



MultiVoice® for APX™/MAX TNT®

Configuration Guide


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.

European Community (EC) RTTE compliance

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

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

Safety, compliance, and warranty Information

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

Security statement

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

Trademarks

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

Ordering Information

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

Feedback

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

.

Customer Service

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

Finding information and software

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

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

Obtaining technical assistance

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Contents



Customer Service	iii
About This Guide	xvii
What you need to know	xvii
Documentation set	xviii
Related publications	xx
 Chapter 1 Introducing MultiVoice Concepts	 1-1
The public switched telephone network	1-1
The MultiVoice network	1-2
Multivoice terms and definitions	1-2
MultiVoice packet processing	1-4
Supported audio codecs	1-4
H.323 implementation	1-5
Integrating PSTN and packet networks	1-6
Overlapping gateway coverage areas	1-7
Using primary and secondary gatekeepers	1-8
Increasing gatekeeper reliability	1-9
How calls are assigned to a MultiVoice gateway	1-12
MultiVoice networks supporting multizone call routing	1-13
Routing across H.323 zones	1-13
Implementing call routing	1-13
IP Device Control implementation	1-14
Overview of the signaling gateway	1-15
IPDC call processing messages	1-17
MultiVoice integration with frame relay networks	1-18
MultiVoice applications	1-18
1+ dialing for residential long distance	1-18
MultiVoice solution features	1-19
Authentication and voice announcements	1-19
Local toll-free service	1-20
Traditional toll-freeservice	1-20
Using MultiVoice with local toll-free service	1-20
Postpaid and prepaid calling-card service	1-21
PC-to-phone calls	1-22
H.323-compliant terminals	1-22
Gateway-to-client keep-alive registration	1-22
Phone-to-PC (also known as Internet call waiting)	1-23
Single-stage, 1+ dialing with interconnection using PSTN or VoIP	1-24
MultiVoice solution features	1-24

Chapter 2	MultiVoice Gateway Configuration.....	2-1
System configuration		2-1
Base profile parameters		2-2
Configured memory requirements		2-3
Using slot cards in a MultiVoice Gateway		2-3
MultiDSP slot cards.....		2-3
Mixing MultiDSP slot cards.....		2-3
Slot card restrictions.....		2-4
Cohabitation on a single DSP		2-4
Ethernet-3 slot card		2-5
Enabling full-duplex mode.....		2-5
Configuring connecting ports on the packet switch or router		2-5
Creating a default network gateway route.....		2-6
System configuration parameters.....		2-6
Assigning identifiers to trunk groups		2-7
Allowing sufficient time to establish the connection		2-7
Setting the number of simultaneous outgoing calls.....		2-7
Generating country-specific call progress tones		2-7
Identifying MultiVoice Gateways on the network.....		2-8
Detecting and responding to misdirected ICMP packets		2-10
Preventing the redirection of UDP packets to the shelf controller		2-10
Preventing premature fax/modem call time-outs		2-11
device-state profiles		2-12
Implementing VoIP audio processing.....		2-12
Configuring VoIP call processing.....		2-13
Creating the default voip profile.....		2-13
Configuring routes for VoIP call processing		2-13
Call routing parameters.....		2-14
Configuring egress call routing.....		2-23
Priority-based call routing.....		2-25
Priority based call routing		2-25
Resetting the slot card		2-27
Configuring IP routing for H.323 call processing.....		2-28
IP addressing schemes		2-29
Packet routing for H.323 VoIP calls.....		2-29
Configuring host routes.....		2-29
Configuring network routes.....		2-31
Configuring routes for IPDC VoIP call processing.....		2-36
Configuring IP routing for IPDC call processing		2-37
Packet routing for IPDC VoIP calls controlled from the signaling gateway		2-37
Using RMCP/AMCP messages to route VoIP calls.....		2-39
Reporting IPDC VoIP call statistics.....		2-42
Supported tags for reporting statistics		2-42
Unsupported tags for reporting statistics		2-43
Call statistics reporting		2-43
ss7nmi debug-level command.....		2-44
Verifying IP route configuration		2-44
Verifying VoIP port caches.....		2-44
Verifying VoIP route caches.....		2-45
Trunk configuration		2-46

Interoperating with an SS7 signaling gateway using IPDC	2-46
Using the ss7-gateway profile.....	2-46
Transport-options subprofile	2-47
Configuring an IP interface to the signaling gateway	2-48
Configuring T1 or E1 lines as SS7 data trunks	2-49
Configuring PRI Tunneling in IPDC (IPDC 0.15)	2-50
Configuring trunk signaling for H.323 VoIP networks	2-54
Enabling DTMF R2 signaling for E1 lines.....	2-57
Enabling and debugging Feature Group D signaling support for T1 lines.	2-58
Enabling collections of variable length dial strings without EOP	2-61
Processing ANI and DNIS for H.323 VoIP	2-64
Configuring 480 ports for G.711-encoded VoIP-only calls	2-65
Transparent fax and modem.....	2-65
Compatibility with other MultiDSP slot cards	2-65
New value for subtype parameter.....	2-66
Configuring the slot card for 480 ports	2-66
Resetting the slot card	2-66
Reverting to universal port mode	2-67
In-call DTMF detection for IPDC.....	2-67
IPDC messages that support in-call DTMF detection.....	2-68
Call Flow.....	2-68
Interaction with break-in voice announcements	2-69
Call re-origination.....	2-70
End-of-call break-in voice announcements.....	2-71
DTMF payout for IPDC.....	2-73
IPDC messages that support DTMF payout	2-74
Basic call flow for DTMF digits played during a packet call.....	2-74
Call flow for out-of-band DTMF transport	2-75
Error Handling	2-77
IPDC country-specific call-progress tone payout for VoIP	2-77
STN message that supports country-specific call-progress tones	2-77
Tag 0x49 (tone type)	2-77
Tag 0xC1 (Country Identifier).....	2-78
STN/ASTN usage	2-79
Sample Call Flows — ringing, then answered scenario	2-79
 Chapter 3 VoIP Call Configuration	 3-1
The voi p profile.....	3-1
Creating DNIS-specific voi p profiles.....	3-7
Configuring call-performance parameters	3-8
Configuring voice compression.....	3-9
G.728 codec support.....	3-10
G.723.1 codec support.....	3-10
Full-Rate GSM codec support.....	3-11
Configuring voice packet size	3-11
Configuring audio codec negotiation.....	3-12
Configuring silence detection and comfort noise generation	3-13
Adjusting the relative silence threshold	3-14
Configuring dynamic call jitter buffers	3-14
Enabling the adaptive jitter buffer	3-14
Configuring the maximum jitter buffer size.....	3-15

Configuring the initial jitter buffer size	3-15
Type of Service (TOS) or Differentiated Service Codepoint (DSCP) marking .	3-16
Type of Service marking.....	3-16
Differentiated Services Codepoint marking.....	3-18
Controlling VoIP call volume.....	3-20
Maxcalls parameter	3-20
Exceeding the maximum call volume	3-21
Configuring H.323 (v2) fastStart	3-21
fastStart vs. standard H.245 procedure	3-21
H.323 (v2) fast connect call flow.....	3-21
Reverting to the H.245 connection	3-22
H.245 call flow	3-22
Using fastStart with H.245 tunneling.....	3-22
Terminating the H.323 V2 Fast Connect Procedure.....	3-23
faststart-enable parameter.....	3-23
Configuring H.323 call management parameters.....	3-23
H.323 gatekeeper communication.....	3-24
Identifying the primary gatekeeper.....	3-24
Identifying a secondary gatekeeper.....	3-25
Setting gateway registration policy	3-25
Setting reregistration policy	3-26
Reporting trunk capacity to the gatekeeper	3-28
H.323 call signaling.....	3-29
Controlling call-progress tones on a local gateway	3-29
Controlling transmission of call-progress tones to the PSTN	3-30
Rerouting DTMF signals.....	3-31
Blocking Caller ID on a local gateway.....	3-33
Enabling keep alive registration between calling end points	3-33
Enabling transparent fax/modem operations.....	3-34
Deactivating trunks used for VoIP calls.....	3-36
Configuring PSTN call signaling	3-37
Multiple Logical Gateways	3-44
Setting H.323 dialing options.....	3-50
Adjusting and troubleshooting the interdigit timer	3-50
Configuring single-stage dialing.....	3-52
Rerouting blocked calls over the local PSTN.....	3-53
Requesting operator assistance.....	3-53
Enabling early ringback.....	3-54
Enabling trunk prefixing	3-55
Configuring PIN collection	3-56
Enabling sequential calls for PIN authentication	3-56
Enabling sequential dialing (H.323 caller originated disconnect)	3-57
Generating RTP QoS statistics	3-58
Gatekeeper CLID substitution	3-59
Configuring two-stage dialing in SS7 networks.....	3-59
VoIP call persistence	3-59
ss7voip-call-persistence parameter	3-60
SS7 VoIP call persistence timer.....	3-60
Interdigit DTMF timer.....	3-61
ss7voip command enhancements.....	3-61
ss7nmi command enhancements.....	3-61
Supported messages and tags.....	3-62

IPDC Packet.....	3-62
LTN message.....	3-62
ALTN message	3-63
ALTN as a response to LTN	3-63
Sample call flow	3-63
ALTN as a response to LTN-cancel	3-64
Sample Call Flow.....	3-64
STN message.....	3-65
ASTN message	3-65
Notes on using LTN/STN messages.....	3-65
Summary of Nonstandard IPDC Behavior	3-65
Call flows—VoIP call-persistence mode enabled.....	3-66
Using H.323 authentication	3-70
Call processing using no authentication	3-71
Call processing using PIN authentication	3-72
Call processing using ANI authentication.....	3-72
 Chapter 4 Voice Announcement Administration	4-1
Using voice announcements	4-1
How voice announcements work	4-1
Voice announcements for time-measure billing plans	4-2
Multiple voice announcements	4-2
Audio file requirements.....	4-3
Voice announcement guidelines.....	4-4
Voice announcement file names	4-4
Enabling voice announcements	4-5
Enabling voice announcements for IPDC calls	4-5
STN Message	4-6
Break-in voice announcements in IPDC	4-6
Enabling voice announcements for H.323 calls.....	4-8
Enabling G.711 m-Law or G.729 encoding	4-9
Creating voice announcements.....	4-10
Formatting flash cards.....	4-10
Creating the voice announcements directory	4-11
Displaying voice announcement files.....	4-12
Voice announcement log messages.....	4-12
 Chapter 5 MultiVoice Real-time Fax.....	5-1
Real-time fax processing	5-1
H.323 Annex D T.38 fax support.....	5-1
Real-time fax configuration	5-2
Base profiles	5-2
Rt-fax-options sub-profile.....	5-2
Routing fax calls	5-4
Using error correction mode (ECM)	5-4
Enabling packet redundancy	5-5
Disabling Packet Redundancy	5-6
Verifying H.323 fax call operations.....	5-7
IPDC message support for real-time fax and transparent modem.....	5-8
Transparent data	5-8
T.38 fax.....	5-8

Echo canceller	5-8
Notify tone (NTN)	5-9
Changes to existing message tags	5-9
RCCP, ACCP, RMCP, and AMCP message tags	5-10
New NTN message tags	5-10
ss7nmi command	5-11
Max Data Transmission Rate Configuration	5-12
Setting the max-data-rate parameter	5-12
Fax session detection	5-13
Fax compatibility	5-14
Chapter 6 Network Reporting	6-1
Network reporting options	6-1
Base profile parameters	6-1
Enabling SNMP traps for MultiVoice	6-1
The VoIP MIB (ascend 28)	6-2
Sending H.323 call information to SNMP log clients	6-4
Billing start records	6-4
Billing stop records	6-5
Call disconnect records	6-5
Fax start records	6-7
H.323 disconnect reasons	6-7
NavisAccess™ support for VoIP call reporting	6-8
Start records	6-9
Stop records	6-10
Call progress records	6-11
NavisAccess™ support for RTP payload information	6-11
Call logging STOP packet	6-12
Remote RTP transmitter and receiver	6-13
End-of-call statistics	6-14
Reporting cause codes to MVAM	6-14
Release codes	6-14
Reporting Q.931 messages	6-16
Modifications to the ss7asg command	6-16
Displaying extended information	6-17
Reporting call failures in cause codes	6-18
Background	6-18
Implementation Details	6-18
Calculating and reporting packet jitter	6-19
Q.931 messaging for SS7 V.110 calls	6-19
Supported Q.931 bearer capability requests	6-20
Octet 5a information element	6-20
Appendix A MultiVoice Packet Processing	A-1
MultiVoice packet format	A-1
Packet sizes by audio codec	A-2
Appendix B Determining Jitter Buffer Size	B-1
Dynamic jitter buffers	B-1
Index	Index-1

Figures

Figure 1-1	Example of call routing over circuit-switched PSTN.....	1-1
Figure 1-2	MultiVoice packet format	1-4
Figure 1-3	Example of a MultiVoice network	1-6
Figure 1-4	Example of a MultiVoice network with overlapping coverage areas	1-8
Figure 1-5	Example of a MultiVoice network with a secondary gatekeeper	1-9
Figure 1-6	Reciprocal secondary gatekeepers.....	1-10
Figure 1-7	Global secondary gatekeeper	1-10
Figure 1-8	Example of a MultiVoice network supporting multizone call routing	1-14
Figure 1-9	The Signaling gateway using IPDC implementation.....	1-16
Figure 1-10	Sample MultiVoice network	1-18
Figure 1-11	Traditional toll-free environment	1-20
Figure 1-12	Using MultiVoice with local toll-free service	1-21
Figure 1-13	Virtual private network using PC telephony	1-22
Figure 2-1	Example IPDC message exchanges	2-41
Figure A-1	MultiVoice packet format	A-1

Tables

Table 1-1	IPDC VoIP call processing messages.....	1-17
Table 2-1	System configuration parameters	2-6
Table 2-2	Call-route types.....	2-18
Table 2-3	Default cost values	2-26
Table 2-4	How Calls are Routed Using Cost Values.....	2-27
Table 2-5	IP address table for TAOS unit-173.....	2-30
Table 2-6	IP Routing table for host routes from TAOS unit-173 to TAOS unit-196	2-30
Table 2-7	Host route IP address table for TAOS unit-196.....	2-31
Table 2-8	Host route IP Route table for TAOS unit-196	2-31
Table 2-9	Network route IP address table for TAOS unit-173	2-32
Table 2-10	Network route IP Route table for TAOS unit-173	2-32
Table 2-11	Network route IP Route table for network router	2-33
Table 2-12	Network route IP address table for TAOS unit-196	2-33
Table 2-13	Network route IP Route table for TAOS unit-196	2-34
Table 2-14	Network route IP Route table for network router	2-34
Table 2-15	Static route parameters.....	2-36
Table 2-16	Ethernet IP address table for TAOS unit-173.....	2-38
Table 2-17	Supported Statistics Tags (IPDC 0.12)	2-42
Table 2-18	Unsupported Statistics Tags (IPDC 0.12).....	2-43
Table 2-19	IPDC messages supporting in-call DTMF detection and generation	2-68
Table 2-20	IPDC messages supporting DTMF playout	2-74
Table 2-21	Error handling.....	2-77
Table 3-1	Trunk Messages.....	3-49
Table 3-2	Digits	3-52
Table 4-1	Guidelines for voice announcements.....	4-4
Table 4-2	File names for voice announcements	4-4
Table 4-3	Error/log messages	4-12
Table 4-4	Warning messages.....	4-13
Table 5-1	Base profile parameters.....	5-2
Table 5-2	Events reported by the <i>h323debug</i> command.....	5-7
Table 5-3	Modified NTN message tag values.....	5-9
Table 5-4	Modified RCCP, ACCP, RMCP and AMCP message tag values.....	5-10
Table 5-5	New the RCCP, ACCP, RMCP and AMCP message tag values	5-10
Table 5-6	New NTN message	5-11
Table 5-7	Notify Tone message tags	5-11
Table 5-8	Detection ranges	5-14
Table 6-1	Qos Information.....	6-12
Table 6-2	Reported Q.931 Cause codes	6-15
Table 6-3	Reported H.225 Cause codes.....	6-16

About This Guide

This guide provides instructions on how to configure an APX™ or MAX TNT® to process MultiVoice voice over IP (VoIP) calls.



