALTN message. This order is guaranteed for such requests. In general, the ASTN message is sent before the ALTN unless the interdigit timer expires while an announcement is playing or the LTN is canceled while an announcement is playing. In both cases, an ALTN is sent and the announcement is not interrupted. When the announcement completes, an ASTN is sent.

If an LTN is to be sent immediately following an STN, the Softswitch should not send the LTN until the ASTN (start) has been received. If an STN is to be sent immediately following an LTN, the Softswitch should not send the STN until the ALTN (start) has been received.

### *Summary of Nonstandard IPDC Behavior*

In addition to the ALTN "Operation Started" message, there are two other non-standard IPDC behaviors introduced into the MAX TNT by this feature.

- In VoIP call-persistence mode, for a packet call, if an LTN or STN message has been successfully processed, the Softswitch must send an RCR message to free the VoIP call route unless an RCCP message has been sent for the call. If an RCCP message has been sent, an RCR is eventually sent to end the call and free the VoIP call route in the usual way. This use of RCR is nonstandard.
- In VoIP call-persistence mode, for a TDM call, if an LTN or STN has been successfully processed, the Softswitch must send an RCR to free the VOIP call route before the RCST is sent for the call. This use of RCR is non-standard.

For more information, see the example call flows below.

### *Call flows—VoIP-persistence mode enabled*

When Voip-persistence mode is enabled, there are many possible call flows for two-stage dialing. Only a few representative flows are described here.

#### Successful Two-Stage Packet Call

The following call flow shows the interaction between the MAX TNT and the Softswitch for a two-stage call over SS7 VoIP that culminates in the successful setup of a packet call.

The first stage of a two-stage call begins with the receipt of the first LTN by the incoming MAX TNT, and ends with the receipt of the last ALTN message by the Softswitch.

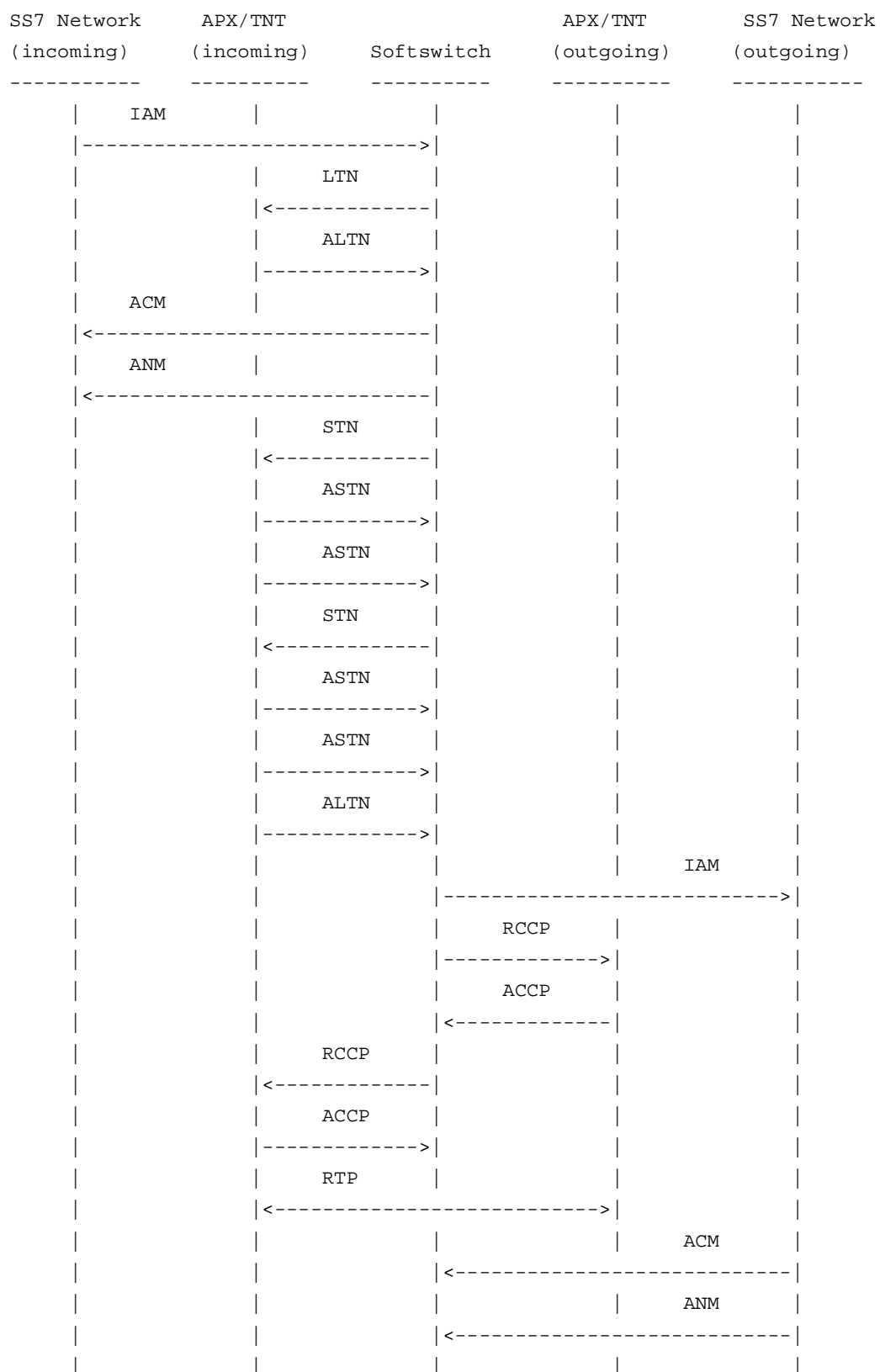
The first (and in this example only) LTN instructs the MAX TNT to enable DTMF VoIP call route setup by the MAX TNT when the LTN is received. Upon setting up the VoIP call route, the MAX TNT sends an ALTN message ("Operation Started") and begins DTMF detection. The Softswitch can now send the STN.

Upon receipt of the first STN message, the MAX TNT sends an ASTN message ("Operation Started") and plays the announcement. In TAOS 9.1.0, it is done using the VoIP call route that was setup when the first LTN was received.

The second ASTN message is sent when the announcement is completed. The second STN message requests to play an announcement that instructs the user to enter the DNIS. Upon receipt of the second STN, the MAX TNT sends an ASTN message ("Operation Started") and plays the announcement. In TAOS 9.1.0, this is done using the VoIP call route that was setup when the first LTN was received.

## MultiVoice features in TAOS 9.1.0

SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x





The fourth ASTN message is sent when the announcement is completed. The MAX TNT sends the ALTN message when the user has completed DTMF entry of the DNIS. The user does not enter any DTMF tones while an announcement was playing. If DTMF tones are entered, the announcement stops and the ASTN message is generated at that time.

The call then continues in the usual way. When the incoming MAX TNT receives the RCCP, it sets up its side of the packet call using the VoIP call route that was setup when the first LTN message was received. When the outgoing MAX TNT receives the RCCP, it sets up a VoIP call route from a MultiDSP card DSP to a line slot card DS0, just as it did in previous versions of TAOS.

**Note:** Additional LTN/STN iterations are possible, for example, if PIN entry is also required or if the DNIS or PIN that is entered is rejected by the Softswitch.

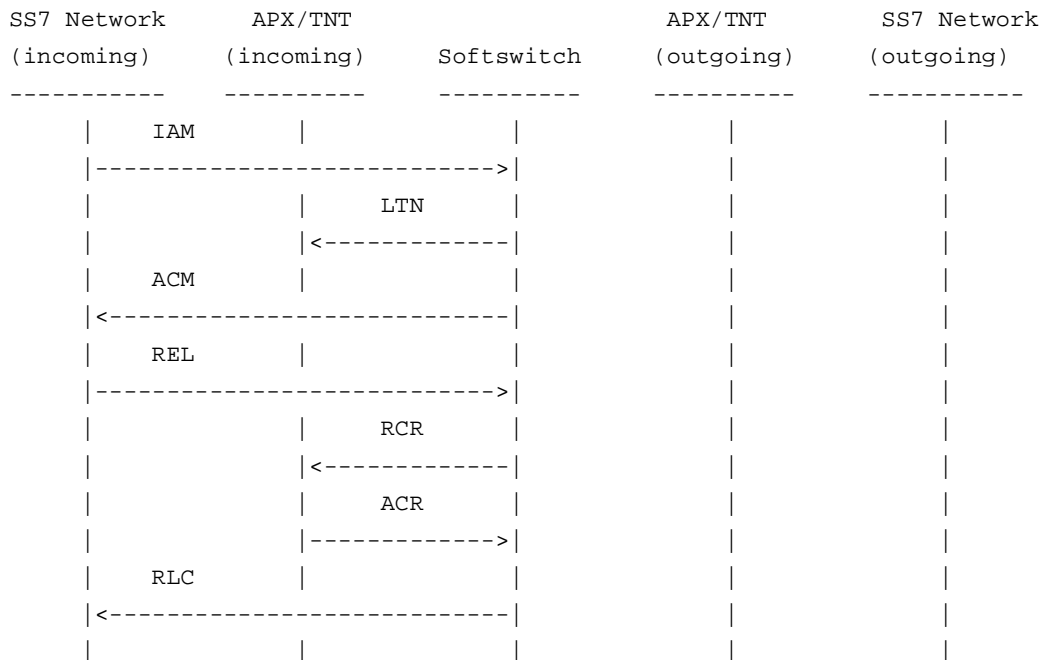
#### Aborted Two-Stage Call - Case 1

The following call flow shows a two-stage call that is aborted by a incoming call release after an STN has been received by the incoming MAX TNT.

The RCR allows the MAX TNT to free the resources (for example, a MultiDSP slot card DSP) associated with the VoIP call route that was setup for the two-stage call when the first LTN was received. If VoIP call-persistence is disabled, the RCR is not needed.