Note This manual describes the full set of features for units running software version TAOS 10.0. Some features might not be available with earlier versions or specialty loads of the software.

The APX family of products includes multiple platforms that differ in call capacity and hardware, but support the same operating system and similar configuration options. The APX family, which includes the APX 8000 and APX 1000 products, shares many features with its MAX TNT predecessor. For features that are supported with no differences across all the platforms, this manual often refers to your product as a *TAOS unit*.







Warning Before installing your unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see the “Safety-Related Electrical, Physical, and Environmental Information” appendix in your unit’s hardware installation guide or *Getting Started Guide*.

What you need to know

This manual is intended for the person who configures and maintains your TAOS unit running MultiVoice. To use the manual effectively, you must have a basic understanding of security and configuration, and be familiar with authentication servers and networking concepts. You also need to understand Internet and telecommuting concepts and dial-in connections (both framed protocol sessions and user logins).

Following are the special characters and typographical conventions used in this manual:

Convention	Meaning
<code>Mnospa ce text</code>	Represents text that appears on your computer’s screen, or that might appear on your computer’s screen.
Boldface monospace text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , following). If you can enter the characters but are not specifically instructed to, they do not appear in boldface.

Convention	Meaning
<i>Italics</i>	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[]	Indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
	Separates command choices that are mutually exclusive.
>	Separates levels of profiles, subprofiles, and parameters in a hierarchical menu when the path to a menu item is referred to in text.
:	Separates levels of profiles, subprofiles, and parameters in a pathname displayed in the command-line interface or referred to in text.
Key1+Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl+H means hold down the Ctrl key and press the H key.)
Press Enter	Means press the Enter or Return key or its equivalent on your computer.
	Introduces important additional information.
Note:	
	Warns that a failure to follow the recommended procedure can result in loss of data or damage to equipment.
Caution:	
	Warns that a failure to take appropriate safety precautions can result in physical injury.
Warning:	
	Warns of danger of electric shock.
Warning:	

Documentation set

The documentation set for APX and MAX TNT products consists of the following manuals, available at <http://www.lucent.com/support> and <http://www.lucentdocs.com/ins>:

- **Read me first:**

- *Edge Access and Broadband Access Safety and Compliance Guide*. Contains important safety instructions and country-specific compliance information that you must read before installing a unit.
- *TAOS Command-Line Interface Guide*. Introduces the TAOS command-line environment and shows how to use the command-line interface effectively. This manual describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.
- **Installation and basic configuration:** *Getting Started Guide* or hardware installation guide for your unit. Shows how to install the unit's chassis and hardware, and includes technical specifications. A *Getting Started Guide* also shows you how to provide the basic configuration needed to access the unit on a network.
- **Configuration:**
 - *Physical Interface Configuration Guide* for your unit. Describes how to provision the slot cards supported in the unit, and how to configure the cards' physical interfaces. This guide also describes system allocation of slot card resources, and how to use the supported cards in a variety of data environments.
 - *APX/MAX TNT ATM Configuration Guide*. Describes how to configure Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) and switched virtual circuit (SVC) ATM interfaces. It includes information about ATM direct and ATM-frame relay circuits.
 - *APX/MAX TNT Frame Relay Configuration Guide*. Describes how to configure frame relay operations on a unit. This guide explains physical layer restrictions and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) interfaces. It includes information about Multilink frame relay (MFR) and link management, as well as frame relay and frame relay direct circuits.
 - *APX/MAX TNT WAN, Routing, and Tunneling Configuration Guide*. Shows how to configure LAN and WAN routing for analog and digital dial-in connections on a unit. This guide includes information about IP routing, Open Shortest Path First (OSPF) routing, Border Gateway Protocol (BGP) routing, Internet Group Management Protocol (IGMP) routing, multiprotocol routers, virtual routers (VRouters), and tunneling protocols.
- **MultiVoice:**
 - *MultiVoice® for APX/MAX TNT Configuration Guide*. Shows how to configure the MultiVoice® application to run on a unit in both Signaling System 7 (SS7) and H.323 Voice over IP (VoIP) configurations.
 - *MultiVoice Access Manager User's Guide*. Describes the installation, configuration, and administration of MultiVoice Access Manager, which provides H.323 gatekeeper functions for MultiVoice networks.
- **RADIUS:** *TAOS RADIUS Guide and Reference*. Describes how to set up a unit to use the Remote Authentication Dial-In User Service (RADIUS) server, and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *APX/MAX TNT Administration Guide*. Describes how to administer a unit, including how to monitor the system and cards, troubleshoot the unit, and configure the unit to use the Simple Network Management Protocol (SNMP).

- **Reference:**

- *APX/MAX TNT Reference*. An alphabetic reference to all commands, profiles, and parameters supported on a unit.
- *TAOS Glossary*. Defines terms used in the documentation for a unit.

Related publications

This guide and documentation set do not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations. Following are some publications that you might find useful:

- ITU Telecommunication sector standard (ITU-T) H.323, *Packet-based multimedia communications systems* (Feb. 1998), International Telecommunications Union.
- RFC 1889, *RTP: A Transport Protocol for Real-Time Applications* (Jan. 1996), IETF.
- RFC 2705, *Media Gateway Control Protocol (MGCP)* (Oct. 1999), IETF.
- *Signaling in Today's Telecommunication Networks*, John G. van Bosse.
- *Delivering Voice over IP Networks*, Dan Minoli, Emma Minoli, Daniel Minoli.
- *Delivering Voice Over Frame Relay and ATM*, Dan Minoli.
- *The Guide to T1 Networking*, William A. Flanagan.
- *TCP/IP Illustrated*, W. Richard Stevens.
- *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin.

Following are some related World Wide Web (WWW) sites:

- <http://www.ietf.org/rfc>
- <http://www.itu.ch/>
- <http://www.cs.columbia.edu/~hgs/rtp/drafts/VoIP97-8.pdf>
- <http://www.cs.columbia.edu/~hgs/rtp/>



Note The listed web sites were available at the time of this manual's publication. Lucent does not maintain these sites and cannot guarantee their availability in the future.

Introducing MultiVoice Concepts

1

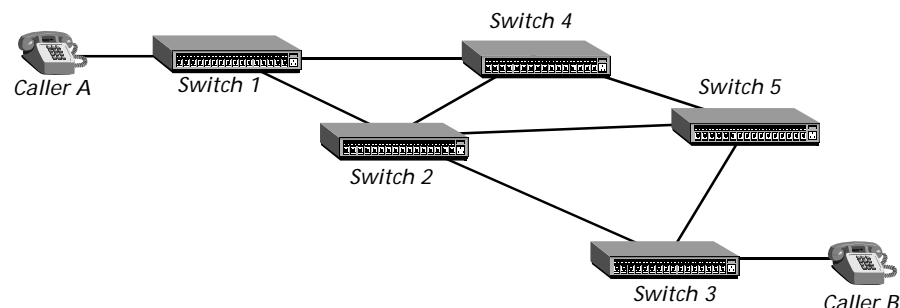
The public switched telephone network	1-1
The MultiVoice network.	1-2
MultiVoice applications	1-18

The public switched telephone network

Traditionally, real-time voice information is sent over the public switched telephone network (PSTN). Circuit-switched technology provides every call with dedicated bandwidth, usually 64Kbps. End-to-end calls are established on the basis of a sequence of dialed digits, and the PSTN dedicates a physical path between callers. Because the telephone equipment establishes the call path at the beginning of the call, the path can change *between* calls, but never while a call is active.

Figure 1-1 illustrates an example of a PSTN network. Caller A dials Caller B's phone number. As Caller A dials the phone number, the network might route the call from Switch 1 to Switch 2 to Switch 3, which connects to Caller B. Once the PSTN establishes the call, communication travels only through Switch 1, Switch 2, and Switch 3.

Figure 1-1. Example of call routing over circuit-switched PSTN



If Caller A dials Caller B again, the PSTN might establish the call by routing it from Switch 1 to Switch 4 to Switch 5 to Switch 3 before finally connecting Caller A to Caller B. Again, the path can change between calls, but not during any specific call.

In contrast, an Internet Protocol (IP) network has a packet-switched architecture. Devices transmit data in packets, and the path of one packet from end to end can vary from another packet within an established session. In addition to data, packets

contain addressing information, which routing devices use to send each packet to its destination. Routing devices maintain tables that instruct them how to direct packets. Dynamic protocols, like Routing Information Protocol (RIP) or Open Shortest Path First (OSPF), define methods that routing devices use to update each other as networking environments change.

In the past, the PSTN was the only network supporting voice communication. With MultiVoice, voice traffic can be transmitted across IP networks.

The MultiVoice network

MultiVoice complies with International Telecommunications Union Telecommunication Standardization sector standard (ITU-T) H.323 for transmitting voice telephone calls across IP networks. The H.323 standard defines a framework for the transmission of real-time voice communications across IP networks. MultiVoice on the APX or MAX TNT also supports integration with Signaling System 7 (SS7) networks by means of IP Device Control (IPDC), a media gateway control protocol, to provide call control for Voice over IP calls originating from SS7 networks.

Multivoice terms and definitions

In addition to the vocabulary used in the TAOS environment, MultiVoice uses some specific voice-related expressions. The following lists the most common terms with their definitions.

Term	Definition
Call end-point	The communications device used to initiate or answer a call, or a call's origin or destination.
Egress	A general voice-related term for an exit. For MultiVoice, a location or device used to route data from the packet network onto the analog network. Related terms: egress PSTN, egress switch
Egress gateway	A term specific to MultiVoice for the TAOS unit which connects a VoIP call to the called telephone number. The egress gateway: <ul style="list-style-type: none">• Dials the destination telephone number• Converts data from the packet network to analog voice• Reports call progress Related terms: egress MultiVoice Gateway, egress TAOS unit
Far end	A general voice-related term for the remote call termination point, relative to the active call end point. For MultiVoice, the location or device—relative to the point-of-origin of network packets, call signals, etc.—where packets, call signals, etc., for the remote call end point are processed. Related terms: far-end PSTN, far-end switch
Far-end gateway	(Specific to MultiVoice) The TAOS unit at the opposite end of the packet network connection—relative to the active call end point. Related terms: far-end MultiVoice Gateway, far-end TAOS unit

Term	Definition
Ingress	<p>(General) An entrance. For MultiVoice, a location or device where voice signals from the analog network are routed onto the packet network.</p> <p>Related terms: ingress PSTN, ingress switch</p>
Ingress gateway	<p>(Specific to MultiVoice) The TAOS unit where a VoIP call originates. The ingress gateway:</p> <ul style="list-style-type: none"> • Accepts calls from the PSTN • Initiates requests for call admissions • Converts analog voice to packet network data • Reports call progress <p>Related terms: ingress MultiVoice Gateway, ingress TAOS unit</p>
MultiVoice Access Manager (MVAM)	<p>A MultiVoice component that supports the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) H.323 standard for managing an IP network. MVAM supports MultiVoice Gateways, user profiles, and authentication.</p> <p>Capabilities supported by MVAM include phone-to-IP address translation, Web-based administration interface, PIN-based user authentication, virtual private network (VPN) support, Telephone number aliases, call detail reporting (CDR), Gateway and user database support, and third-party billing system support.</p>
MultiVoice Gateway	<p>A MultiVoice component that supports the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) H.323 standard for transmitting voice over an IP network.</p> <p>When a voice call is received at a local MultiVoice Gateway, the voice signal is packetized, compressed, and transmitted over the packet network using standard protocols and voice-compression technologies.</p> <p>At the remote gateway, the process is reversed and the call is delivered over the remote packet network to its intended destination.</p>
Near end	<p>(General) A local call termination point, relative to the active call end point. For MultiVoice, the location or device—relative to the point-of-origin of network packets, call signals, etc.—where packet processing, call signaling, etc., is initiated for the active call end point.</p> <p>Related terms: near-end PSTN, near-end switch</p>
Near-end gateway	<p>(Specific to MultiVoice) The TAOS unit which provides the local connection to the packet network—relative to the active call end point.</p> <p>Related terms: near-end MultiVoice Gateway, near-end TAOS unit</p>

MultiVoice packet processing

MultiVoice voice and data are processed using User Datagram Protocol (UDP) packets. UDP is a protocol within the TCP/IP protocol suite that is used in place of TCP for processing real-time audio and video traffic. UDP is used with Real-time Transport Protocol (RTP) to provide delivery, packet sequence checking, and error notification for MultiVoice call processing.