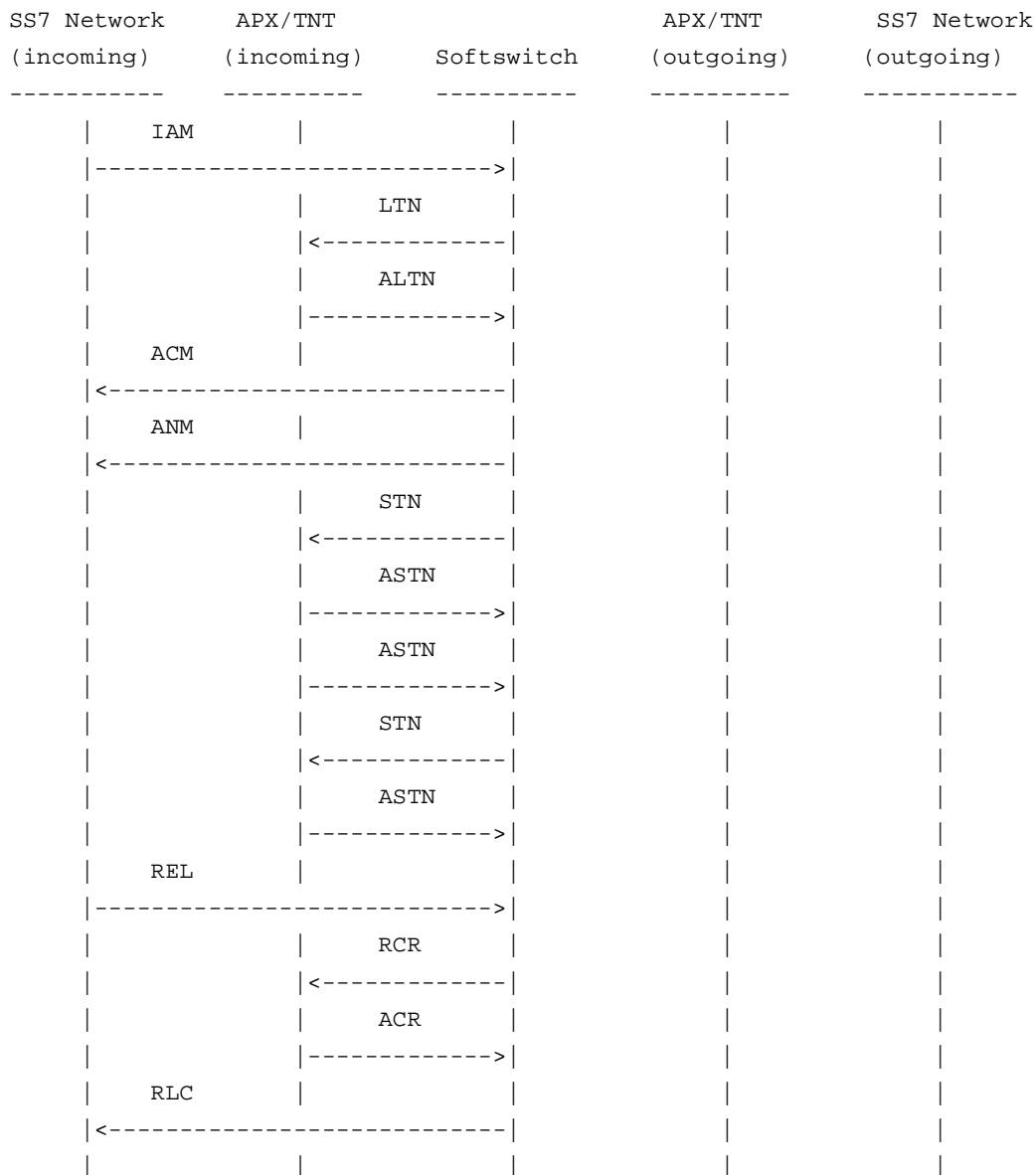
#### Aborted Two-Stage Call - Case 2

The following call flow shows a two-stage call that is aborted by a incoming call release after an LTN has been received by the incoming MAX TNT.



## MultiVoice features in TAOS 9.1.0

SS7 IPDC: DTMF collection via IPDC/Lucent Softswitch 3.x

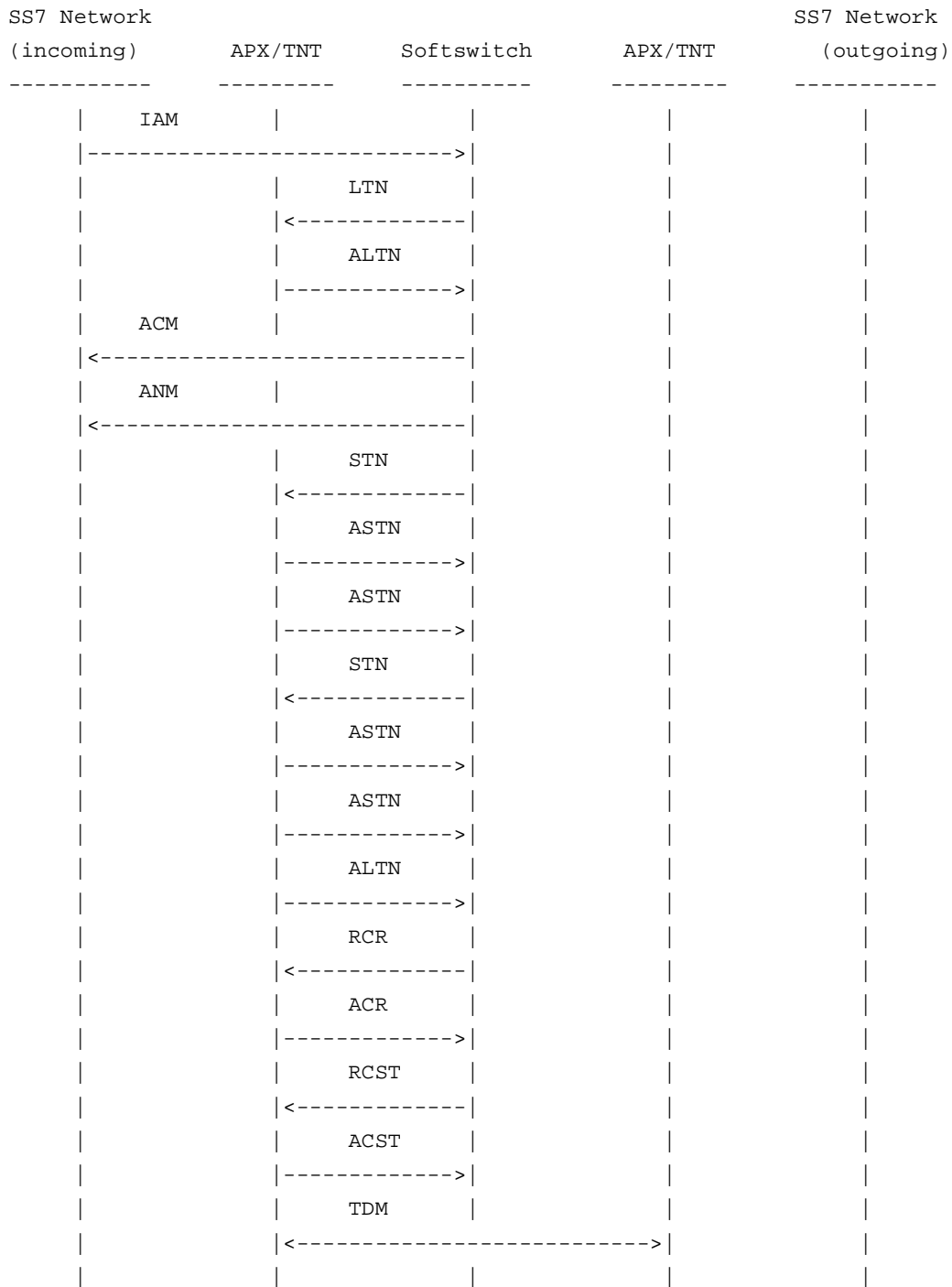


The RCR message allows the MAX TNT to free the resources (for example., a MultiDSP slot card DSP) associated with the VoIP call route that was set up for the two-stage call when the first LTN message was received.

If VoIP call-persistence is disabled, the RCR is not needed.

### Successful Two-Stage TDM Call

The following call flow shows the interaction between the MAX TNT and the Softswitch for a two-stage TDM call.



The RCR allows the MAX TNT to free the resources (for example, a MultiDSP slot card DSP) associated with the VoIP call route that was set up for the two-stage call when the first LTN message was received.

It is necessary to do this because the TDM channel and the channel used for the VoIP call route cannot be shared. If VoIP call-persistence is disabled, the RCR is not needed.

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

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

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

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

### **New Next Call parameter**

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

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

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

### **Enabling next calls**

The following procedure illustrates how to enable the Next Call feature with a value other than the default:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set single-dial-enable=no
admin> set dtmf-tone-passing=dtmf-tone-passed-outofband
admin> set sequential-call-enable=yes
admin> next-call=**10
admin> write
VOIP/{ 0 0 } written
```

## *Contingencies*

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

- The Single Dial Enable parameter  
Must be set to `no` because the MultiVoice Gateway must use two-stage dialing. The Single Dial Enable parameter enables or disables single-stage dialing of VoIP calls when MultiVoice is configured to perform H.323 call processing. In two-stage dialing, callers must dial the MAX TNT, before being prompted to dial the called telephone number.
- The DTMF Tone Passing parameter  
Must be set to `Dtmf Tone Passed Outofband`. The parameter filters the tone from the voice path and passes the corresponding digits to the far-end gateway using a non-RTP path. Once received at the far end, the digits are played out. This out-of-band processing works even with both gateways operating in opposite modes. For example, when an inband gateway is talking to an out-of-band gateway, the inband gateway accepts the out-of-band DTMF play-out commands.
- The Sequential Call Enable parameter  
Must be set to `yes`. When this parameter is set to `yes` and a PIN is required to authenticate MultiVoice calls, reentering the PIN is not required to dial the next VoIP call, as long as the connection between the PSTN and near-end MultiVoice Gateway has not been terminated.

## *Three calling card features using IPDC*

In this release, three additional features have been added to support two-stage dialing for SS7. They are:

- Voice announcement playlists.
- Break-in voice announcements.
- In-call Dual Tone Multi-Frequency (DTMF) detection and notification (for call re-origination).

These features can be used by any SS7 VoIP customer, but require obtaining a pre-paid billing application.

**Note:** Refer to *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15* specification for an explanation of all messages and tags that are referred to in this feature description.

## Voice announcement playlists

This feature allows a list of announcement files to be signaled to the MultiVoice Gateway in the STN message.

### *STN Message*

The following changes were made in the STN message in IPDC to support this feature.

#### Tag 0x33 (Tone String)

This tag previously took as its value the name of an announcement file (for example, h323dns.au).

This tag will now accept the name of an announcement file, or a comma-separated list of announcement files (for example, h323dns.au, 1.au, 2.au). Intervening blanks are optional.

In addition, a playlist format is supported. This format is:

```
(c,d,(filename,c,d)...(filename,c,d))
```

where:

c = playCount (default = 1)

d = delay (default = 0) in milliseconds.

An example is:

```
(1,0(file1.au,1,5)(file2.au,2,5)(file3.au,1,5))
```

This format is useful if you want to specify non-default playcount and delay values for individual files in the playlist, since there is no way to signal this through IPDC.

#### Tag 0x86 (Announcement Treatment)

If a list of announcement files has been specified, the value of this tag is applied to the entire list in sequence. For example, if the value is "2", the entire list is played twice.

If playlist format is used, this value is ignored.

Example:

```
Tag 0x33 = h323f.au,h323dns.au
```

```
Tag 0x86 = 2
```

is equivalent to:

```
Tag 0x33 = (2,0,(h323f.au,1,0),(h323dns.au,1,0))
```

## Break-in voice announcements

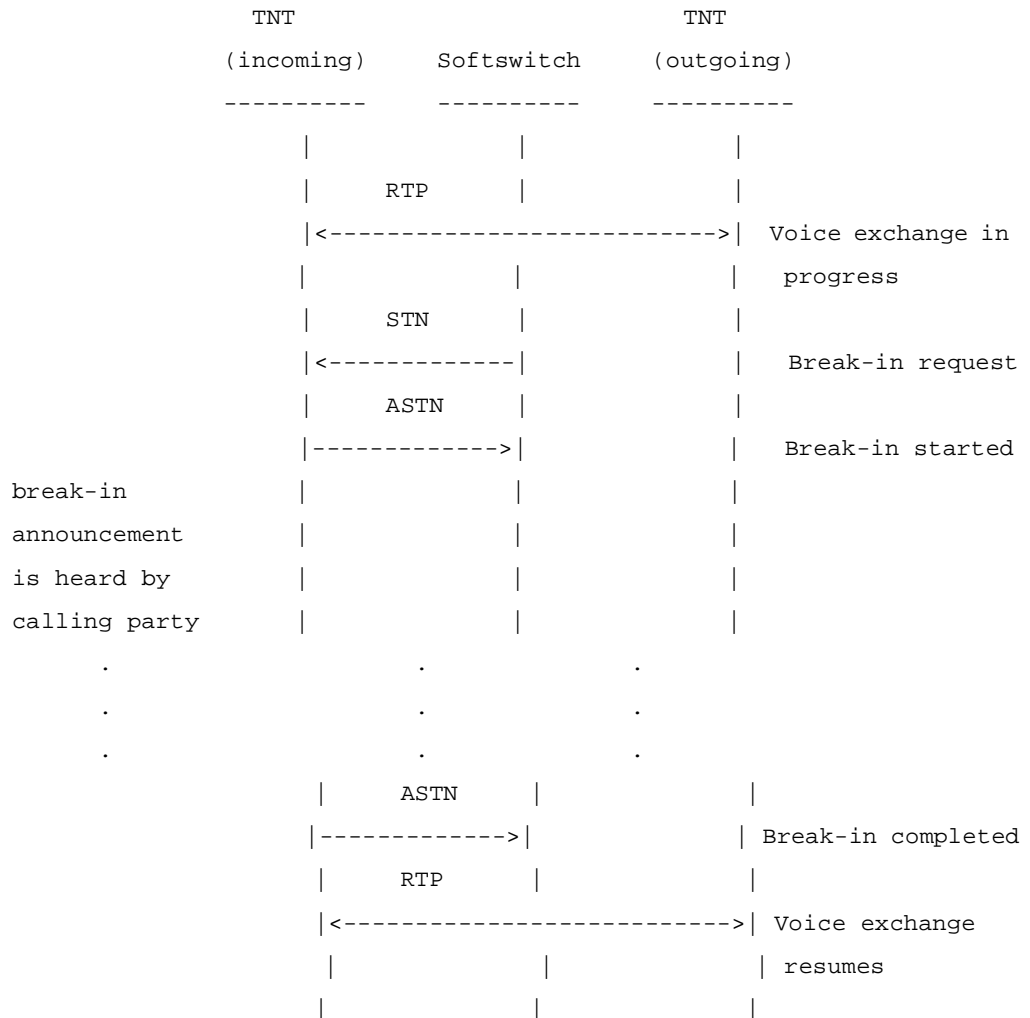
This feature allows a voice announcement to be played while a packet call is in progress. While a break-in voice announcement is playing, the Real-time Transport Protocol (RTP) flow to the called party is suspended, the calling party hears the voice announcement, and the called party hears silence.

While a break-in announcement is typically played to the calling party, it could be played out to the called party instead of or as well.

### STN/ATN Messages

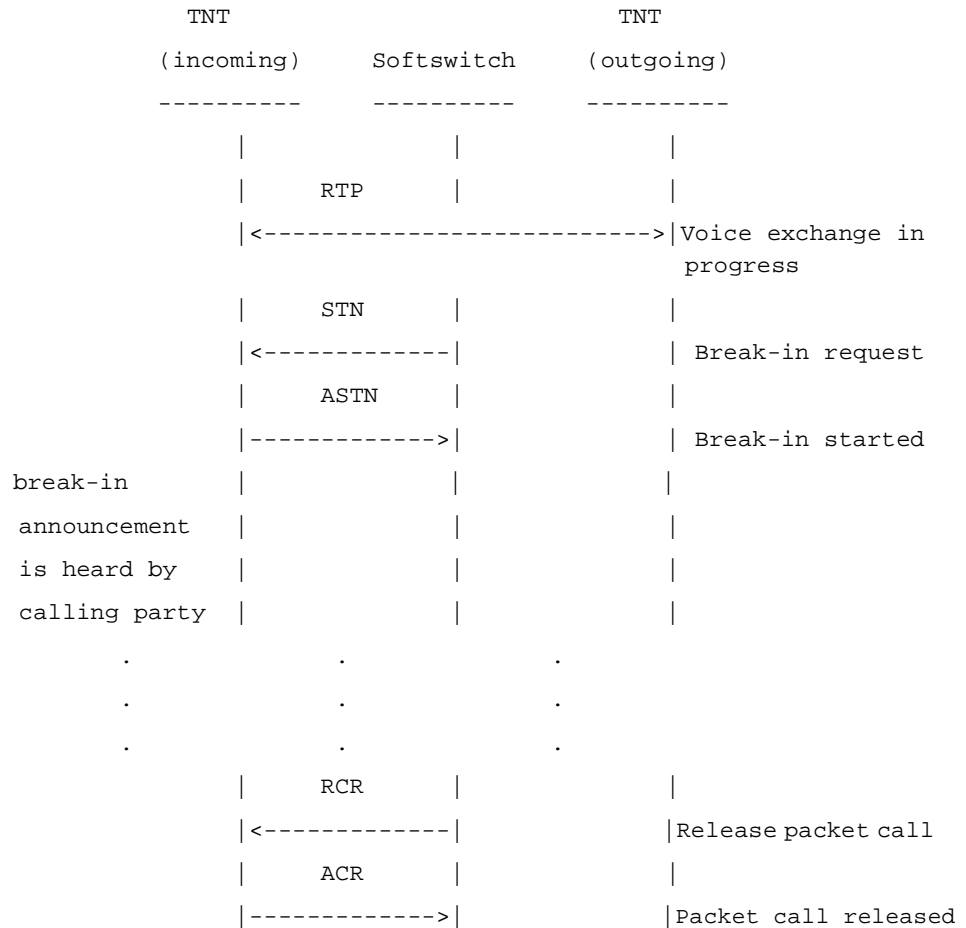
Break-in voice announcements utilize existing STN/ASTN messaging without modification. The cancel operation is fully supported.

#### Call flow



#### Call Flow — Call Release

If a break-in announcement is playing and an RCR is received, the call is released and an ACR is sent containing the RTP statistics for the packet call:



#### Caveats

Break-in voice announcements are supported for packet calls, not for TDM calls.

## In-Call DTMF detection

This feature allows the Softswitch to direct the MultiVoice Gateway to perform DTMF detection and notification while a packet call is in progress. This support is provided by modification to the RCCP, RMCP, and NTN messages.

Any DTMF digits entered during the call while DTMF detection is enabled will still be played out to the other party.

### *RCCP Message*

The following changes were made in the RCCP message in IPDC to support this feature.

#### Tag 0x75 (Constant DTMF Tone Detection)

This tag is now supported. The following tag values are supported:

- 0x00 - DTMF tone detection off
- 0x01 - DTMF tone detection on



If tag is missing, DTMF tone detection is off.

## *RMCP Message*

The following changes were made in the RMCP message in IPDC to support this feature.

### Tag 0x75 (Constant DTMF Tone Detection)

This tag is now supported. The following tag values are supported:

- 0x00 - DTMF tone detection off
- 0x01 - DTMF tone detection on

If tag is missing, there is no effect on current state of detection.

## *NTN Message*

The following changes were made in the NTN message in IPDC to support this feature.

### Tag 0x49 (Tone Type)

The following tag value is now supported:

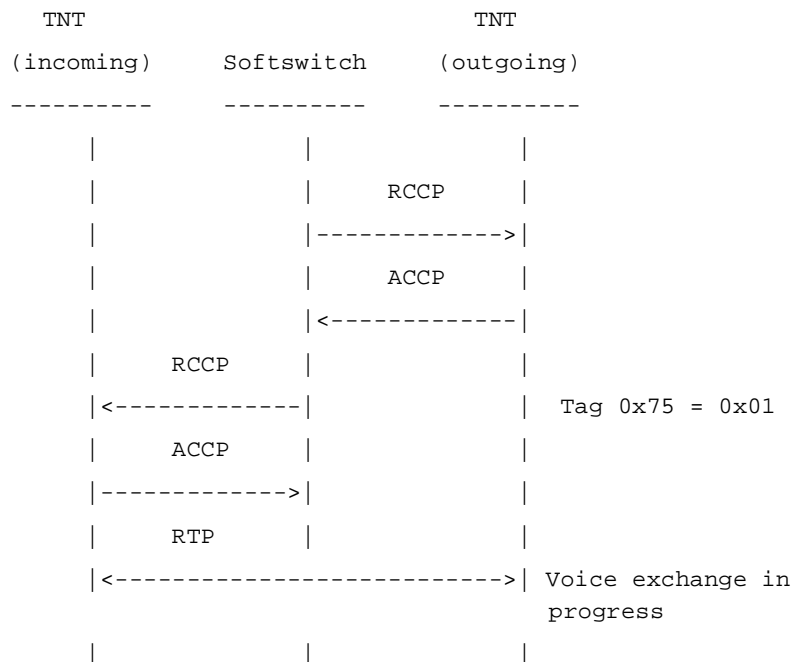
- 0x01 - DTMF tone

### Tag 0x33 (Tone String)

This tag will contain the DTMF digit that was detected. The length of this tag value will be 1.

## *Call-Flow*

In the following call flow, a packet call is setup with DTMF detection enabled. After 2 DTMF digits are entered, the call is modified to disable DTMF detection.



## MultiVoice features in TAOS 9.1.0

### Three calling card features using IPDC

---

|              |        |  |                    |
|--------------|--------|--|--------------------|
| user enters  | NTN    |  |                    |
| a dtmf digit | -----> |  | Tag 0x33 = <digit> |
| user enters  | NTN    |  |                    |
| a dtmf digit | -----> |  | Tag 0x33 = <digit> |
|              | RMCP   |  |                    |
|              | <----- |  | Tag 0x75 = 0x00    |
|              | AMCP   |  |                    |
|              | -----> |  |                    |
| user enters  |        |  |                    |
| a dtmf digit |        |  |                    |
| user enters  |        |  |                    |
| a dtmf digit |        |  |                    |

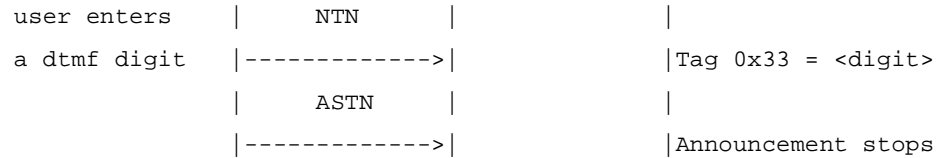
---

### Interaction with break-in voice announcements

If in-call DTMF detection is enabled and a break-in announcement is played, the first DTMF entered will stop the announcement:

| TNT<br>(incoming) | Softswitch | TNT<br>(outgoing)          |
|-------------------|------------|----------------------------|
| -----             | -----      | -----                      |
|                   | RCCP       |                            |
|                   | ----->     |                            |
|                   | ACCP       |                            |
|                   | <-----     |                            |
| RCCP              |            |                            |
| <-----            |            | Tag 0x75 = 0x01            |
| ACCP              |            |                            |
| ----->            |            |                            |
| RTP               |            |                            |
| <----->           |            | Voice exchange in progress |
|                   |            |                            |
| STN               |            |                            |