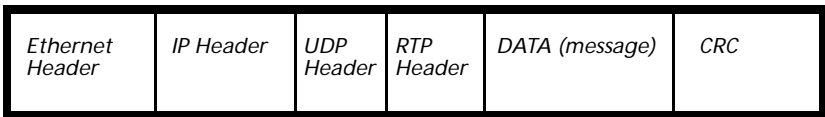
Voice over IP (VoIP) call data is compressed into frames assembled inside RTP packets. Each RTP packet is wrapped within a UDP packet and includes timestamping and synchronization information in its header for proper reassembly of the voice frames at the receiving end.

In a UDP/IP stack, the RTP header is created first and then the packet is moved down the stack to UDP and IP. UDP hands over these packets to the IP protocol layer along with the IP address of the destination node.

At the IP layer, the target address information for the destination gateway is processed, then passed to the Ethernet layer which establishes the data link between the two MultiVoice Gateways; completing the connection between the packet network and the PSTN.

Figure 1-2 illustrates how each MultiVoice packet is formatted for transmission across the packet network.

Figure 1-2. MultiVoice packet format



For more details on MultiVoice packet processing see Appendix A, “MultiVoice Packet Processing.”

Supported audio codecs

MultiVoice provides support for the following audio compression/decompression algorithms (codecs) as defined by the International Telecommunications Union Telecommunications sector standards (Series G) for telephonic audio transmission:

Audio codec	Description
G.711	This algorithm transmits and receives a-law and μ -law pulse code modulation (PCM) voice signals at digital bit-rates of 48Kbps, 56Kbps, and 64Kbps. Digital telephone sets on digital PBXs and ISDN channels use this algorithm. Support is required by the H.323 standard. MultiVoice supports both G.711 A-law and G.711 μ -law.
G.723.1	This algorithm performs speech compression/decompression using a low bit rate—5.3Kbps or 6.3Kbps—output quality. This codec is designed specifically for voice transmission over low bit-rate links (greater than 56Kbps). MultiVoice supports this codec at both bit-rates.

Audio codec	Description
G.728	This algorithm performs speech compression/decompression at 16Kbps using low-delay code excited linear predictive methods, with a frame size of 2.5 milliseconds. MultiVoice implements this codec using a frame size of 5 milliseconds. It uses the same bitstream as the ITU-T standard and allows speech processed by a MultiVoice Gateway to be processed by any other gateway that supports the G.728 standard.
G.729(A)	This Conjugate Structure, Algebraic Code Excited Linear Predictive (CS-ACELP) algorithm is used for compression/decompression of speech at 8Kbps, as defined by the ITU-T Standard G.729, with Annex A.
Full-rate GSM	<p>This algorithm is a voice encoder/decoder standard for cellular communications. It compresses the speech samples from 64Kbps PCM to 13.2Kbps, requiring less network than G.711 a-law/μ-law. European, Japanese and Australian cellular communications systems follow this standard, and certain Web phone applications support it.</p> <p>Full-rate GSM uses a speech frame size of 160 samples (20 msec) and the encoder produces 33 bytes per frame. The decoder produces 160 samples (20msec) of speech from the 33-byte encoder output.</p> <p>This algorithm also supports silence detection and comfort noise generation for Full-rate GSM.</p>

H.323 implementation

MultiVoice implements the H.323 standards defined for both gateways and gatekeepers. Gateways connect the PSTN to the IP-based network. Calls originate at a MultiVoice Gateway and travel across the IP network, which are then routed to a second MultiVoice Gateway that is connected to the PSTN and, then ultimately, to the destination phone. The gatekeeper manages the network, supporting all gateways, user profiles, and authentication. The MultiVoice Access Manager (MVAM) performs the gatekeeper functions for a MultiVoice network.

Supporting the H.323 direct-call model for Voice over IP networks, MultiVoice implementation includes

- Integrating PSTN and packet networks to complete calls
- Using primary and secondary gatekeepers
- Using overlapping gateway coverage areas

Integrating PSTN and packet networks

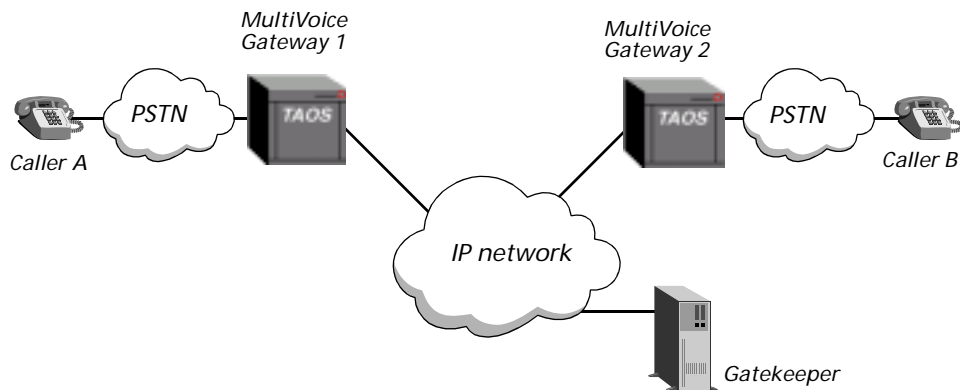
A MultiVoice network integrates both the PSTN and packet networks. Two gateways connect Caller A to Caller B. An NT or Solaris-based server running MVAM is the gatekeeper.

In Figure 1-3, when Caller A dials Caller B, the following high-level events occur:

- 1 Caller A dials Gateway 1 and enters the PIN authentication (if required) and Caller B's phone number.
- 2 Gateway 1 establishes a session with the gatekeeper.
- 3 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.
- 4 The gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.
- 5 Gateway 1 establishes a session with Gateway 2.
- 6 Gateway 2 forwards the call request to Caller B.

When Caller B answers the phone (goes off-hook), voice traffic is transmitted in IP packets between Gateway 1 and Gateway 2 using RTP protocol.

Figure 1-3. Example of a MultiVoice network



If the callers in Figure 1-3 used a traditional voice communications network, Caller A would require a long-distance carrier's services to reach Caller B. But, Caller A is in Gateway 1's coverage area, and can reach the gateway with a local call. The IP-routed network performs the same function as a long-distance carrier's circuit-switched network.

Coverage areas

Each MultiVoice Gateway services a *coverage area*. The coverage area consists of a group of telephone numbers that may dial and receive calls through a particular gateway. Coverage areas for each gateway are defined by assigning dial strings, such as country codes, area codes, country code/area code combinations, area code/exchange combinations, or complete telephone numbers, to a database on the gatekeeper.

Inclusion areas

Individually, each of the telephone numbers and dial strings assigned to a coverage area represents an individual *inclusion area*. Together, these inclusion areas represent the coverage area for a MultiVoice Gateway. For example, an inclusion area could be specified by the partial telephone number 1732. This number is composed of a country code of 1 and area code of 732. A gateway with this inclusion area would cover all telephone numbers within the 732 area code.

Overlapping gateway coverage areas

In a MultiVoice network with overlapping gateway coverage areas, two or more gateways can process incoming calls to telephone numbers in the same coverage area. The MVAM allows you to assign the same inclusion areas, defined by country codes, area codes, country code/area code combinations, area code/exchange combinations, or complete telephone numbers, to two or more gateways, creating overlapping coverage areas.

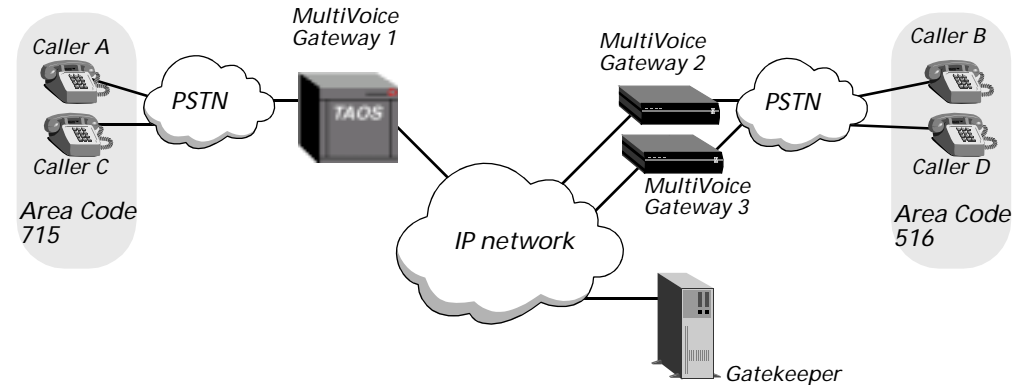
Identical coverage areas may be configured on the gatekeeper for each MultiVoice Gateway in the group. This type of network configuration provides for dynamic call management and allow the gatekeeper to perform call load-leveling across a group of gateways.

Figure 1-4 illustrates a MultiVoice network with overlapping coverage areas. Two gateways provide coverage to area code 516. An NT or Solaris-based server running MVAM is the gatekeeper. When Caller A dials Caller D, Caller C dials Caller B, and both dialed phone numbers are part of the same coverage area, the following high-level events occur:

- 1 Caller A dials Gateway 1, and enters the PIN authentication (if required) and Caller D's phone number.
- 2 Gateway 1 establishes a session with the gatekeeper.
- 3 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.
- 4 The gatekeeper attempts to authenticate Caller A and, if successful, identifies all the MultiVoice Gateways that support the coverage area for Caller D's phone number.
- 5 The gatekeeper forwards the IP address of Gateway 2 to Gateway 1.
- 6 Gateway 1 establishes a session with Gateway 2.
- 7 Gateway 2 forwards the call request to Caller D.
- 8 Now, Caller C dials Gateway 1, and enters his or her PIN authentication (if required) and Caller B's phone number.
- 9 Gateway 1 establishes a session with the gatekeeper.
- 10 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.
- 11 The gatekeeper attempts to authenticate Caller C and, if successful, identifies the MultiVoice Gateways that support the coverage area for Caller B's phone number.
- 12 This time the gatekeeper forwards the IP address of Gateway 3 to Gateway 1.
- 13 Gateway 1 establishes a session with Gateway 3.

14 Gateway 3 forwards the call request to Caller B.

Figure 1-4. Example of a MultiVoice network with overlapping coverage areas



In Figure 1-4, the gatekeeper, having already routed a call from Caller A to Caller D through Gateway 2, determines that the call from Caller C to Caller B should be routed through Gateway 3 instead of Gateway 2 to keep the call volume balanced.

Since MultiVoice uses one port per call, the gatekeeper attempts to assign calls to each gateway based upon port availability, alternating call assignments between covering gateways.

Using primary and secondary gatekeepers

Figure 1-5 shows an example of a MultiVoice network that uses primary and secondary gatekeepers to manage VoIP network operations. The VoIP network configuration in Figure 1-5 provides the MultiVoice network with redundant call-management capability.

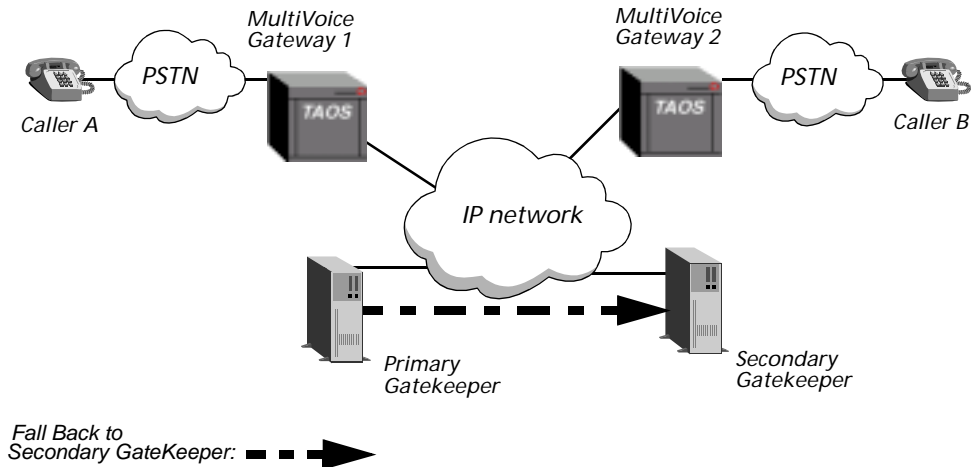
Each MultiVoice Gateway may be configured to register with a secondary gatekeeper when it cannot register with the primary gatekeeper. This enables call processing to continue in the event that the primary gatekeeper cannot be reached by a gateway (redundancy).

As illustrated in Figure 1-5, two MultiVoice gateways can connect Caller A to Caller B. Either of the NT or Solaris-based servers running MVAM can be the gatekeeper.

When Caller A dials Caller B, the following high-level events occur:

- 1 Caller A dials Gateway 1 and enters the PIN authentication (if required) and Caller B's phone number.
- 2 Gateway 1 attempts to register with its primary gatekeeper.
If the registration fails, Gateway 1 attempts to register with its secondary gatekeeper.
- 3 When registration is established with the secondary gatekeeper, Gateway 1 forwards the phone number and PIN authentication to the secondary gatekeeper.
- 4 The secondary gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.
- 5 Gateway 1 establishes a session with Gateway 2.
- 6 Gateway 2 forwards the call request to Caller B.

Figure 1-5. Example of a MultiVoice network with a secondary gatekeeper



The primary and secondary gatekeepers are separate NT or Solaris-based servers, each with a unique network identity, each running its own copy of the MVAM application, and functioning independently of each other. Each gatekeeper has unique gateway and user databases, and each maintains separate call and activity logs. To ensure coverage, the two gatekeepers must:

- Have duplicate gateway and user information
- Be administered using the same time
- Be synchronized using some third-party clock synchronization mechanism (such as NTP)

The secondary gatekeeper does not report call activity to, nor share call records with the primary gatekeeper. Therefore, if a third-party billing system is used with MultiVoice, all the gatekeepers on the network must communicate with that billing system server.

Increasing gatekeeper reliability

The ITU-T H.323 standard defines a zone as a group of gateways that register with and are administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

To maximize gatekeeper reliability, and reliability of a MultiVoice network, multiple MVAM systems, each servicing its own H.323 zone, may be configured as redundant gatekeepers. This is called *sparing*.

In Figure 1-6, MVAM systems in a MultiVoice network are paired for use as reciprocal secondary gatekeepers. Each MVAM serves as both a primary gatekeeper for its selected zone and a secondary gatekeeper for adjoining zones. If a MultiVoice Gateway fails to register with the MVAM in that zone, that gateway attempts to register with its paired MVAM. In this configuration, each gatekeeper maintains duplicate gateway and user information for the reciprocating gatekeeper's zone.

Figure 1-6. Reciprocal secondary gatekeepers

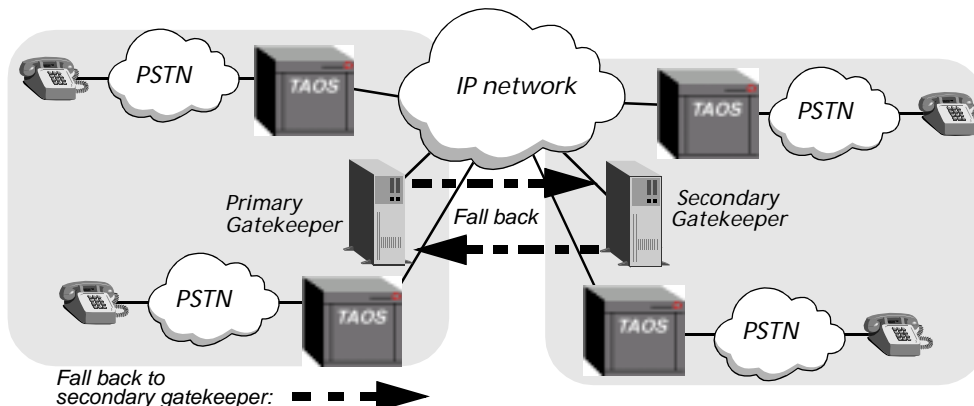
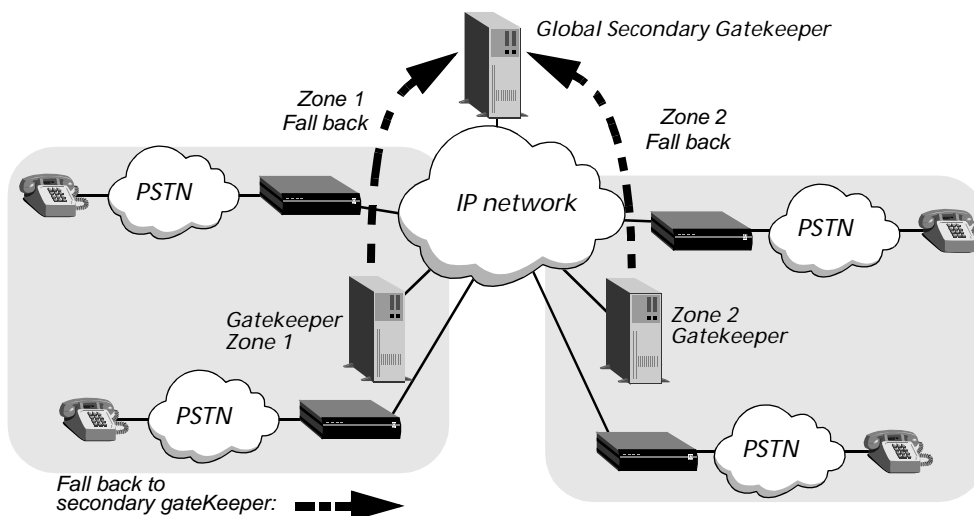


Figure 1-7 illustrates how a MultiVoice network may be configured to use a single MVAM as the secondary gatekeeper for the entire network. If any MultiVoice Gateway fails to register with its primary gatekeeper, that gateway attempts to register with the MVAM performing the global gatekeeper function. The MVAM that performs the global gatekeeper function maintains duplicate gateway and user information for all other gatekeeper zones in the MultiVoice network.

Figure 1-7. Global secondary gatekeeper



Keep-alive registration

Once registered with a gatekeeper, a MultiVoice Gateway must periodically reregister. This is called *keep-alive registration*. Keep-alive registration informs the gatekeeper that a gateway is available to accept calls. By default, a MultiVoice Gateway attempts keep-alive registration with its primary gatekeeper every 120 seconds. At registration time, the gateway makes up to five registration attempts, at 5-second intervals, until successfully contacting the gatekeeper.

When keep-alive registration fails, the MultiVoice Gateway does one of the following, if:

- A valid IP address (non-null) is configured for the Gatekeeper-IP-Sec parameter, the gateway attempts to register with its secondary gatekeeper. Once registration is accomplished, the gateway implements the same keep-alive registration policy with the secondary gatekeeper as it did with its primary gatekeeper.
- No valid IP address is configured for the Gatekeeper-IP-Sec parameter, the gateway goes into a *slow poll mode* with the primary gatekeeper. In this mode the gateway attempts to register with its primary gatekeeper at 30-second intervals, until successfully contacting the gatekeeper.



Note While attempting to register with the primary gatekeeper, the MultiVoice Gateway is effectively *unregistered* with any gatekeeper. During this period, new calls are blocked. However, existing calls continue to operate normally.

Reregistration with a primary gatekeeper

Once the MultiVoice Gateway registers with the secondary gatekeeper, the gateway continues to attempt to reregister with its primary gatekeeper periodically. By default, the gateway makes one attempt to reregister with its primary gatekeeper after every five successful keep-alive registrations with the secondary gatekeeper. After the fifth successful registration with the secondary gatekeeper, the gateway makes up to five registration attempts, at 5-second intervals, to contact its primary gatekeeper. If the MultiVoice Gateway cannot register with its primary gatekeeper after five attempts, the gateway continues to perform keep-alive registration with its secondary gatekeeper.

Gatekeeper registration policy

Gatekeeper registration policy is set on both the MVAM and MultiVoice Gateway. The MultiVoice Access Manager uses the RegistrationDuration parameter to set the interval at which a MultiVoice Gateway must perform keep-alive registration. This parameter defaults to 150 seconds, adding a 30-second buffer to the reregistration interval.

The MultiVoice Gateway uses the following parameters in the voi p { 0 0 } profile to control gatekeeper registration:

Parameter	Setting
gatekeeper-ip-sec	The IP address of the gateway's secondary gatekeeper.
gatekeeper-keepalive	The time interval at which a gateway performs keep-alive registration with a gatekeeper.
registration-retries	The number of registration attempts a gateway performs during keep-alive registration.
registration-retry-time	The time interval between each registration attempt a gateway performs during keep-alive registration.
primary-retries	The number of registrations with the secondary gatekeeper after which a gateway attempts to reregister with its primary gatekeeper. This value represents a cycle of successful keep-alive registrations with the secondary gatekeeper.

For more information about setting gatekeeper registration policy see “H.323 gatekeeper communication” on page 3-24.

How calls are assigned to a MultiVoice gateway

When a call request is received from a gateway, the MVAM first identifies all the gateways which could be used to complete the call. The MVAM may connect calls by selecting a gateway based on the following:

- The available port capacity of each gateway
- The current call volume of each gateway

The selection method is controlled by parameters contained in the MVAM initialization file. See the *MultiVoice Access Manager User's Guide* for a detailed explanation of these parameters.

Call assignment based on port capacity

The MVAM assigns calls based on the available gateway port capacity when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

- 1 Identifies all the gateways that could possibly connect the call.
- 2 Checks the ratio of ports in use to ports available for each covering gateway.
- 3 Selects a gateway with the most available resources for connecting the call (such as, the smallest ratio of ports in use to ports available).

Using the ratio of the gateway's ports in use to the gateway's number of available ports provides better load balancing across gateways with overlapping coverage areas and maximizes the use of available network assets.

Using routing based on port capacity, when three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the TAOS unit having the most idle ports (ports available), based on the total port capacity of the gateway.

Call assignment based on call volume

The MVAM assigns calls based on current call volume of each gateway when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

- 1 Checks the current call volume of each covering gateway.
- 2 Determines which gateway is connecting the fewest calls.
- 3 Assigns the call to the gateway currently connecting the fewest calls.

Calls routed based on call volume do not take into account the port capacity of the individual gateway (a port being the combination of a digital signal level 0 (DS0) and digital signal processor (DSP)) how many ports are currently idle and available for connecting calls on a given gateway.

When using the call volume routing, if three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the TAOS unit

with the fewest active calls (ports in use), disregarding the total port capacity of that gateway.



Note If the call is rejected by the selected gateway, the call is dropped.

MultiVoice networks supporting multizone call routing

MultiVoice supports routing calls between gateways that are registered with different MVAMs (Gatekeepers). Calls originating at one gateway, registered to and administered by one gatekeeper, are connected using a different gateway that is registered to and administered by another gatekeeper.

The ITU-T H.323 standard defines a zone as a group of gateways that are registered with and administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

Routing across H.323 zones

When calls are routed between zones, the gatekeeper in the zone where the call originates contacts a gatekeeper in another zone to locate a gateway to connect the call. When routing between zones, two MVAMs reside on separate servers, each with their own unique set of registered gateways. The two access managers set up the call between two gateways residing in different zones.

Implementing call routing

MVAMs use the optional called endpoint signaling method of call routing, which allows an MVAM to route a call through another gatekeeper.

Each MVAM in a MultiVoice network system maintains a database of peer gatekeepers. Each entry in this database contains a gatekeeper's identifier (a unique name) and its IP address. Each MVAM in the system also has a database of peer gatekeeper inclusion areas.

These inclusion areas define the telephone numbers that a gatekeeper is responsible for covering. Overlapping coverage areas are also supported for gatekeepers.

Figure 1-8 shows an example of a MultiVoice call routed between two gateways in different zones. The gatekeeper MVAM_east requests a call routing for a call originating in New York City to a telephone number in Los Angeles from the gatekeeper MVAM_west, which cannot be connected through an East Coast Zone gateway.

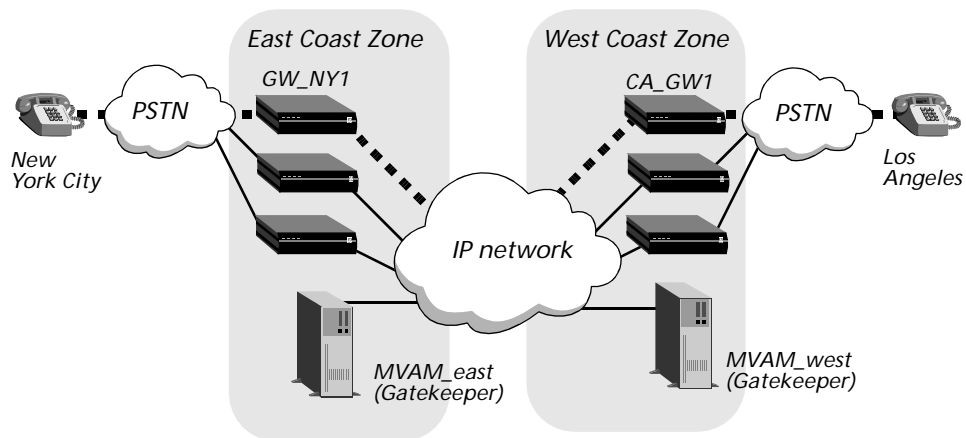
When a MVAM is asked by a gateway to route a call, it first determines if the call can be routed to a gateway within its own zone. If the call cannot be routed within its zone:

- 1 The East Coast gatekeeper, MVAM_east, receives a request to send a call from the East Coast gatekeeper GW_NY1 to a destination telephone number in Los Angeles, CA.
- 2 MVAM_east checks its gateway database. It determines that this call cannot be completed through a gateway in the East Coast zone.

- 3 MVAM_east checks its known gatekeeper database to determine if the coverage area is supported in another zone and locates a coverage area supported by the West Coast gatekeeper, MVAM_west.
- 4 MVAM_east sends a Location Request message (LRQ) to MVAM_west.
- 5 MVAM_west checks its gateway database. It determines that its gateway, CA_GW1, can connect the call.
- 6 MVAM_west sends a Location Confirmed (LCF) message containing the IP address of gateway CA_GW1.
While waiting for a response, MVAM_east sends a Request-In-Progress message to GW_NY1.
- 7 When MVAM_east receives the Location Confirmed (LCF) message from MVAM_west, an Admission Confirmed (ACF) message containing the conferenceId is sent to GW_NY1.
- 8 CA_GW1 completes the call.

If the covering gatekeeper decides it does not have a covering gateway, it returns a Location Reject (LRJ) message.

Figure 1-8. Example of a MultiVoice network supporting multizone call routing



While waiting for the covering gatekeeper to respond with gateway information, the MVAM generates pointers to a potential ACF message and the LRQ message in the Active Call Table, and returns without generating an ACF or an Admission Reject (ARJ) message. The LRQ message has the conferenceIdentifier for the call in its nonStandardData parameter, and the covering gatekeeper returns this in the nonStandardData parameter of the LCF or LRJ message.

IP Device Control implementation

IP Device Control (IPDC) is a Media Gateway Control Protocol (MGCP) that is used to connect voice calls originating from the PSTN using a TAOS unit (an APX or MAX TNT). It analyzes incoming data signals, inband control signals and tones, and sets up and controls the appropriate gateways. It also handles management and reporting.

Connection with the SS7 network is achieved through a signaling gateway (SoftSwitch), which provides a traditional SS7 interface to circuit switches and/or

signal transfer points (STPs) and interworks ISDN User Port (ISUP) messages to IPDC. The signaling gateway (SoftSwitch) acts as a media controller, analyzing incoming signals and determining the appropriate backbone network and services required to route the data; controlling point-to-point connections for establishing calls across packet and circuit (PSTN) networks (that is, initiating and managing call setup and release and executing call routing).

Overview of the signaling gateway

The signaling gateway (SoftSwitch) is the call controller and provides an interface to PSTN for signaling using SS7 and it controls MultiVoice Gateways using IPDC.