| <-----            |            |                            |
| ASTN              |            |                            |
| ----->            |            | Announcement starts        |
|                   |            |                            |

---



An RMCP that is received by the MultiVoice Gateway while a break-in announcement is playing will be rejected. An MRJ will be sent with Tag 0xFE (Cause Code) set to 0x65 (Message Not Compatible With Call State).

#### Caveats

In-call DTMF detection is supported for packet calls, not for TDM calls.

If DTMF is being carried inband, then the first DTMF digit entered during a break-in announcement is not played out to the other party.

### *Call re-origination*

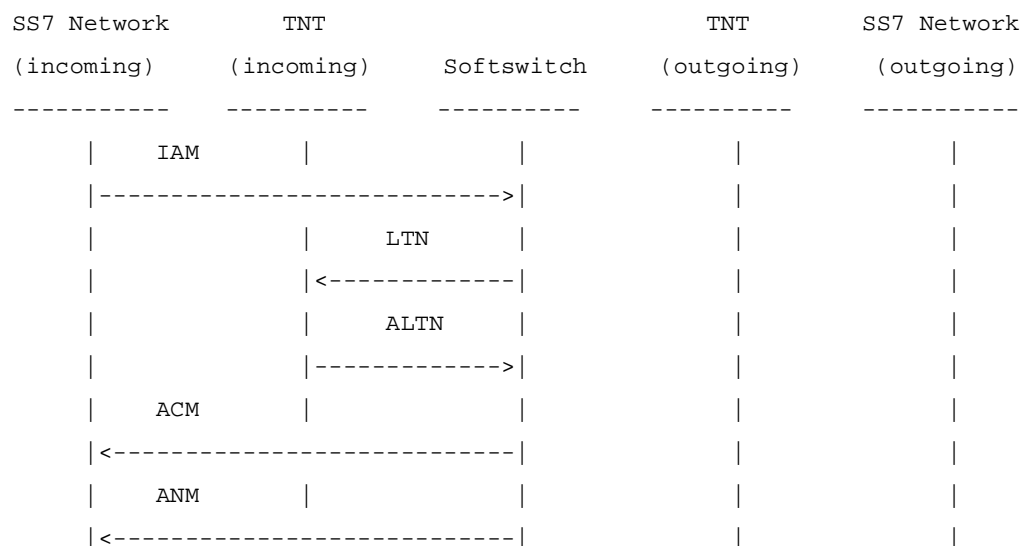
In-call DTMF detection can be combined with existing IPDC support on the MultiVoice Gateway to provide a call re-origination application.

Using in-call DTMF detection, the MultiVoice Gateway forwards DTMF received during an active packet call to the Softswitch. The DTMF is sent in the NTN message, one digit per message. The Softswitch monitors the received DTMF stream for a pattern (eg. "\*\*\*9") that indicates that the calling party wishes to terminate the active call and start a new call.

The Softswitch then sends an RCR, waits for the ACR, then sends an LTN to start the two-stage dialing for the next call, while maintaining the signaling for the incoming CIC with the PSTN.

The RCR tells the incoming MultiVoice Gateway to terminate the VoIP call. This tears down the VoIP call route and frees the resources associated with the VoIP call. The ensuing LTN would be identified as the first one for a call. This tells the incoming MultiVoice Gateway to setup a new VoIP call route.

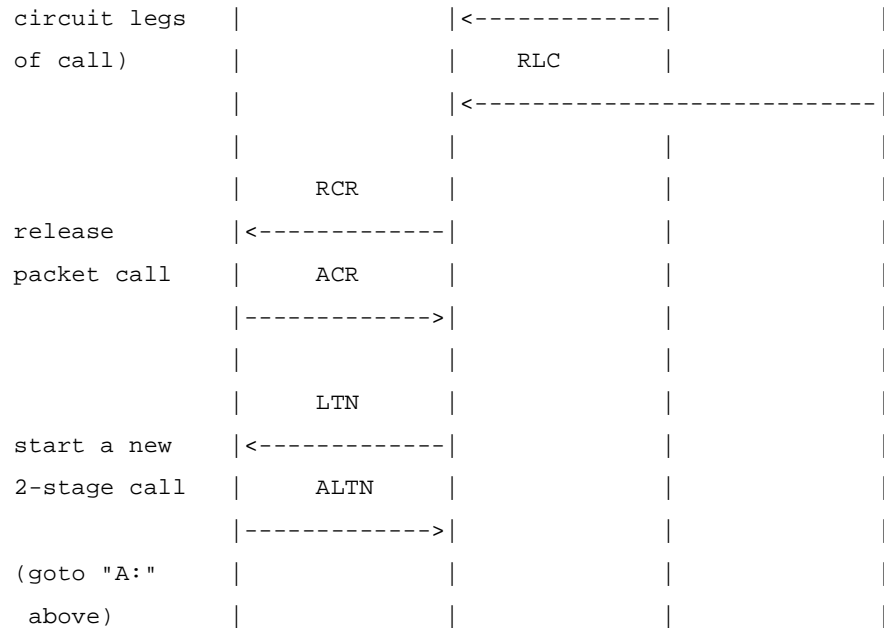
The following call flow shows how in-call DTMF detection is utilized for call re-origination.



## MultiVoice features in TAOS 9.1.0

### Three calling card features using IPDC

|                       |         |        |     |  |
|-----------------------|---------|--------|-----|--|
| A:                    | STN     |        |     |  |
| play                  | <-----  |        |     |  |
| announcement          | ASTN    |        |     |  |
| to enter              | ----->  |        |     |  |
| dnis                  | ASTN    |        |     |  |
|                       | ----->  |        |     |  |
| dnis entered          | ----->  |        |     |  |
|                       |         |        | IAM |  |
|                       |         | -----> |     |  |
|                       |         |        | ACM |  |
|                       |         | <----- |     |  |
|                       |         |        | ANM |  |
|                       |         | <----- |     |  |
|                       |         | RCCP   |     |  |
|                       |         | -----> |     |  |
|                       |         | ACCP   |     |  |
|                       |         | <----- |     |  |
|                       | RCCP    |        |     |  |
| packet call           | <-----  |        |     |  |
| set up                | ACCP    |        |     |  |
| dtmf detection        | ----->  |        |     |  |
| enabled               | RTP     |        |     |  |
|                       | <-----> |        |     |  |
|                       |         |        |     |  |
| user enters           | NTN     |        |     |  |
| a dtmf digit          | ----->  |        |     |  |
|                       |         |        |     |  |
| user enters           | NTN     |        |     |  |
| a dtmf digit          | ----->  |        |     |  |
|                       |         |        |     |  |
| softswitch recognizes |         |        |     |  |
| the 2 digits as the   |         |        |     |  |
| pattern to initiate   |         |        |     |  |
| the next call         |         |        |     |  |
|                       |         | REL    |     |  |
| softswitch            |         | -----> |     |  |
| releases other        |         | RCR    |     |  |
| end (both             |         | -----> |     |  |
| packet and            |         | ACR    |     |  |

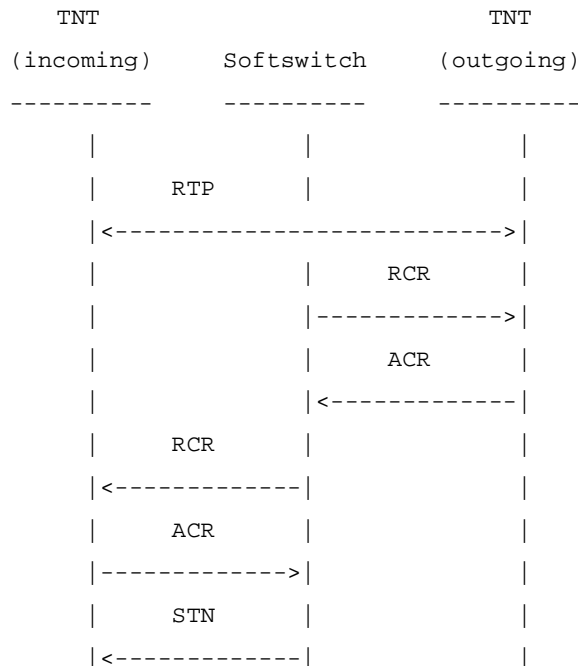


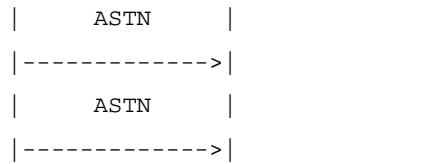
Note that call re-origination when signaled over SS7 VoIP does not use the Voip profile parameters sequential-call-enable and next-call. These parameters are used when call re-origination is signaled over H.323 VoIP.

### *End-of-call break-in voice announcements*

This section reviews the possible call flows for the special case of playing a break-in voice announcement at the end of a call. Such an announcement could be played either before or after the call is released, with VoIP call persistence enabled or disabled.

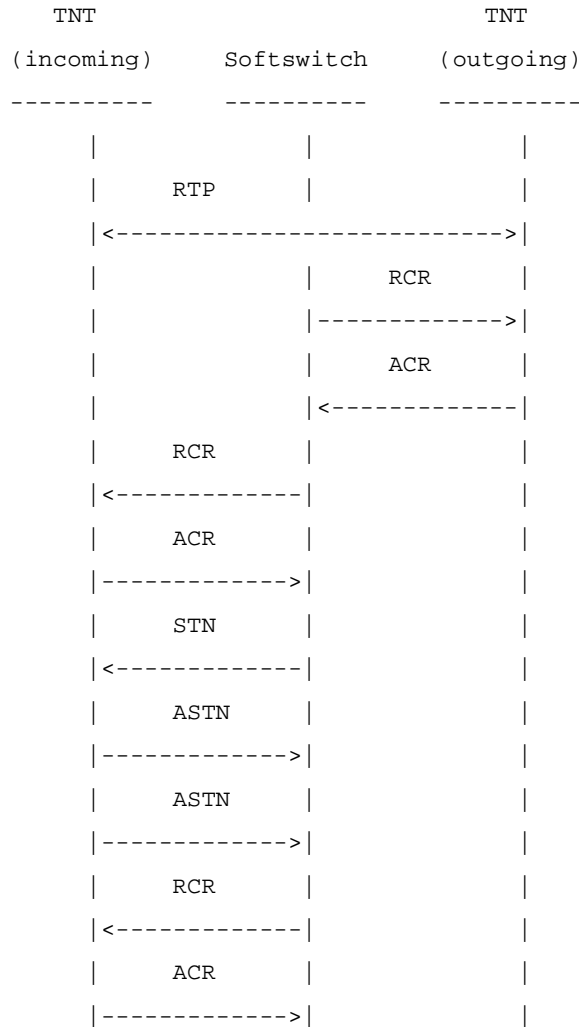
- 1 End-of-call break-in announcement played after call release, with VoIP call persistence mode disabled.





The STN will result in the setup of a new VoIP call route. Note that this messaging is possible without support for break-in announcements by using existing capabilities.

**2** End-of-call break-in played after call release, with VoIP call persistence mode enabled.

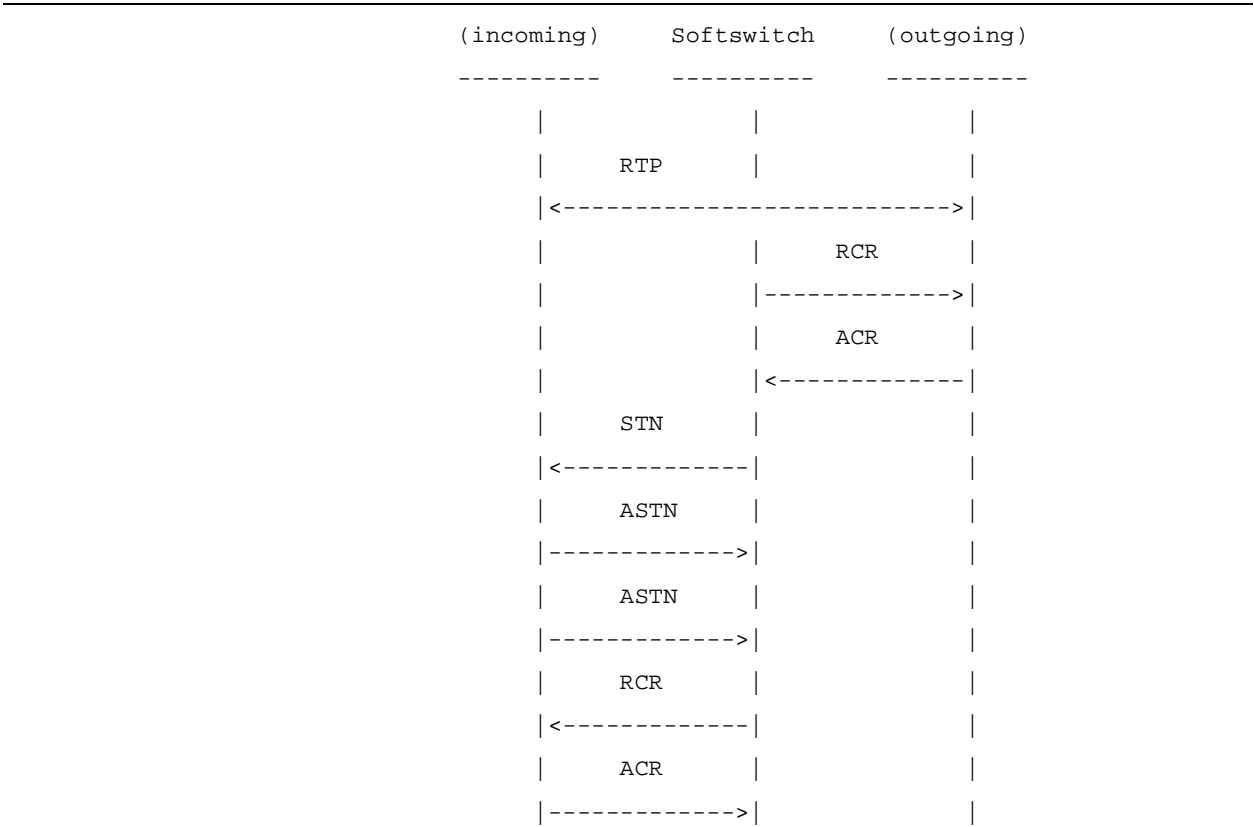