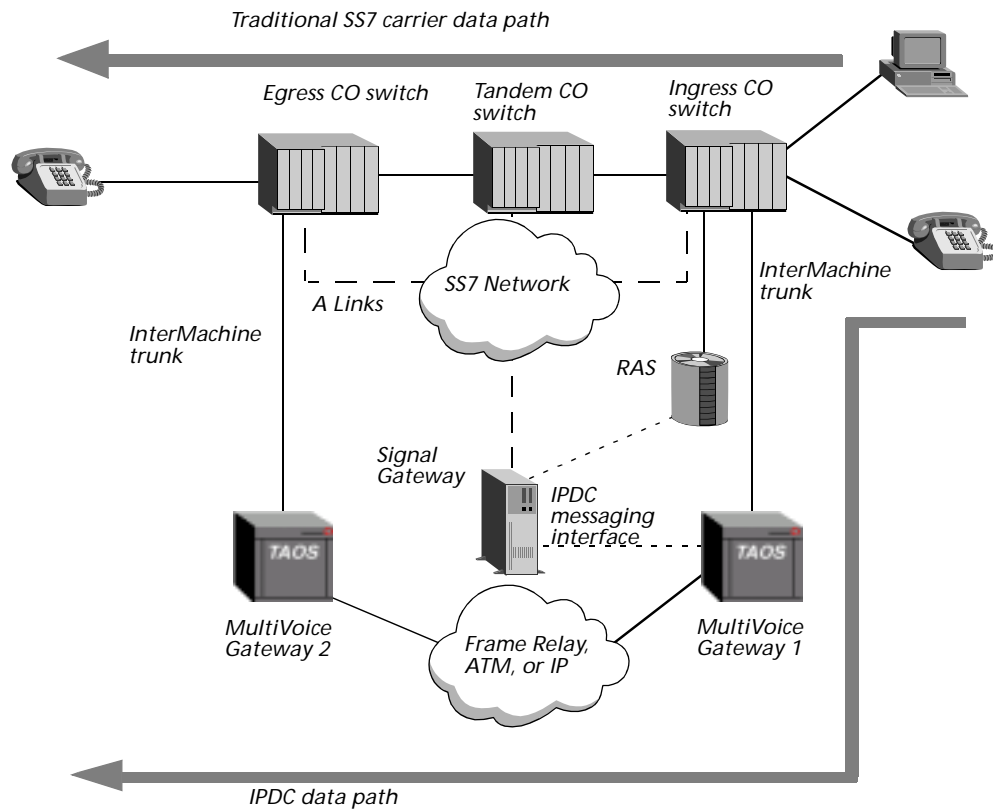
The signaling gateway (SoftSwitch) uses the IPDC protocol to convert SS7 signaling information and call data from the PSTN into IPDC packets, which are sent to the TAOS unit. The signaling gateway (SoftSwitch) also uses IPDC to convert IPDC packets received from a TAOS unit into SS7 messages, before sending the call to the PSTN.

A TAOS unit on the call initiating end uses IPDC to extract Time Division Multiplexing (TDM) and IP routing instructions from the IPDC packets received from the signaling gateway (SoftSwitch) before sending call data across the IP network.

The connecting TAOS unit forwards IPDC packets to the signaling gateway (SoftSwitch), where those packets are converted back into SS7 messages before the call is connected.

Figure 1-9 illustrates the IPDC implementation, which combines a signaling gateway (SoftSwitch) for routing voice, fax and modem calls across a packet network.

Figure 1-9. The Signaling gateway using IPDC implementation



The signaling gateway (SoftSwitch) represents a signal switching point (SSP) node in an SS7 network; which connects, in turn, to a signaling transfer point (STP); which is peered to the core of the signaling network. The signaling gateway (SoftSwitch) uses multiple A-links (v.35, DS-0/A, etc.) to connect to the STP. The remote access server (RAS), on the trunk side, has an intermachine trunk (IMT) (T1, E1, etc.) provisioned from a Class 5 switch. On the line side, the RAS will typically have an ethernet connection to the SG and/or connect through a media controller that will either be integrated with the SG or physically stand alone. The specific configuration depends on the network configuration (that is, ICD, VoIP, Tandem replacement, etc.) and product used for the signaling gateway (SoftSwitch) and media controller.

IPDC call processing messages

IPDC messages exchanged between the TAOS unit and the signaling gateway (SoftSwitch) during VoIP call processing are described in Table 1-1.

Table 1-1. IPDC VoIP call processing messages

Message	Sent by	Purpose
RCCP (Request Confirm Call Parameters)	Signaling gateway (SoftSwitch)	This is a call request message. It contains the call setup information the TAOS unit needs for routing the call to its destination. This includes all IP addressing, RTP port setup, codec and packet loading information.
ACCP (Accept Confirm Call Parameters)	TAOS unit	This is a call confirmation message. It verifies the call setup information the TAOS unit used for routing the call to its destination.
RMCP (Request Modify Call Parameters)	Signaling gateway (SoftSwitch)	This is a request to modify the VoIP call parameters for the current call. It changes call parameters, such as, the active audio codec and switchover to fax, while a VoIP call is in progress.
AMCP (Accept Modify Call Parameters)	TAOS unit	This message confirms modifications to the VoIP call parameters for the current call. It verifies that the requested changes are implemented.
STN (Send Tones Message)	Signaling gateway (SoftSwitch)	This is a call progress message. It directs that certain call-progress tones or voice announcements are played for callers during a VoIP call.
ASTN (acknowledge result of Send Tones Message)	TAOS unit	This message confirms playout of requested call-progress tones or voice announcements during a VoIP call.

Configuration of IPDC messages is performed on the media controller for the signaling gateway (SoftSwitch). One signaling gateway (SoftSwitch) and media controller can manage calls routed through multiple TAOS unit systems.

MultiVoice integration with frame relay networks

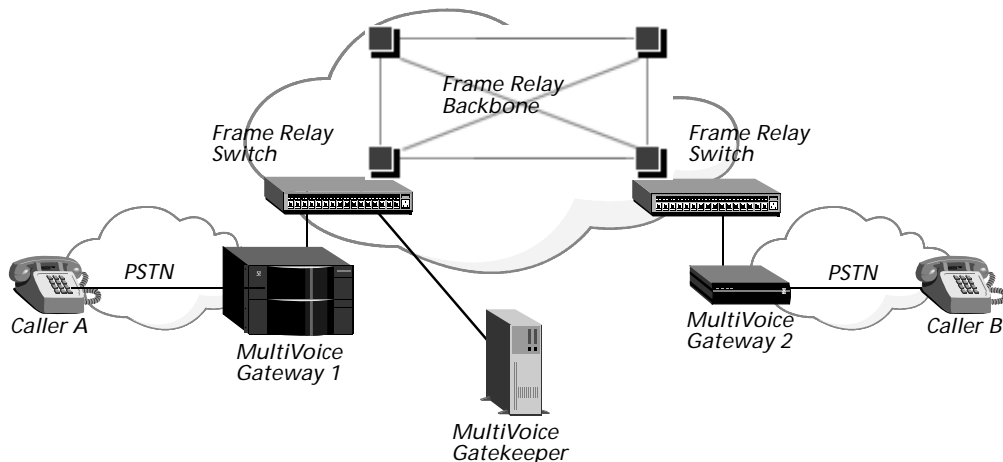
MultiVoice supports transmission of voice packets across Frame Relay networks as a means of providing improved Quality of Service (QoS). MultiVoice packets can be routed onto a Frame Relay network by connecting through either a router or switch, such as Lucent Technologies Pipeline 85 or Xedia Access Point 45, to the Frame Relay network.



Note While the TAOS unit may be configured as a Frame Relay gateway, MultiVoice is not supported as a Voice over Frame Relay application. It is not recommended that MultiVoice Gateways be used as Frame Relay gateways.

Figure 1-10 shows how MultiVoice Gateways integrate with Frame Relay networks. The MVAM must also be connected to the same Frame Relay backbone network that connects the MultiVoice Gateways.

Figure 1-10. Sample MultiVoice network



MultiVoice applications

MultiVoice supports a variety of applications, including:

- 1+ dialing for residential long distance
- Local toll-free service
- Postpaid and prepaid calling-card service
- PC-to-phone over a virtual private network or an ISP's point of presence (PoP)
- Phone-to-PC (also known as "Internet Call Waiting")
- Single-Stage, 1+ dialing services with interconnection using PSTN or VoIP

1+ dialing for residential long distance

This service is offered for both single-stage and dual-stage dialing of VoIP calls.

With single-stage dialing, the Dialed Number Identification Service (DNIS) string is extracted for the destination telephone number from a single dialed entry. The destination number is passed to the distant gateway during call setup.

With dual-stage dialing, callers are required to dial the MultiVoice Gateway first, then wait for a subsequent dial tone before dialing the called telephone number. The MultiVoice Gateway will prompt the caller for various forms of information, depending on the carrier's service.

MultiVoice solution features

The 1+ dialing for residential long distance application provides the following features:

- PSTN Interconnection — T1 with Feature Group D must be supported.
- Deployable Worldwide — This service is supported in many countries around the world. Check with your Lucent account representative for the comprehensive list of supported countries.
- Compressed Voice and Fax — Multiple encoding schemes are supported. However, most carriers use G.729A codec and real-time fax.
- Transparent Modem — Backhaul of modem sessions over the VoIP network using G.711 must be supported when a modem tone is detected.
- Reliable DTMF with Compressed VoIP — DTMF is recognized on ingress and passed out-of-band in the H.245 user input fields. On egress, the DTMF is generated via the out-of-band DTMF feature.
- Transport of Cause Codes from End-to-End — Carriers use this information to understand the reason why a particular call drops. This information is extremely useful for troubleshooting the application.
- Transport of ANI Info Bits from End-to-End — Requires Feature Group D trunks.
- Single-stage dialing — Requires that the VoIP carrier support Feature Group D or E1 R2 trunks that interface into the ingress side of the PSTN. Subscribers can either dial the carriers' PIC code (for example, 1010-321) or be pre-subscribed in the Central Office (CO) switch by the Local Exchange Carrier (LEC to the VoIP Long-Distance carrier.

Authentication and voice announcements

PIN and ANI authentication can be set up on the MVAM. When dual-stage dialing has been configured on a MultiVoice Gateway, the caller can be prompted to enter a PIN. The following call processing types are supported:

- 1 Configure ANI authentication. If ANI fails, then prompt for PIN.
- 2 Configure ANI authentication and only prompt for DNIS.
- 3 Configure ANI authentication and prompt for PIN and DNIS.
- 4 Do not configure ANI authentication, but prompt for DNIS.
- 5 Do not configure ANI authentication, but prompt for PIN and DNIS.

Voice announcements stored on the MultiVoice Gateway provide prompts for the caller. Service providers can customize the creation and installation of these announcements. For details on voice announcements, refer to Chapter 4, "Voice Announcement Administration".

Local toll-free service

For example, local toll-free service (800 or 888) can be much more cost-effective than traditional toll-free service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

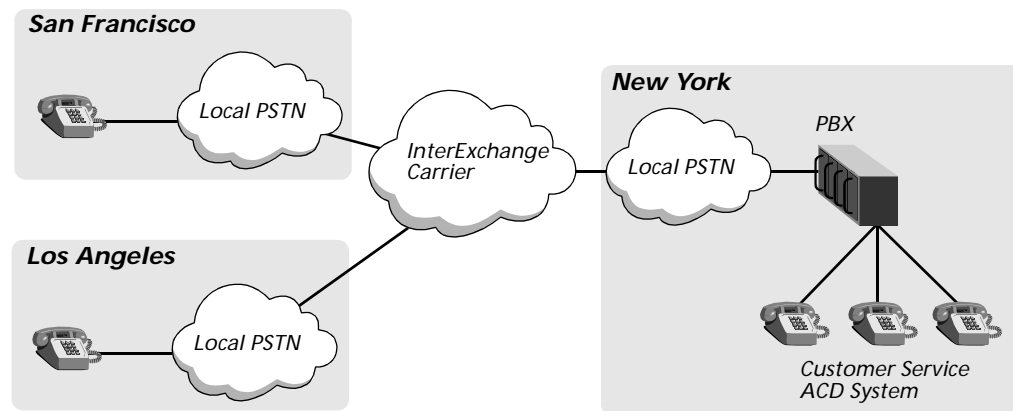
Traditional toll-free service

Suppose a company maintains a customer service department, offering their customers a traditional 800 or 888/877 phone number that they dial to receive assistance. Figure 1-11 shows an example of an environment without MultiVoice.

To reach a customer service representative, callers in San Francisco and Los Angeles dial a toll-free phone number that has been leased to a company's customer service department by its InterExchange Carrier (IXC).

The IXC routes the calls to the company's Automatic Call Distributor (ACD) system through a PBX. Because the dialed number is toll-free for the caller, the IXC bills the company for any long-distance charges, in addition to the leasing charges for the toll-free service.

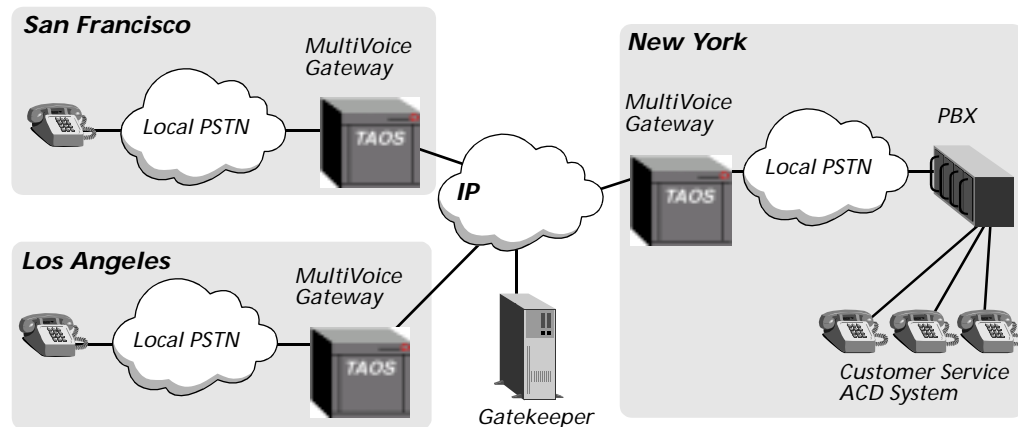
Figure 1-11. Traditional toll-free environment



Using MultiVoice with local toll-free service

Instead of leasing traditional 800 service, supposed the company in Figure 1-12 leases local toll-free service in San Francisco and Los Angeles. Each local PSTN routes local toll-free calls to a local TAOS unit, which forwards them to the customer service site in New York. Figure 1-12 illustrates how a company can use MultiVoice devices and local toll-free service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

Figure 1-12. Using MultiVoice with local toll-free service



Postpaid and prepaid calling-card service

Both prepaid and postpaid calling-card services are supported by MultiVoice. With a postpaid calling-card, callers are required to make an access call to the MultiVoice Gateway. Depending on the access number called, the MultiVoice Gateway prompts the caller for various information. The most common call processing types are as follows:

- 1 Do not configure ANI authentication, but prompt for PIN and DNIS.
- 2 Configure ANI authentication and prompt for PIN and DNIS.
- 3 Configure ANI authentication and only prompt for DNIS.