The STN will result in the setup of a new VoIP call route. A second RCR is required to destroy the VoIP call route setup by the STN to play the break-in announcement.

**Note:** The exception to this is if call re-origination is in progress. In this case, the second RCR is replaced with a LTN/STN/RCCP 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.

**3** End-of-call break-in played before call release, VoIP call persistence mode enabled or disabled.

|     |     |
|-----|-----|
| TNT | TNT |
|-----|-----|



This messaging is now possible with support for break-in announcements. The STN utilizes the existing VoIP call route for the call. This will reduce gateway processing, but will add extra seconds to the call.

## ITU G.168-2000 echo canceller

A new echo canceller, compliant with International Telecommunications Union’s (ITU) G.168-2000 standard is introduced for G.711 and G.729A audio codecs within this release of TAOS.

### Overview

Echo occurs when a speaker’s speech signal is coupled into the receive path from the far end. If the echoed signal has sufficient amplitude and delay, the speaker may experience annoying echo. The primary cause of the returned echo signals is the “hybrid”, which performs the necessary 4-wire to 2-wire conversion between the 4-wire facilities of the telecommunications network and the 2-wire telephone circuit.

### ITU G.168-2000 Recommendation

The ITU’s G.168-2000 Recommendation defines objective tests, that if passed, will ensure a minimum level of quality within the network. This recommendation increases the scope of the tests defined in G.165 and ensures that echo canceller performance is adequate under wider

network conditions, such as performance on voice, FAX, residual acoustic echo signals, and mobile networks.

Lucent Technologies' echo canceller meets or exceeds all of the objective tests defined in the G.168-2000 Recommendation. Additionally, several subjective evaluations have been performed to ensure the highest possible performance and robustness.

The new echo canceller provides 64ms echo tail cancellation for the G.711 audio codec and 32ms echo tail cancellation for the G.729A audio codec in order to properly model and cancel the echo from severe hybrid impedance mismatch. All other voice codecs (for example, G.728, G.723.1, RT-24, Full-Rate GSM) use the ITU-G.165 standard.

## ***DTMF Carriage in header of RTP per IETF RFC 2833***

This release incorporates support for RFC2833, an IETF standard that provides for the reliable in-band transport of Dual Tone Multi-Frequency (DTMF) tones. By following the RFC2833 standard, DTMF carriage in the Real-time Transport Protocol (RTP) header allows packet calls to use a non-inband DTMF tone passing mode.

**Note:** In this release, support is provided only for the G.711 and G.729(A) voice codecs. Future releases may implement RFC2833 support for the more complex and higher compression codecs (such as, G.723.1).

## **Background**

The higher compression codecs (e.g. G.723.1 or RT-24) achieve their compression by only transferring the signal features that are most relevant for human perception. When they are applied to pure tones (such as DTMF), they distort them. This distortion is severe enough to prevent in-band transmission of DTMF tones through these codecs.

To avoid this distortion, the encoding DSP must detect the DTMF signal and pass the tone information via another channel to the decoding DSP. Previously, the only available channel was via the H.245 protocol.

### ***Transfer via the RTP Stream***

RFC2833 defines a public standard mechanism for the transfer of these tone signals within the RTP stream. Using the RTP stream will allow gateways to transfer DTMF tones.

In addition to allowing DTMF transfer when using voice channels that cannot reliably transmit DTMF tones, the use of RFC2833 for DTMF transfer will also allow:

- The exact synchronization of DTMF with the voice stream, and the reproduction of the tone's duration (up to a maximum of 8 seconds).
- Redundant DTMF information transfer that will allow the correct reproduction of DTMF in unreliable networks.

**Note:** The MultiVoice product line does not support the negotiation of dynamic payload types. Consequently, a fixed payload type value has been provided for the current RFC2833 implementation. Also, there is no negotiation of support for RFC2833 at call setup time, hence all machines in a network must support RFC2833 for any one of them to use it.



## User Interface Changes

This enhancement modifies the Dtmf-Tone-Passing parameter in the Voip { X X } profile as illustrated as follows.

### dtmf-tone-passing parameter

**Description:** When the value of the dtmf-tone-passing parameter is set to `rfc2833` on a gateway, DTMF tones are transferred and passed via another channel to the decoding DSP, according to the RFC2833 standard. This enhancement will go into effect starting with the next VoIP call.

**Example:** The following example illustrates how to enable the transferal and passing of DTMF tones on an IPDC-based gateway:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set dtmf-tone-passing=rfc2833

admin> write
VOIP/{ 0 0 } written
```

**Dependencies:** This option will only be available when the Packet-audio-mode parameter has been set to use the G.711 or G.729(A) codec.

## IPDC support for VoIP DTMF playout

In this release, the IPDC implementation in TAOS currently provides support for Dual Tone Multi-Frequency (DTMF) digit playout signalled by the STN message. It plays the DTMF digits utilizing a Digital Signal Processor DSP on the line card.

This functionality extends that support to also allow playout on a (DSP) on the MultiDSP card. Since a (DSP) on the MultiDSP card can be associated with a VoIP call route, the new capability allows a Softswitch to direct a MAX TNT to play the DTMF digits during an active VoIP call.

**Note:** Refer to *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15* specification for an explanation of all messages and tags that are referred to in this feature description.

## IPDC Changes

The sections that follow describes the IPDC messages, message tags and message values that are affected by the feature. Since the feature utilizes existing messages, tags and values, only those pertaining to this new feature are listed here.

## *STN Message*

The following changes were made in the STN message in IPDC to support this feature.

*Table 11. Tags for STN Message*

| <b>Tag</b>                   | <b>Description</b>                                                                       |
|------------------------------|------------------------------------------------------------------------------------------|
| Tag 0x49 (Tone Type)         | Specify the following value to play DTMF digits:<br>0x01 - DTMF tone                     |
| Tag 0x4A (Apply/Cancel Tone) | The following value is supported:<br>0x00 - Apply tone                                   |
| Tag 0x32 (Num Tones)         | The value associated with this tag indicates the number of DTMF digits to be played out. |
| Tag 0x33 (Tone String)       | The value associated with this tag contains the DTMF digits to be played out.            |

## *ASTN Message*

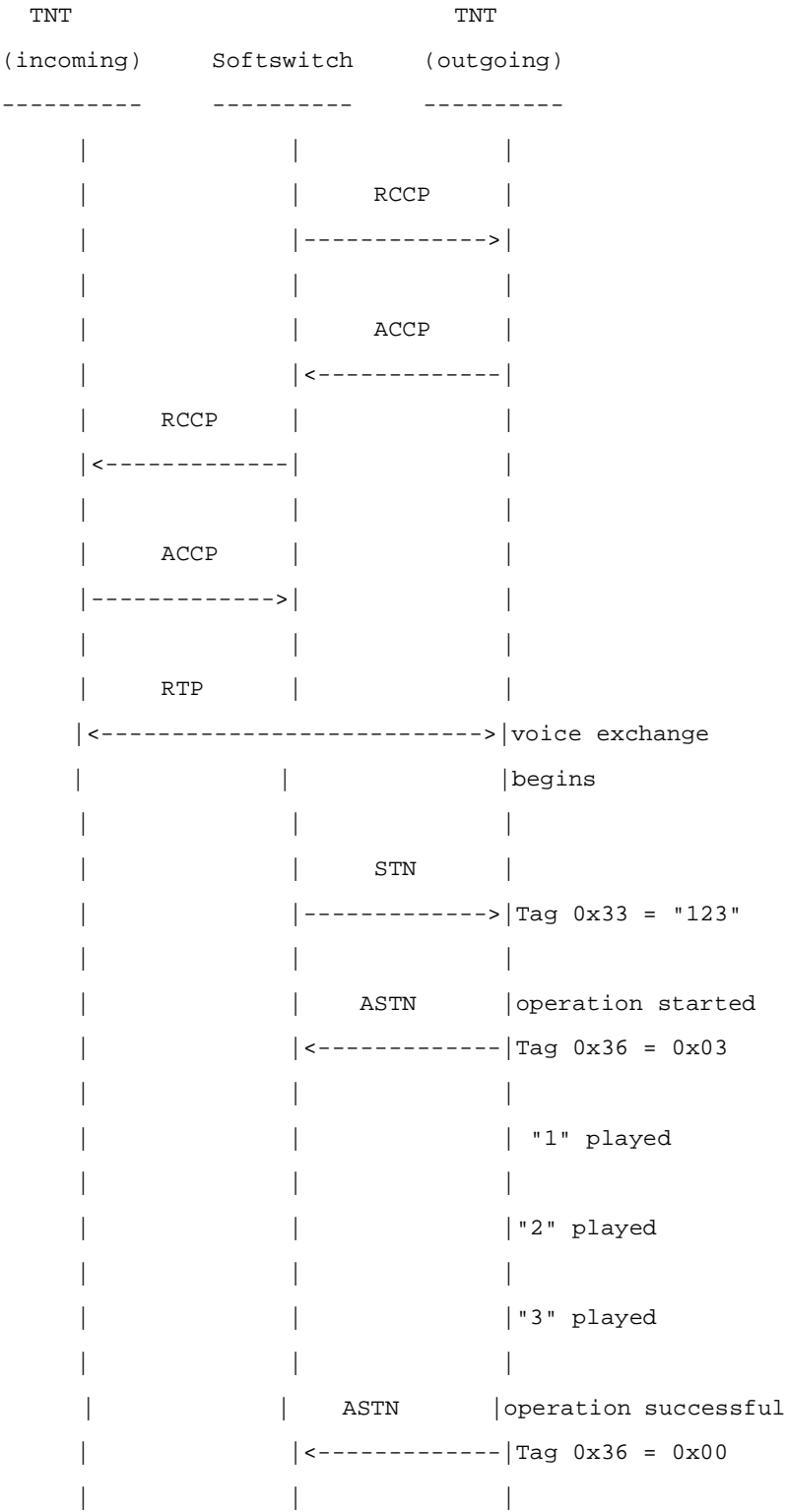
The following changes were made in the ASTN message in IPDC to support this feature.

*Table 12. Tags for ASTN Message*

| <b>Tag</b>                   | <b>Description</b>                                                                                                                                                                    |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tag 0x36 (Completion Status) | The following values are returned: <ul style="list-style-type: none"><li>• 0x00 - Operation successful</li><li>• 0x01 - Operation failed</li><li>• 0x03 - Operation started</li></ul> |

Call Flow - Basic Operation

The following call flow illustrates how the STN message is used to play DTMF digits during an active packet call. It shows a Softswitch setting up a packet call and then arbitrarily requesting that the MAX TNT at the far end play three DTMF digits: 1, 2 and 3.



## Call Flow - Out-of-band DTMF Transport

The following call flow illustrates how the DTMF playout feature is used in conjunction with the in-call DTMF detection feature to achieve true out-of-band DTMF transport using IPDC signalling.

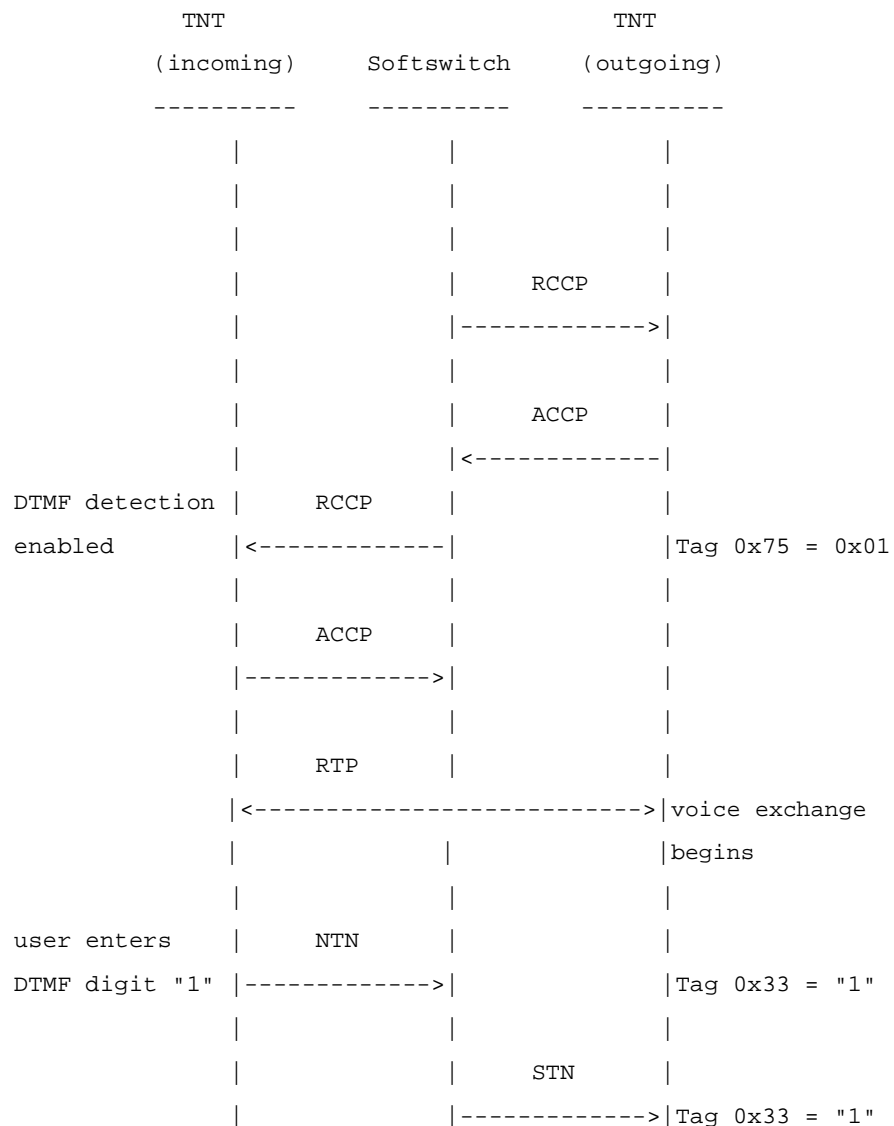
In this example, the call originator enters two DTMF digits, 1 and 2, after the voice exchange has begun. When performing out-of-band DTMF transport, it is necessary to remove the entered DTMF from the RTP stream. To do so, set the Voip profile on the MAX TNT(s) as follows:

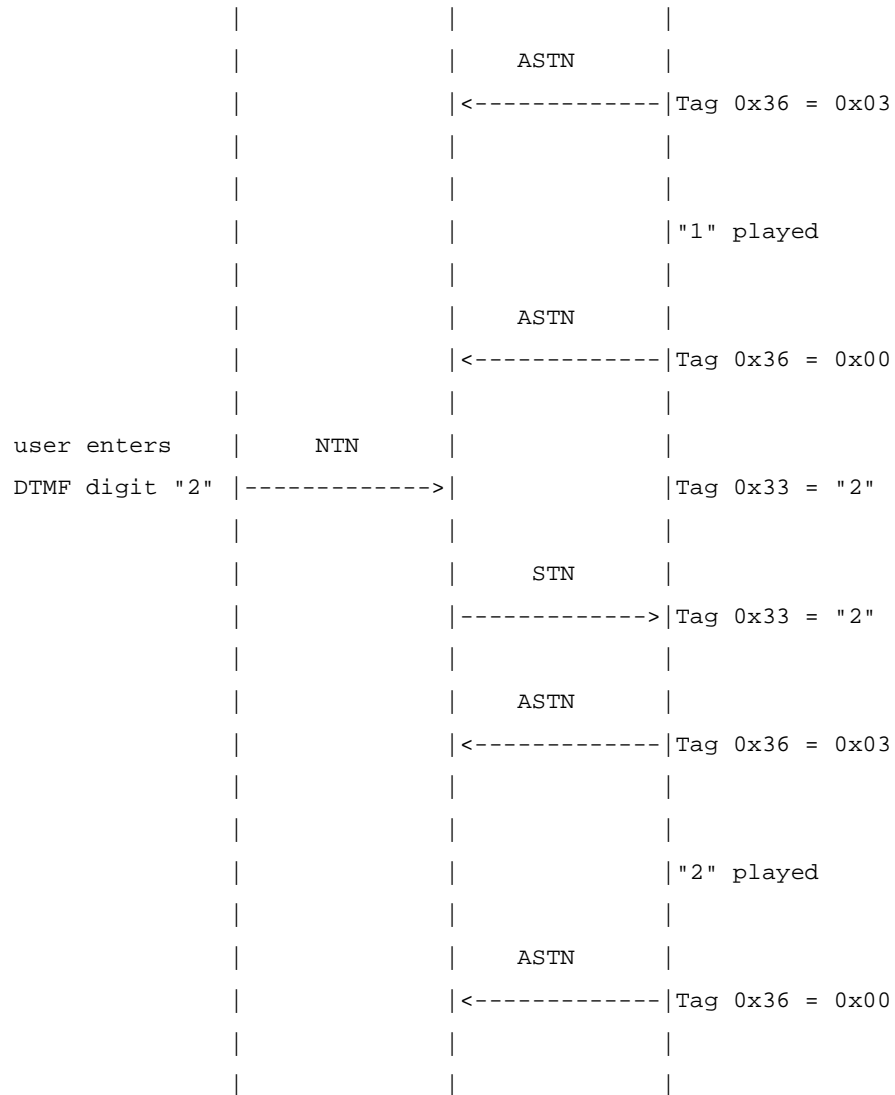
```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set dtmf-tone-passing = dtmf-tone-passed-outofband

admin> write
VOIP/{ 0 0 } written
```

The call flow for out-of-band DTMF transport is as follows:





## Notes

An STN request for DTMF playout over VoIP is accepted only for an active VoIP call in voice exchange mode. It is rejected for an active VoIP call that is performing pre-call DTMF collection, playing a pre-call announcement or playing a break-in announcement.

Only the apply command is allowed, cancel is not allowed.

The operation is allowed regardless of the setting of the dtmf-tone-passing parameter in the Voip profile, be it inband, out-of-band or rfc2833.

## **Error Handling**

In addition to the existing conditions whereby an STN request can be rejected, the following error responses are generated:

*Table 13. Error Handling*

| Softswitch will receive:                                         | For any of the following:                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MRJ with Tag 0xFE (Cause Code) = 0x65 (Wrong Message For State)  | <ul style="list-style-type: none"><li>• STN while a VoIP call is performing pre-call DTMF detection.</li><li>• STN while a VoIP call is playing a pre-call voice announcement.</li><li>• STN while a VoIP call is playing a break-in voice announcement.</li></ul> |
| ASTN with Tag 0x36 (Completion Status) = 0x01 (Operation Failed) | <ul style="list-style-type: none"><li>• STN with Tag 0x4A (Apply/Cancel Tone) = 1 (Cancel)</li></ul>                                                                                                                                                               |

## **Reporting call failures in cause codes**

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

## **Background**

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

## **Implementation Details**

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

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

## H.323 (v2) fastStart support

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

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

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

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

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

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

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

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

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

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

- Codec
- Rate
- RTP/RTCP addresses

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

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

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

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

- A separate H.245 channel

## Reverting to the H.245 connection

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

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

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

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

## H.245 call flow

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

- Cap exchange
- Master/slave determination

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

## Using fastStart with H.245 tunneling

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

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

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

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

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

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

---



## Terminating the H.323 V2 Fast Connect Procedure

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

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

## New Faststart Enable parameter

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

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

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

## Enabling fastStart

The following procedure illustrates how to enable fastStart:

```
tnt> set faststart-enable=yes
tnt> wri
```

**Example:** The following example shows how the fastStart-enable parameter is disabled:

```
tnt> set faststart-enable=no
tnt> wri
```

**Dependencies:** none

**Location:** VoIP profile

## External Interface Changes

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

## *H.323 Annex D T.38 Fax Support*

### Feature definition

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

## User Interface

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

To enable Fax mode:

- 1 Activate VoIp profile
- 2 Activate rt-fax-options subprofile
- 3 Enable Fax mode

To enable Fast Start for the Annex D FAX feature:

- 1 Activate VoIp profile
- 2 Activate faststart-enable
- 3 Configure to yes

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

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

## ***Additional Navis Support for RTP Payload Information***

### Feature definition

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

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

The RTP QoS feature can be observed in three factions: Polling, Call Logging, and IPDC.

- In polling, a VoIP profile parameter is introduced: `rtpqos-polling-enable`. When you activate this parameter, the i960 processor will request periodic statistics of the SARMS.
- In call logging, for each active call these statistics will be returned every 60 seconds, and once received, will forward the statistics to the call logging mechanism.
- For IPDC, one end-of-call statistic, Estimated Jitter, will be available for the IPDC signaling layer.

**Note:** This feature is available only on an MAX TNT, configured with MultiDSP cards.

## User Interface Changes

TAOS collects information periodically during the voice call; the general information content is described in Table 15.

**Note:** The RTP statistics set, sent to the STOP packet's call logging server, is enhanced through the addition of attributes into that packet. TAOS collects periodic information during voice calls. Table 14 is a description of this QoS information content.

Table 14. :Qos Information

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

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

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

For call logging and IPDC, N/A is appropriate.

Table 15. :Polling: MAX TNT/APX VoIP Profile user interface

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

## External Interface Changes

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

:

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

:

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

:

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

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

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

The following are statistics regarding Remote RTP Transmitter and Receiver:

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

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

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

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

## MultiVoice features in TAOS 9.1.0

### Additional Navis Support for RTP Payload Information

---

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

The end-of-call statistics are supported by two IPDC messages; the RCR and the ACR message:

#### *RCR Message*

Tag 0 x 99 (Estimated Latency): This tag is now added. It will contain a value estimating the latency (delay) measured during the call.

Tag 0 x A3 (Estimated Jitter): This tag is was already included with the end-of-call statistics, but its value is always set to 0. It will now contain a value estimating the jitter measured during the call.

#### *ACR Message*

Tag 0 x 99 (Estimated Latency): This tag is now added. It will contain a value estimating the latency (delay) measured during the call.

Tag 0 x A3 (Estimated Jitter): This tag is was already included with the end-of-call statistics, but its value is always set to 0. It will now contain a value estimating the jitter measured during the call.

# Problems corrected in TAOS 9.1.0

## *Data corrected problems*

The following Data trouble reports/problems have been corrected in this TAOS release.

|            |                                                                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TR 2493    | PIAFS call generated an unknown event MIB record.                                                                                                                                                                                                         |
| TR 5401    | An extra address free request would be sent when a PPP session went down.                                                                                                                                                                                 |
| TR 258886  | RADIUS: If a call on a modem using RADIUS failed calling line ID (CLID) authentication four times in a row, the modem was put on the list of suspect modems.                                                                                              |
| TR 6000541 | Outgoing modem calls failed with a message, "No Channel Avail" when modems and T1 channels were available.                                                                                                                                                |
| TR 6000657 | Acct-Authentic incorrectly logged as "Local" instead of as "Radius" for callback sessions authenticated by the Radius server.                                                                                                                             |
| TR 6000712 | IPCP incorrectly sent a Configure-Reject response instead of a Configure-Nak when an unacceptable value was specified by the client for DNS.                                                                                                              |
| TR 6000737 | Prior to having a connection profile activated such as a LAN session up, the "wandsess" debug command would not work if activated on a Hybrid Access III slot card (HDLC11), Series56 III Digital Modem slot card (CSM3V), and MultiDSP slot card (MADD). |
| TR 6000935 | Internal warnings 179 and 104 occurred on Series56 III Digital Modem (CSMX) and MultiDSP (MADD) cards.                                                                                                                                                    |
| TR 6000983 | Parameter "Dialout-Poison" in profile IP-GLOBAL would not disable IP dialout route advertising when no T1 trunk was available.                                                                                                                            |
| TR 6000997 | The netstat command incorrectly showed that tunnel0 was configured with a /22 netmask instead of the correct /32 netmask.                                                                                                                                 |
| TR 6001072 | RADIUS incorrectly logged truncated usernames when the name was longer than 39 characters.                                                                                                                                                                |