A postpaid calling-card service can be split into multiple services that include a branding requirement. With branding, carriers can have up to two different sets of voice announcements to prompt a caller for the PIN and the DNIS. For example, one set of voice announcements could be recorded and played in the English language and another set could be recorded and played in Spanish.

Prepaid calling-card services provide the same call processing types as the postpaid calling-card service, but provides these additional features as well:

- Provide ANI info bits — This determines call origination (pay phone, prison, or other location and so forth).
- Call Cutoff — When the prepaid call time runs out.
- Play Account Balance.
- Play-Talk-Time-Remaining.
- Play Multiple Low-Balance Warnings.
- Sequential Dialing ("Next Call Please").

The only known limitations of TAOS 9.0 and MVAM 3.1 is the ability to support two languages for Play Account Balance and Play-Talk-Time-Remaining features.

PC-to-phone calls

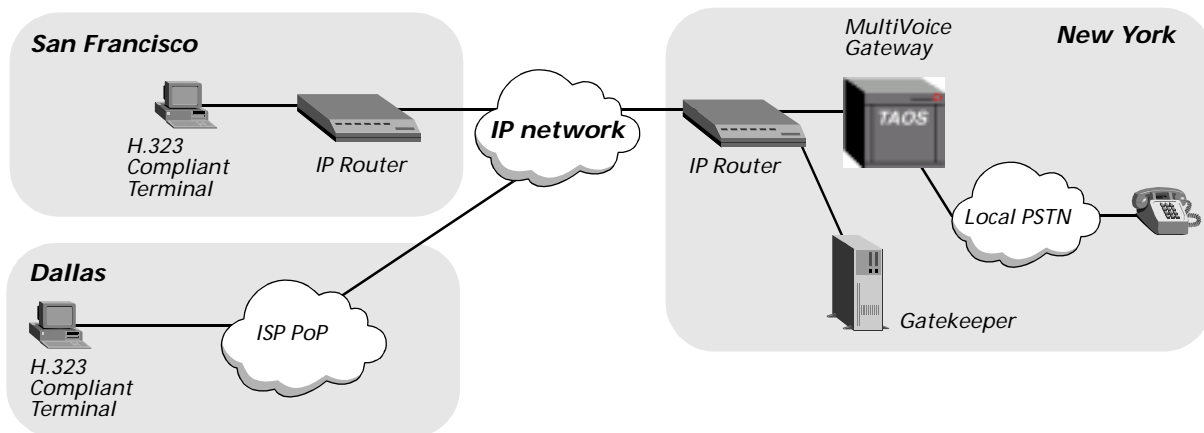
Calls initiated from PCs connected to a network are processed as if the PC was one of the MultiVoice Gateways. This requires that the PC be a fully *H.323-compliant terminal*. It must be able to register and communicate with the gatekeeper as if it were a gateway. It must also be able to communicate with the MultiVoice Gateway at the other end of the call.

Figure 1-13 shows how to PC-to-phone calls could be connected using either a *virtual private network (VPN)* or an ISP's PoP.

The callers in San Francisco use their PCs to place calls to phone numbers in New York from inside the VPN, utilizing the backbone IP network as the link to the destination MultiVoice Gateway.

The callers in Dallas use their PCs to place calls to phone numbers in New York through a local PoP provided by an ISP, utilizing the Internet connection as the link to the destination gateway.

Figure 1-13. Virtual private network using PC telephony



H.323-compliant terminals

H.323-compliant terminals are described in detail in the ITU-T Recommendation H.323. To work with MultiVoice, a PC must use a telephony application which supports:

- Registration, Admission and Status (RAS) messaging with a gatekeeper
- The G.711 audio coder/decoder (required)
- The G.729(a) and G.723.1 audio coder/decoders (optional)



Caution Not all third-party telephony software has full RAS messaging capability, or works with a gatekeeper. Microsoft's NetMeeting, version 3.0, was successfully tested and proven compatible with MultiVoice networks. Calls made from PCs using other applications may fail.

Gateway-to-client keep-alive registration

MultiVoice supports the use of a keep-alive protocol for gateway-to-clients (PCs) and/or gateway-to-gateway connections. This allows the gateway to detect terminated call connections when a remote endpoint becomes unreachable. The

MultiVoice administrator may disable this feature or control the keep-alive time interval through the gateway interface. If the keep-alive timer expires during an active call, the call will be dropped by the gateway and reported to the MVAM with the disconnect reason “forcedDrop.”

Phone-to-PC (also known as Internet call waiting)

The Phone-to-PC service allows customers to offer voice call termination from a phone to an Internet user. This is oftentimes referred to as “Internet Call Waiting.” To provide this service, the following components are required:

- MultiVoice PC Client (MVC)
- MVAM
- MultiVoice Gateways (APX, MAX TNT)

The MVAM Application Programming Interface (API) also includes an interface to a Lucent RADIUS authentication server. The MVC is used in a standalone format (also known as the cell phone version).

The following explains how the Phone-to-PC service works:

- 1 Internet users install the MVC on their PC. The MVC installation application can be downloaded from a web page or set to the user on a CD-ROM.
- 2 Internet users buy/request forward-on-busy from their Local Exchange Carriers (LEC)s. The LECs configure the service to forward calls to the ICW service provider’s VoIP network when an Internet user’s phone is busy.
- 3 An Internet user starts a dial-up modem session and is authenticated by RADIUS. The telephone line is now busy.
- 4 The MVC registers with the customer’s MVAM. This alerts MVAM that the user is online and able to accept calls on their PC.
- 5 Simultaneously, the MVAM API asks the RADIUS server for approval to add the users to the MVAM routing database. Upon approval from RADIUS, the users’ routing information is added to MVAM.
- 6 When a caller dials the Internet user’s phone number, the line is busy because the Internet user is online. The call is then forwarded from the LEC to a MultiVoice Gateway in the ICW service provider’s network.
- 7 The MultiVoice Gateway captures the originally dialed number (the number of the Internet user) and routes the call the MVC of the Internet user based on a routing table in MVAM.
- 8 The Internet user decides to accept or reject the call by clicking a button on the “ringing” MVC user interface.
- 9 If accepted, the VoIP call path is set up from the MultiVoice Gateway to the MVC using H.323.
- 10 The user can surf the WWW and talk at the same time.

With the Phone-to-PC service, a RADIUS server provides all user authentication (security) and user provisioning. Although Call Detail Records are available from MVAM (for billing), we recommend that service providers offer this service as a differentiator for their dial-up service customers—as a free or flat-fee offering.

Single-stage, 1+ dialing with interconnection using PSTN or VoIP

MultiVoice supports interconnection to other networks. These interfaces can be via PCM using standard PSTN trunking or via VoIP. The various forms of network interconnection include:

- MultiVoice Gatekeeper-to-Gatekeeper communications
- MultiVoice Gatekeeper-to-Gatekeeper communications with AT&T Harvester
- MultiVoice Gatekeeper-to-Clearinghouse using the Open Settlement Protocol (OSP)

MultiVoice solution features

Similar to the 1+ dialing for residential long distance application, the features for this service include the following:

- PSTN Interconnection — T1, T3, E1, CAS, PRI, R2, Feature Group D.
- Deployable Worldwide — This service is supported in many countries around the world. Check with your Lucent account representative for the comprehensive list of supported countries.
- Compressed Voice and Fax — Multiple encoding schemes are supported. However, most carriers use G.729A codec and real-time fax.
- Transparent Modem — Backhaul of modem sessions over the VoIP network using G.711 must be supported when a modem tone is detected.
- Reliable DTMF with Compressed VoIP — DTMF is recognized on ingress and passed out-of-band in the H.245 user input fields. On egress, the DTMF is generated via the out-of-band DTMF feature.
- Transport of Cause Codes from End-to-End — Carriers use this information to understand the reason why a particular call drops. This information is extremely useful for troubleshooting the application.
- Transport of ANI Info Bits from End-to-End — Requires Feature Group D trunks.

MultiVoice Gateway Configuration

2

System configuration	2-1
Implementing VoIP audio processing	2-12
Configuring VoIP call processing	2-13
Configuring routes for VoIP call processing	2-13
Configuring routes for IPDC VoIP call processing	2-36
Verifying IP route configuration.	2-44
Trunk configuration	2-46
Configuring 480 ports for G.711-encoded VoIP-only calls.	2-65
In-call DTMF detection for IPDC	2-67
DTMF playout for IPDC	2-73
IPDC country-specific call-progress tone playout for VoIP.	2-77

System configuration

To use a TAOS unit as a MultiVoice Gateway, it must be

- Licensed to provide the appropriate feature support for VoIP call processing
- Configured to process audio signals for VoIP calls
- Configured to allow the TAOS unit to be recognized and communicate as a MultiVoice Gateway



Caution MultiVoice does not work on a multishelf MAX TNT. Before installing MultiVoice on a multishelf MAX TNT, it must be reconfigured as a single-shelf unit.

Base profile parameters

TAOS unit support for VoIP is determined by settings on the shelf controller. The settings are displayed in the read-only base profile. The parameters that specify VoIP functionality follow.

Parameter	Setting
voip-enabled	Enables VoIP call processing. When this parameter is set to yes, the TAOS unit has been licensed to process VoIP calls.
voip-max-capacity-allowed	Sets the maximum VoIP call processing limit for an APX. When this parameter is set to yes, the VoIP software license imposes a limit on the maximum number of simultaneous VoIP calls an APX can process, regardless of how many DS3, T3, MultiDSP, or Ethernet slot cards are installed. This parameter is always set to no on a MAX TNT.
xcom-ss7	Enables/disables IPDC processing on an APX or a MAX TNT. When this parameter is set to enabled, the TAOS unit has been licensed to perform IPDC packet processing, in support of SS7 networks. The parameter value must be set to enabled to perform IPDC VoIP.

The `voip-max-capacity-allowed` parameter imposes a limit (that is, 2688 VoIP calls) on APX resources allocated for processing VoIP calls. This parameter works in conjunction with the default setting of the `maxcalls` parameter in the `voip` profile (see “Controlling VoIP call volume” on page 3-20 for details).

In multiple application environments (where both data and VoIP calls are processed by the same APX), this parameter allows you to scale VoIP support to match demand for VoIP services.



Note If an APX is licensed to process up to 2688 VoIP calls, VoIP call request 2689 is rejected.

To display all parameters in the read-only base profile, do the following:

```
admin> get base
[in BASE]
shelf-number = 1
software-version 9
.....
voip-enabled = yes
voip-max-capacity-allowed = yes
.....
```



Note These are read-only parameters that cannot be changed without relicensing the MultiVoice Gateway.

Configured memory requirements

The MAX TNT requires installation of a 32Mb JEDEC DRAM slot card and an 8Mb flash card to boot up and function properly.

The APX requires installation of a 32Mb flash card to boot up and function properly.

Using slot cards in a MultiVoice Gateway

The next few sections discuss slot cards that can be (or must be) installed in a MultiVoice Gateway. After you have installed a slot card, use the show command to verify the card is operational. For example:

```
admin> show
```

```
Shelf 1 ( standalone ):
```

	Reqd	Oper	Slot Type
{ shelf-1 slot-1 0 }	UP	UP	ether3nd-card
{ shelf-1 slot-2 0 }	UP	UP	madd3-card
{ shelf-1 slot-5 0 }	UP	UP	t3-card

MultiDSP slot cards

To use an APX or a MAX TNT as a MultiVoice Gateway, you need to install a MultiDSP slot card. A MultiDSP card is a single-slot card that supports VoIP services. A digital signal processor (DSP) is specially optimized for signal processing.

Each DSP has two channels, but when running a VoIP session, only one channel is used per call. The second channel cannot be used. A VoIP session removes the sister channel from the available list.

Two MultiDSP slot cards are available for use with MultiVoice:

- 48-port MultiDSP slot card (TNTV-SL-ADI-C)
- 96-port MultiDSP slot card (APX8-SL-96DSP)

Both slot cards can handle up to two services per slot card. The 48-port MultiDSP slot card supports 48 ports of any service. When running two services per slot card, the services can be used only in one of the following combinations:

- Data (modem/ISDN) with V.110
- Data (modem/ISDN) with Personal Handyphone System (PHS)
- Data (modem/ISDN) with VoIP

The 96-port MultiDSP slot card currently supports 96 ports of data (modem/ISDN) and/or V.110 service. When running two services per slot card, one service must be data and the other must be V.110.

Mixing MultiDSP slot cards

For H.323, if both 48-port (TNTV-SL-ADI-C) and 96-port (APX8-SL-96DSP) MultiDSP slots cards are enabled in the same chassis, only simple codecs (that is, G.711 and G.729) are permitted. H.323 VoIP calls use codecs that are supported by ALL MultiDSP cards enabled in the chassis.

If the 288-port slot card is configured to use 480 ports, then only the G.711 codec is supported for all slot cards. Enabling a 480-port card limits the H.323 codec selection

to G.711. Enabling a 96-port card limits the codecs to G.711 and G.729. See “Configuring 480 ports for G.711-encoded VoIP-only calls” on page 2-65 for details.

If using IPDC, both simple (that is, G.711 and G.729) and complex (that is, G.723, G.723-6.4kps, G.728, and FRGSM) codecs are supported if at least one card in the chassis supports the desired codec. If a gateway has both a 480-port card and a 288-port card, then IPDC VoIP calls can be made using G.711, G.729, and G.723 codecs. In order to support G.728 and FRGSM, a 48-port card needs to be enabled.

Slot card restrictions

The following configuration restrictions apply to both APX and MAX TNT units used as MultiVoice Gateways:

- The dual-port Series56™ Digital Modem slot card (TNT-SL-48MOD-S56) cannot be used in the same TAOS unit with MultiDSP slot cards.
- Multiple 48-port MultiDSP cards can be used in the same TAOS unit.
- The Series56™ II (TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C) and the Series56™ III (TNT-SL-48MODV3-S-C) Digital Modem slot cards can be used in the same TAOS unit with MultiDSP slot cards.

For installation information, see the *APX 8000 Hardware Installation Guide*, the *MAX TNT Hardware Installation Guide*, and the *APX 8000/MAX TNT Physical Interface Configuration Guide*. Profile configuration procedures are described in the *APX 8000/MAX TNT Physical Interface Configuration Guide* and the *TAOS Command-Line Interface Guide*.

When a TAOS unit detects the presence of a slot card in one of its slots, the TAOS unit creates default profiles that are specific to that type of slot card. Each profile is indexed by its physical address (shelf number, slot number, and item number) within the TAOS unit. You might need to reconfigure default profiles when a new slot card is installed.

Cohabitation on a single DSP

Cohabitation refers to the ability to run multiple applications on a single DSP. Cohabitation can be configured in the following combinations:

- One VoIP session using either the G.729A or G.711 audio codec, and one modem session
- Two VoIP sessions using either the G.729A or G.711 audio codec
- Two modem sessions

StrongARM processor

Cohabitation enables a MultiVoice Gateway to support multiple application processing on the same platform for a combination voice and data calls. During the call setup process, the StrongARM processor allocates DSPs to either voice or data calls depending upon the following:

- Call type
- Requested audio codec
- Available DSP channels

Cohabitation is restricted to performing VoIP calls plus one other data call type (such as a modem call).

DSP allocation

As call requests are processed by the MultiVoice Gateway, the StrongARM processor on the MultiDSP slot card checks each incoming call to determine an application type and subtype. Application type and subtype determines how DSPs are allocated for that call. Modem and VoIP calls, regardless of the audio codec requested, have the same application type. The application subtype is different for the complex audio codecs.

Modem, G.729, and G.711 calls all belong to the modem application type and have no application subtype. For cohabitation processing, when the modem application type is detected, only one DSP channel is allocated for the call. The twin channel on the DSP is assigned the value of no application subtype and is considered available for processing other calls.

When a 48-port MultiDSP slot card is being used, calls using G.723, G.728, and Full-Rate GSM codecs have the application subtype VOIP. When that application subtype is detected, a whole DSP is allocated for the call.

Audio codec selection

Audio codec selection is determined during H.245 terminal capabilities between the two TAOS units that connect a call. When the call request is received by the MultiDSP slot card, the call is brought up initially as a modem application type. If the call request asks for one of the complex audio codecs, the complex codec is loaded on a DSP where both channels are available.

Ethernet-3 slot card

APX and MAX TNT units do not support routing of VoIP calls through the shelf-controller Ethernet port. Instead, the Ethernet-3 slot card (TNT-SL-E100-V-C), a high-performance Ethernet module with one 100Mbps interface, is used for routing VoIP call data between TAOS units.

For installation information see the *Hardware Installation Guide* for your TAOS unit. For descriptions of profile configuration procedures see the *APX 8000/MAX TNT Physical Interface Configuration Guide* and the *TAOS Command-Line Interface Guide*.

Enabling full-duplex mode

When using the Ethernet-3 slot card to support VoIP call processing, the slot card must operate in full-duplex mode. The card operates in full-duplex mode by default, as specified in the setting of the following parameter in the ethernet profile:

```
[in ETHERNET/{ any-shelf any-slot 0 }]  
duplex-mode = full-duplex
```

Configuring connecting ports on the packet switch or router

The 100Mbps interface on the Ethernet-3 slot card is not auto configurable. Do not connect it to a hub or router port that has auto negotiation enabled. Connecting the Ethernet-3 card interface to an auto negotiated port can have negative effects on VoIP

calls, including poor voice quality for connected calls and increased instances of initial call failures.

To ensure the best performance and quality for VoIP calls, make sure that the switch or router port that connects the Ethernet-3 card to the packet network complies with the following recommended configuration:

- Port auto configuration must be disabled
- Port speed must be configured to operate at 100Mbps only
- Port must be configured for full-duplex transmission

For specific instructions on configuring the Ethernet ports, refer to the manufacturer-provided documentation for your particular network hub, router, or switch.



Note It is not necessary to apply the recommended configuration to ports providing the outbound connection from the hub or router to the rest of the IP network. This configuration is required only for the port connecting to the Ethernet-3 slot card.

Creating a default network gateway route

To ensure that VoIP calls can always find a route to the first-hop network gateway on the packet network, configure a default route for VoIP traffic. This prevents dropping RTP packets due to lack of routing information. For example, the following commands configure a default route named VoIP to a next-hop network gateway at 2.2.2.2:

```
admin> new ip-route voip
IP-ROUTE/voip read
admin> set gateway = 2.2.2.2/24
admin> write
IP-ROUTE/VoIP written
```

System configuration parameters

Modifications to certain TAOS unit parameters are necessary to support VoIP call processing. These parameters are as follows:

Table 2-1. System configuration parameters

Profile	Parameters
system	num-digits-trunk-groups max-dial-out-time parallel-dialing country
ip-global	system-ip-addr send-icmp-dest-unreachable throttle-no-port-match-UDP-traffic-on-slot
answer-defaults, connection	idle-timer

Assigning identifiers to trunk groups

For H.323 VoIP, the value of the `num-digits-trunk-groups` parameter in the system profile assigns two-digit, three-digit, or four-digit identifiers to trunk groups used by an egress TAOS unit to dial calls to the PSTN.

When a TAOS unit is configured to use trunk groups for out-dialed calls to the PSTN (`use-trunk-groups = yes`), this parameter allows the TAOS unit administrator to define up to 9999 trunk groups. MultiVoice uses trunk groups to route inbound calls to selected MultiDSP cards, and to route outbound calls over selected DS0s.

To use two-digit trunk group identifiers, the `num-digits-trunk-groups` parameter requires a value of 2 (`num-digits-trunk-groups = 2`), as in the following example:

```
Adm-172> list
[in SYSTEM]
use-trunk-groups = yes
num-digits-trunk-groups = 2
```

Once defined, the administrator can enter values from 1 through 9999 for the trunk-group parameter in the `t1` and `call-route` profiles, and can use the `trunk-prefix-enable` parameter in the `voip` profile to assign trunk prefixes to each outbound dial string for VoIP calls. See “Configuring trunk signaling for H.323 VoIP networks” on page 2-54 for more information on using trunk prefixes.

Allowing sufficient time to establish the connection

For VoIP processing, the `max-dial-out-time` parameter in the system profile should be set to 60 (seconds) or greater to allow sufficient time for the egress TAOS unit to establish the connection to the called destination.

For H.323 VoIP processing, using the 60-second value makes this parameter consistent with other internal H.323 timers, which are hard coded to time-out after 60 seconds. This allows the TAOS unit to clear abandoned/failed outgoing calls quickly and more efficiently.

Setting the number of simultaneous outgoing calls

For H.323 VoIP, the value of the `parallel-dialing` parameter in the system profile should be set to 32. This parameter sets the number of simultaneous outgoing calls to the PSTN an egress TAOS unit system can run.

When the number of outgoing calls exceeds the set value, outgoing calls are queued and sent to the PSTN when a free slot becomes available. Meanwhile, callers hear silence while waiting for the TAOS unit to complete the call.



Note Using the default value for `parallel-dialing` (`parallel-dialing = 2`) causes frequent delays in connecting calls.

Generating country-specific call progress tones

For H.323 VoIP, the `country` parameter in the system profile enables the TAOS unit to generate country-specific local call-progress tones for VoIP calls. This feature localizes call-progress tone processing by the TAOS unit for the selected country, based on the ITU spec TSM Circular 18: *Update of Supplement No. 2, ITU-T (former CCITT) Blue Book, Fascicle II.2 - “Various tones used in national networks.”*

The country parameter allows the TAOS unit to return the appropriate signals to the PSTN, based on the H.323 call state. These signals include dial tone, ringback (alerting tone), and busy and fast busy (congestion) tones, with the following exceptions:

- If near-end cut-through is enabled in the voi p profile (cut-thru-enable-nearend = yes), this parameter applies only to dial tone, busy, fast-busy, and number unobtainable tones. Ringback is typically carried via RTP from the far-end in this case.
- If announcements are enabled in the voi p profile (h323-voice-ann-enabled=yes), this parameter applies only to busy and number unobtainable tones. Announcements are played in all other cases with this configuration.

The following list identifies the countries with country-specific call progress tones currently supported by MultiVoice:

- Argentina
- Australia
- Belgium
- China
- Costa Rica
- Finland
- France
- Germany
- Hong Kong
- Italy
- Japan
- Korea
- Mexico
- Netherlands
- New Zealand
- Singapore
- Spain
- Sweden
- Switzerland
- United Kingdom
- United States (default)

Identifying MultiVoice Gateways on the network

For VoIP processing, the system-ip-addr parameter in the ip-global profile identifies and locates MultiVoice Gateways on the packet network. The system-ip-addr parameter is used by the MultiVoice Access Manager (MVAM) and may be used by the SS7 media gateway controller to identify MultiVoice Gateways.

An IP address is assigned to the system-ip-addr as illustrated by the following example:

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

```
admin> set system-ip-addr = 192.168.100.128
admin> write
IP-GLOBAL written
```

For MultiVoice, the system-ip-addr parameter may use the following IP addresses associated with a TAOS unit:

- The IP address of the shelf controller Ethernet port
- The IP address of an Ethernet-3 card Ethernet port
- The soft IP address associated with the TAOS unit

The IP address of both the shelf controller Ethernet port and the Ethernet-3 slot card are associated with physical network connections on the TAOS unit. The soft IP address is a virtual network connection, which is broadcast to the network. The soft IP address may be used to communicate with the TAOS unit so long as one of the unit's physical IP interfaces (for example, an Ethernet slot card port) is up.



Note When a APX is configured for redundancy, the system-ip-addr parameter should be set to the soft IP address. This soft IP interface always routes to the primary shelf controller and is hidden from the secondary. When failover occurs and the secondary controller becomes primary, the soft IP interface is re-initialized and is now associated with the new primary controller.

The soft IP address is an internal interface that never goes down and is always associated with the TAOS unit itself rather than a specific hardware interface. The soft IP interface is set up by the system once the TAOS unit's power is turned on and the shelf controller is up. The ip-interface profile with the zero index is reserved for the soft IP interface. For example:

```
admin> dir ip-interface
 6 06/17/1999 03:06:00 { { any-shelf any-slot 0 } 0 }
19 06/21/1999 23:54:02 { { shelf-1 left-controller 1 } 0 }
19 06/25/1999 17:45:30 { { shelf-1 right-controller 1 } 0 }
```



Note If RIP is enabled, a TAOS unit advertises the soft IP interface address as a host route (with a prefix length of /32) using the loopback interface. If RIP is not enabled, routers one hop away from the TAOS unit must have a static route to the soft interface address.

The soft IP interface is activated by entering an IP address for { { any-shelf any-slot 0 } 0 }. The following example shows how to set the soft IP address. In this example, the address is set to 192.168.100.128/24:

```
admin> read ip-interface { 0 0 0 }
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } read
admin> set ip-addr = 192.168.100.128/24
admin> write
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } written
```

For H.323 VoIP call processing, the system-ip-addr parameter identifies gateways to the gatekeeper and for call routing by the gatekeeper (see "Configuring MultiVoice Gateways" in the *MultiVoice Access Manager User's Guide*). When this parameter uses the soft IP address, the TAOS unit can continue to run keep-alive registration with the gatekeeper and accept calls even in the event the network connection on the shelf controller fails.

For IPCD VoIP processing, the TAOS unit can allocate its own system IP address for the listen IP address and Real-time Transport Protocol (RTP) port and can specify its

own send address and RTP port. When allowing a TAOS unit that is acting as MultiVoice Gateway to allocate its own address, you must set the system-ip-addr parameter in the ip-global profile to an interface address other than the shelf-controller Ethernet port. For example, the following commands set the system address to the address of a port on an Ethernet card in slot 12:

```
admin> get ip-interface { { 1 12 1 } 0 } ip-address
[in IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 }:ip-address]
ip-address = 1.1.1.1/24
admin> read ip-global
IP-GLOBAL read
admin> set system-ip-addr = 1.1.1.1/24
admin> write
IP-GLOBAL written
```

VoIP traffic (communications between TAOS unit) is processed through the Ethernet slot card interfaces on a TAOS unit by setting up either host routes or network routes for communication between remote gateways using IP addresses assigned to the Ethernet slot card interfaces on a TAOS unit. See “Configuring IP routing for H.323 call processing” on page 2-28 and “Configuring IP routing for IPDC call processing” on page 2-37 for details.

Detecting and responding to misdirected ICMP packets

For H.323 VoIP, the value of the send-icmp-dest-unreachable parameter in the ip-global profile should be set to yes for MultiVoice operations. The yes setting allows a TAOS unit to detect and respond to misdirected ICMP packets by responding with an ICMP-unreachable packet, rather than redirecting the packet to the shelf controller when operating under heavy call volumes. Enabling this parameter also reduces the load placed on the shelf controller.

For each VoIP call, UDP packets can arrive at a rate of 200 packets per second, per direction. When setting up or tearing down calls, if the TAOS unit is not listening on a port for these packets, it can generate ICMP packets at a rate of one ICMP packet per one UDP packet, which can flood the network.



Note Currently, enabling this parameter breaks MTU path discovery and traceroute on an APX or a MAX TNT.

Preventing the redirection of UDP packets to the shelf controller

The throttle-no-port-match-udp-traffic-on-slot parameter in the ip-global profile prevents the TAOS unit from redirecting UDP packets (for UDP ports that are currently unknown to the TAOS unit) to the shelf controller. When two TAOS units are establishing the link for transmission of a VoIP call, both units do not always complete the call setup at the same time. However, a gateway starts sending UDP packets to the receiving gateway as soon its own call setup is complete. Enabling this parameter delays processing of these UDP packets until the link is fully established.

The `throttle-no-port-match-udp-traffic-on-slot` parameter accepts the following values:

Parameter	Setting
<code>throttle-no-port-match-udp-traffic-on-slot</code>	<p>Set this parameter to either:</p> <ul style="list-style-type: none"> <code>yes</code>—Enables delaying processing of UDP packets for an unknown UDP port on a receiving gateway until call setup is completed on both APX units. Note This is the recommended setting for MultiVoice operations, to prevent overloading of the shelf controller when both gateways do not always complete the VoIP call setup at the same time. <code>no</code>—Allows redirection of UDP packets for an unknown UDP port on a receiving gateway to its shelf controller. This is the default value. If the receiving gateway has not yet set up its port caches, the shelf controller receives the UDP packets until the call is fully set up.

Preventing premature fax/modem call time-outs

For H.323 VoIP, the `idle-timer` parameter in the `answer-defaults` profile prevents fax/modem calls from timing out prematurely. By default, once a fax/modem call is initiated at the near-end APX or MAX TNT, it only waits 120 seconds (2 minutes) for a response to the call request from the distant APX. When the near-end TAOS unit doesn't receive a response within that time, the call is dropped.