## Problems corrected in TAOS 9.1.0

### *Data corrected problems*

---

|                   |                                                                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>TR 6001084</i> | Certain client modems were experiencing connectivity problems with Series56 III Digital Modem slot cards (CSM/3V).                                                                                                                                                                                                        |
| <i>TR 6001089</i> | The PPTP control connection incorrectly stayed active after all sessions had disconnected.                                                                                                                                                                                                                                |
| <i>TR 6001097</i> | Frame Relay interface would report incorrect or missing information if queried via SNMP twice in 3 seconds.                                                                                                                                                                                                               |
| <i>TR 6001167</i> | AM36 Modem could be stuck in online mode event after the session was disconnected.                                                                                                                                                                                                                                        |
| <i>TR 6001168</i> | The callback feature wouldn't work when connecting to an ASG 3.x                                                                                                                                                                                                                                                          |
| <i>TR 6001179</i> | IPX pings over a WAN interfaced did not work.                                                                                                                                                                                                                                                                             |
| <i>TR 6001185</i> | FTP transfers failed when using L2TP over Frame Relay.                                                                                                                                                                                                                                                                    |
| <i>TR 6001226</i> | Too many 185/41 cause codes were logged for AOL tcp-clear connections.                                                                                                                                                                                                                                                    |
| <i>TR 6001264</i> | Telnet protocol violated RFC 854 by incorrectly responding to all DO requests with a WILL response when both sides of the connection had the same RFC 854 violation.                                                                                                                                                      |
| <i>TR 6001265</i> | A zero length Framed_Route RADIUS attribute was sent to the TAOS unit. A "warning 109" was generated because a zero length memory allocation request had been issued. For all coredump warnings that are hardwired 101-to-121 the slot card will be reset.                                                                |
| <i>TR 6001267</i> | Incorrect cause code numbers reported in LAN session info.                                                                                                                                                                                                                                                                |
| <i>TR 6001270</i> | If a MAX TNT was configured as an L2TP Access Concentrator with Proxy LCP and the authentication feature, it would receive a PAP-Authenticate-Request with a Request-ID = 0. This MAX TNT would then send an ICCN (Incoming Call Connected) message to the LNS with a Proxy-Authen-ID(32) = 1. This was an RFC violation. |
| <i>TR 6001300</i> | Empty RADIUS attribute 213 was being sent in violation of RFC 2865.                                                                                                                                                                                                                                                       |
| <i>TR 6001314</i> | TCP-Clear connections that authenticate via DNIS report only a series of questions marks as the username when logging to a RADIUS server.                                                                                                                                                                                 |

---



|                   |                                                                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>TR 6001330</i> | Value incorrectly set for L2TP attribute 0x026 (38) receive connect speed.                                                                      |
| <i>TR 6001360</i> | An end-of-call record was not being produced when a V110/PHS/modem call terminated.                                                             |
| <i>TR 6001419</i> | When idle timeout occurred, a TAOS unit would send a Terminate-Request followed by a CBCP packet, even when CBCP was disabled.                  |
| <i>TR 6001443</i> | Username was missing from syslog when a tunnel failed to establish.                                                                             |
| <i>TR 6001444</i> | L2TP username was truncated in syslog messages if it was longer than 31 characters.                                                             |
| <i>TR 6001449</i> | SNTP configuration lacked UTC+1300 setting for New Zealand Daylight Savings.                                                                    |
| <i>TR 6001451</i> | MRU setting in Answer Defaults was not used when CLID/DNIS pre-auth was specified.                                                              |
| <i>TR 6001458</i> | An egress gateway would incorrectly report normal call clearing instead of busy status.                                                         |
| <i>TR 6001475</i> | A MAX TNT sometimes reset giving a Warning 104 message when receiving IPDC STN messages.                                                        |
| <i>TR 6001507</i> | R1-inband signalling required FGD to be enabled.                                                                                                |
| <i>TR 6001561</i> | Syslog did not report the fact that an L2TP tunnel was established.                                                                             |
| <i>TR 6001568</i> | A warning 179 sometimes occurred after reset when a <code>slot -d</code> and a <code>slot -r</code> command is performed on an HDLC2 slot card. |
| <i>TR 6001582</i> | The shelf controller sometimes reset several times per day.                                                                                     |
| <i>TR 6001592</i> | There was an incomplete coredump of a shelfcontroller when connected to a Cisco router over ethernet.                                           |
| <i>TR 6001600</i> | Channels got blocked when E1-R2 signalling was used on an E1 line.                                                                              |
| <i>TR 6001606</i> | The T1 Inband Timer sometimes expired and an answer signal would then not be sent when True Connect was enabled.                                |

## Problems corrected in TAOS 9.1.0

### Data corrected problems

---

|                   |                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>TR 6001609</i> | L2F Idle Timeout terminated the session even if traffic was being sent over that connection.                                                                            |
| <i>TR 6001641</i> | SNMP login incorrectly reported a zero value for eventInOctets and eventOutOctets when using either telnet or TCPRaw                                                    |
| <i>TR 6001653</i> | A MAX TNT with a DS3-ATM card sometimes experienced gradual performance degradation.                                                                                    |
| <i>TR 6001692</i> | The boot-sr parameter was set to a null value after restoring the SYSTEM profile.                                                                                       |
| <i>TR 6001704</i> | The TAOS unit reported an incorrect NAS-Port-Type when logging to a RADIUS accounting server.                                                                           |
| <i>TR 6001708</i> | Bouncing the secondary D channel in an NFAS group reset all channels in group.                                                                                          |
| <i>TR 6001717</i> | There was no way to make L2TP accept an unencrypted password.                                                                                                           |
| <i>TR 6001737</i> | Modems sometimes got stuck in a connected state and were not available for subsequent connections.                                                                      |
| <i>TR 6001762</i> | The refresh -n command did not correctly update all permanent connections until it was executed a second time.                                                          |
| <i>TR 6001778</i> | Rebooting a Cisco terminal server when it was connected to the console port of a shelf controller reset the shelf controller.                                           |
| <i>TR 6001832</i> | A Warning 179 occurred when a TAOS unit received many SNMP queries.                                                                                                     |
| <i>TR 6001861</i> | When a TAOS unit had auth-radius-compatible set to 16-bit-vendor-specific the unit failed to send an access-request out when attempting to authenticate a dial-in user. |
| <i>TR 6001881</i> | A configuration involving ATMP and IPX caused FE36 resets on a unit with one or more SWAN cards.                                                                        |
| <i>TR 6001900</i> | EMEA: Incomplete MIF command caused the MAX TNT to reset with W330 & FE1.                                                                                               |
| <i>TR 6001901</i> | It was possible to set the Frame Relay MRU to 1600 even if the system supported a maximum MRU of 1524.                                                                  |

---

---

|            |                                                                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| TR 6001912 | When an ether3/3rd interface changed state to link UP or link DOWN, there was no console or syslog message generated to reflect this status change.      |
| TR 6001975 | A Warning 179 occurred on CSMV3 slot cards when communication was interrupted while transmitting data.                                                   |
| TR 6002010 | A TAOS unit sometimes sent NMS messages with a Number-of-Lines parameter (0x20) but not a Line Status Array parameter (0x21).                            |
| TR 6002052 | SS7/Q.931+Service: When the switch took an E1 line out of service, users with a status of "call-on-busy" were released and not restored back to service. |
| NA         | Username longer than 127 characters was not authenticated by TACACS+.                                                                                    |

## ***MultiVoice corrected problems***

The following MultiVoice trouble reports/problems have been corrected in this TAOS release.

|            |                                                                                                                                                                                                                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA         | The hairpin failed when trunk groups were in use. Current hairpin functionality and previous release bugs need to be documented.                                                                                                                                                                                                                             |
| NA         | The VoIP system sent erroneous and confusing progress code and cause codes to syslog.                                                                                                                                                                                                                                                                        |
| NA         | Significant failure rate of calls occurred between the Cisco gateway to the MAX TNT, where gateway routing included a third-party Alcatel gatekeeper.                                                                                                                                                                                                        |
| NA         | There was need to configure the number of retries for PIN and DNIS in the VoIP profile, where there was originally no capability.                                                                                                                                                                                                                            |
| NA         | Break-in announcements played improper messages in response to certain dialing or announcement conditions. Hanging up during an announcement triggered the "You have entered an invalid number..." message. When the called phone hung up, the entire break-in announcement was replayed, indicating that the wrong message might be in the queue or buffer. |
| NA         | Hanging up the called phone during a break-in announcement generated an error message (two-stage call with PIN on TNT38, terminating on TNT 39, with originating gateway reporting error).                                                                                                                                                                   |
| TR 6001324 | When using the MAX TNT, with a third-party Alcatel gatekeeper generating 10 simultaneous calls at 60 seconds each, repeating every 90 seconds, WARNING 109 and Index 385 occurred.                                                                                                                                                                           |

---

## Problems corrected in TAOS 9.1.0

### *MultiVoice corrected problems*

---

|                   |                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>TR 6001516</i> | Using G.728, no busy signal is heard for a busy call. Using G.729, a busy-buzz-busy signal is heard.                                                                                                                                                                                                                                                                                     |
| <i>TR 6001488</i> | Arbitrary announcement was cut-off when call is connected.                                                                                                                                                                                                                                                                                                                               |
| <i>NA</i>         | An announcement specified in a disengage request (DRQ) was not played on the ingress gateway.                                                                                                                                                                                                                                                                                            |
| <i>NA</i>         | An announcement that is supposed to be continuous only played once from its gateway.                                                                                                                                                                                                                                                                                                     |
| <i>NA</i>         | An error in the process of receiving IRR resulted in multiple transmissions of IRQs.                                                                                                                                                                                                                                                                                                     |
| <i>TR 6001292</i> | Ingress PSTN call was not dropped properly in GateKeeper Router Mode.                                                                                                                                                                                                                                                                                                                    |
| <i>TR 6000923</i> | H.323 call ID was not unique during a GateKeeper routed call.                                                                                                                                                                                                                                                                                                                            |
| <i>TR 6000964</i> | Protection violation messages from Enet-3 card using 8.0.3.                                                                                                                                                                                                                                                                                                                              |
| <i>TR 6001496</i> | E1/R2 - links remain seized after called party hangs up. When B party hangs up and A party remains in the call, the channels remain seized without a end-of call time out (120 seconds).                                                                                                                                                                                                 |
| <i>TR 6001498</i> | E1/R2 - Fix sending of calling subscriber category & I-15/I-12 signaling. It is not possible to discriminate at the destination the subscriber type or category of the originating party (common subscriber, testing equipment, payphone, etc.) because the TAOS unit always sends the "common subscriber " indication no matter the subscriber category sent by the originating switch. |
| <i>TR 6001606</i> | E1/R2 calls complete, but line signaling for an ANSWER was not sent back if True Connect was enabled and the called party did not answer within 10 seconds.                                                                                                                                                                                                                              |
| <i>TR 6001095</i> | Gateway continuously calls to phone that has been forwarded to the Gateway. When the same call ID was reused, the Gateway thought this was another redirecting call to that same phone.                                                                                                                                                                                                  |
| <i>TR 6001259</i> | Busy Signal not played when cause codes were not enabled.                                                                                                                                                                                                                                                                                                                                |
| <i>TR 6001458</i> | Egress GW populated P26 with CC = 16 for a busy call. This resulted in a stop record that shows normal call clearing for this call. The behavior for the ingress Gateway is normal.                                                                                                                                                                                                      |

---

*TR 6001499*

The TAOS unit can drive variable length numbering plans using the I-15 signal or Time-Out as "end of number". When a TAOS unit was configured to use "number-complete = time-out", and "caller-id = get-caller-id", the TAOS unit can't complete the signaling dialog and dropped the call.