To ensure that these calls connect properly, the value of the `idle-timer` setting should be set to 0 (`idle-timer = 0`), causing the TAOS unit to wait without timing out for a response to the call request, as in the following example:

```
admin> read answer
ANSWER-DEFAULTS read
admin> list session
[in ANSWER-DEFAULTS:session-info]
call-filter = ""
data-filter = ""
filter-persistence = no
filter-required = no
fill-1 = 0
fill-2 = 0
idle-timer = 0
```

When Connection profiles are used, the value of the `idle-timer` setting should also be set to 0 (`idle-timer = 0`), as in the following example:

```
admin> read connection 1
CONNECTION/1 read
admin> list session
[in CONNECTION/1:session-options]
call-filter = ""
data-filter = ""
old-call-filter = 0
old-data-filter = 0
```

```
filter-persistence = no
filter-required = no
fill-1 = 0
idle-timer = 0
```

device-state profiles

When a DSP card enters the UP state for the first time, a device-state profile is created for each channel. When a DSP card is replaced by a different type of card or by the `slot -r` command, device-state profiles are deleted.

Implementing VoIP audio processing

An APX or MAX TNT performs centralized call processing of VoIP calls. The shelf controller handles the H.323 gateway administration, connection profile administration, and Dialed Number Identification Service (DNIS) call discrimination. The DSP card handles voice processing (such as codec processing, RTP/UDP processing, jitter buffer operation, echo cancellation, etc.).

VoIP audio routing is implemented as follows:

- 1 The caller dials a local access number for a MultiVoice Gateway.
- 2 The call is answered by a TAOS unit. This is the near-end TAOS unit.
 - If the TAOS unit is configured for two-stage dialing, the caller first hears a dial tone from the unit, then enters the destination telephone number. When callers are required to enter a Personal Identification Number (PIN), they enter their PIN at this first dial tone or prompt, then enter the destination telephone number when they hear a subsequent dial tone.
 - If the TAOS unit is configured for single-stage dialing, the caller dials the local access number and destination telephone number as a single string. When callers are required to enter a Personal Identification Number (PIN), they enter their PINs at a prompt from the TAOS unit.
- 3 The TAOS unit routes the call to a DSP on the MultiDSP card.
 - If the trunk connection from the PSTN/PBX supports DNIS signaling (T1/PRI or ISDN), the TAOS unit can use DNIS discrimination to identify VoIP calls.
 - If the trunk connection from the PSTN/PBX does not support DNIS signaling (T1 inband or R2), the TAOS unit uses the value assigned to the default `call-type` parameter in the `call-route` profiles to identify VoIP calls.
- 4 When two-staged dialing is used, the DSP decodes DTMF tones and passes each number entered to the H.323 stack.



Note A MultiVoice Gateway automatically enables a-law companding upon detection of the DTMF by the decode DSP during call setup on a T1 card. As the call comes up on the T1, the DSP checks for a companding mode message that specifies a-law companding. When no message is sent, the DSP defaults to μ -law.

- 5 When the complete number is entered, the H.323 stack does a gateway lookup on the phone number to get the IP address of the far-end TAOS unit.
- 6 The H.323 stack negotiates with its peer on the far-end TAOS unit. Negotiations include exchanging UDP port numbers, frame mode, etc.

- 7 The far-end TAOS unit allocates a DSP on the MultiDSP card and places the outgoing call to the dialed telephone number.
- 8 The far-end TAOS unit informs the near-end TAOS unit when the call connects.
- 9 The callers proceed with the VoIP call.

Configuring VoIP call processing

Configuring VoIP call processing on the TAOS unit consists of two steps:

- 1 Creating the default voi p profile (voi p { 0 0 })
- 2 Configuring the TAOS unit to process calls using IPDC or H.323 protocols

Creating the default voip profile

To configure or modify the VoIP call processing parameters, the default voi p profile (voi p { 0 0 }) must first be created on the TAOS unit. This is done using the **new** and **write** commands:

- 1 Use the **new** command to create the default voi p profile, assigning 0 0 as the profile address:

```
admin> new voip { 0 0 }  
VOIP/{ 0 0 } read
```
- 2 Use the **write** command to save the default profile:

```
admin> write  
VOIP/{ 0 0 } written
```

Configuring routes for VoIP call processing

To configure call routes on an APX or a MAX TNT for VoIP call processing, you must perform the following tasks:

- Route VoIP calls from the PSTN to the MultiDSP cards for processing. This configuration includes the following:
 - Defining the default t-call l-type parameter for inbound call routing
 - Defining DNIS-specific trunk mappings
 - Modifying MultiDSP card call-route profiles to process voice or data calls
 - Defining preferred-source routing
- Route packetized voice across the IP network. This configuration includes the following:
 - Defining IP addressing schemes
 - Defining packet routing for H.323 VoIP calls
 - Configuring host routes or network routes for MultiVoice calls

Call routing parameters

TAOS supports simultaneous processing of VoIP and data calls. To simplify routing of VoIP and data traffic between the TAOS unit and PSTN for non-ISDN signaling trunks:

- Use the default `t-call-type` parameter to identify inbound calls from a T1 or E1 trunk as VoIP or data for ingress call processing.
- Use DNIS-specific trunk mappings for routing of ingress VoIP calls.
- Process data and VoIP calls on different MultiDSP cards.
- Use preferred-source routing method (optional) for processing ingress data call types.
- Use trunk routing (optional) for processing egress VoIP calls.

For trunks using ISDN signalling, a TAOS unit ascertains the bearer capability (voice or data) of a call and uses that information to route the call to a modem (if a voice-service call) or HDLC channel (if a data call).

Using default-call-type for inbound call routing

When a T1 or E1 lines uses inband robbed-bit signaling, the default `t-call-type` parameter in the `call-route` profile specifies the default call-type for incoming calls, for ingress call routing purposes:

Parameter value	Description
<code>digital</code>	Treat incoming calls as digital.
<code>voice</code>	Treat incoming calls as analog calls. Used for routing modem calls from the PSTN.
<code>dni s-or-voice</code>	Assign the call type based on the dialed number (must configure one or more DNIS profiles). Default to voice call type if there is no DNIS match.
<code>dni s-or-digital</code>	Assign the call type based on the dialed number (must configure one or more DNIS profiles). Default to digital call type if there is no DNIS match.
<code>voip</code>	Treat incoming calls as voice over IP.

When `default t-call-type=voip`, all calls received on this trunk are processed as Voice over IP calls. When `default t-call-type=digital`, all calls received on this trunk are processed as digital calls.

For example, if a TAOS unit is connected to a T1 line using inband signaling, the T1 profile contains the following:

```
[in T1/{ shelf-1 slot-1 2 }:line-interface]
signaling-mode=inband
robbed-bit-mode=inc-w-200
default t-call-type=voip
```

As the call comes up from the T1 line, if the `default t-call-type` for the associated T1 is set to `voip`, all calls received over that T1 are processed as VoIP calls. Calls associated with that trunk are routed by the shelf controller to the DSP card for processing.

This same routing method is used when a TAOS unit is configured to process single-stage dialed numbers for H.323 VoIP calls. In this instance, multiple DNIS strings are collected by the TAOS unit. These multiple strings include:

- All or part of the TAOS unit gateway access number (this value is telephone company/provisioning dependent)
- The destination (called) telephone number



Note For trunks using ISDN signaling, use `default t-call-type=voip` on a TAOS unit that processes only VoIP calls, and use `default t-call-type=dni s-or-di gi tal` on a TAOS unit that processes both VoIP and data calls.

To change the value of the `default t-call-type` parameter, enter the commands as follows:

```
admin> read t1 {1 1 2}
T1/{ shelf-1 slot-1 2 } read
admin> set line-interface default t-call-type = voip
admin> write
T1/{ shelf-1 slot-1 2 } written
```

In-bound calls received on all channels of this T1 line will be processed by the TAOS unit as VoIP calls.

Using DNIS-specific trunk mappings

The default `voip` profile, `voip { 0 0 }`, is a systemwide profile used for processing all VoIP calls. Additional `voip` profiles can be created to simplify processing and routing of VoIP calls. These user-defined `voip` profiles map incoming calls by identifying all calls associated with a specific DNIS string as VoIP calls.



Note The `default t-call-type` parameter found in the T1 or E1 profiles should be set to `default t-call-type=dni s-or-di gi tal` when using DNIS-specific trunk mappings.

For example, if you created the following `voip` profiles, the TAOS unit processes all calls from the PSTN with these DNIS strings as VoIP calls.

```
admin> dir voip
 46 12/23/1998 09:48:55 { 0 0 }
 31 12/18/1998 09:50:06 { 8093190 0 }
 31 12/18/1998 10:07:16 { 8903190 0 }
```

The `voip-index` subprofile distinguishes between the default `voip` profile, `voip {0 0}` and any user-defined `voip` profiles:

```
admin> read voip { 8903190 0 }
V0IP/{ 8903190 0 } read
admin> list voip-index
[in V0IP/{ 8903190 0 }:voip-index]
gateway-access-number = 8903190
far-end-number = 0
```

The `voip-index` subprofile includes the following parameters:

Parameter	Setting
<code>gateway-access-number</code>	This is the telephone number dialed by a caller to access the TAOS unit. This telephone number is associated with a T1 trunk, which is used by the TAOS unit to receive in-bound calls from the PSTN. If the TAOS unit is configured to perform two-stage dialing of VoIP calls, this telephone number is dialed to access the TAOS unit.
<code>far-end-number</code>	This is the telephone number dialed by the TAOS unit to connect the call. This value should always be set to 0, since the caller normally enters the destination telephone number.

For DNIS-collecting trunks, a match is done on the DNIS to determine whether a call is a VoIP call. As the call comes from the T1 card, the supplied phone number is run through the current set of Voip profiles. When a match is found between this phone number and the `gateway-access-number` in the `voip-index` subprofile, the call is treated as a VoIP call.



Note Once the TAOS unit is initialized and these changes are committed, save the new configuration to flash memory or a TFTP server. The saved image can be retrieved to restore this configuration in the event that the TAOS unit must be re-initialized.

User-defined voip profiles are defined using the `set`, `new`, and `write` commands.

Using set and write commands to modify default voip profiles

To use the `set` and `write` commands, all the parameters in the default voip profile, `voip { 0 0 }`, must be set to their default values. The default voip profile is used to create user-defined voip profiles.

- 1 Use the `read` command to make the default voip profile the current working profile.
- 2 Use the `list` command to open the `voip-index` subprofile:

```
admin> list voip-index
[in VOIP/{ 0 0 }:voip-index]
gateway-access-number = 0
far-end-number = 0
```
- 3 Use the `set` command to assign the DNIS associated with a gateway access number on the TAOS unit to the `gateway-access-number` parameter:

```
admin> set gateway-access-number = 8903116
```
- 4 Use the `write` command to create the user-defined voip profile:

```
admin> write
VOIP/{ 8903116 0 } written
```



Note Using `set` and `write` does not work if you have already edited other parameters contained in the default voip profile.

Using new and write commands to create user-defined voip profiles

The new and write commands may be used, without restriction, to create user-defined voip profiles:

- 1 Use the read command to make the default voip profile the current working profile.
- 2 Use the new command to assign a profile for the gateway access number:

```
admin> new voip { 8903190 0 }  
VOIP/{ 8903190 0 } read
```

- 3 Use the write command to save the new profile:

```
admin> write  
VOIP/{ 8903190 0 } written
```

Processing VoIP and data calls on different MultiDSP slot cards

To enable the simultaneous processing of voice and data calls, you must create exclusive call routing types for each MultiDSP slot card. You create exclusive call-routing types by deleting call-route profiles for non-VoIP call types.

At startup, when a TAOS unit first detects the presence of a slot card, it automatically creates default call-route profiles to handle different call types. Software licenses on the shelf-controller that are enabled determine which type of call-route profiles are created. For each resource supported by the slot card (digital calls, PHS calls, VoIP calls), a separate call-route profile is created. The TAOS unit uses the presence or absence of a particular profile to filter calls that are accepted and processed by each MultiDSP card.

For each installed MultiDSP slot card, of call-route profiles can be created, these call-route profiles can be created as illustrated in the following callroute command output:

```
admin> callroute -d  
device    #  source      type                tg  sa  phone  
1:03:01/0 1 0:00:00/0  digital-call-type  0   0  
1:03:01/0 2 0:00:00/0  phs-call-type      0   0  
1:03:01/0 3 0:00:00/0  voip-call-type     0   0  
1:03:01/0 4 0:00:00/0  v110-call-type     0   0  
1:03:01/0 4 0:00:00/0  voice-call-type    0   0  
1:03:01/0 4 0:00:00/0  g729-call-type     0   0  
1:03:01/0 4 0:00:00/0  g728-call-type     0   0  
1:03:01/0 4 0:00:00/0  g723-call-type     0   0  
1:03:01/0 4 0:00:00/0  rtfax-call-type    0   0  
1:03:01/0 4 0:00:00/0  frgsm-call-type    0   0
```

The call-route-type parameter in the call-route profile identifies the type of resource (for example, digital-call-type, phs-call-type, voip-call-type). For each supported resource, a new call-route profile is created when the slot card is first installed.

The supported call-route types for the MultiDSP card include:

Table 2-2. Call-route types

Call-Route type	Description
any-call-type	Any type calls can be routed to a device with this call route type.
voice-call-type	Voice bearer calls, which do not include 3.1kHz audio call types or VoIP calls can be routed to a device with this call route type.
digital-call-type	General digital calls, including 3.1kHz audio bearer channel calls, routed to a host device can be routed to a device with this call route type.
trunk-call-type	Digital calls sent to a trunk device used for routing outbound calls to a particular trunk group can be routed to a device with this call route type.
phs-call-type	PHS calls can be routed to a device with this call route type.
v110-call-type	Digital calls recognized as containing V.110 rate-adapted bearer channels can be routed to a device with this call route type.
wormarq-call-type	Digital calls recognized as using WORM-ARQ technology for personal digital cellular phones can be routed to a device with this call route type. <i>WORM-ARQ is not currently supported on the APX 1000 platform.</i>
rtfax-call-type	When using the IPDC protocol, VoIP calls using T.38 fax can be routed to a device with this call route type.
g729-call-type	When using the IPDC protocol, VoIP calls using the G.729(A) codec can be routed to a device with this call route type.
g728-call-type	When using the IPDC protocol, VoIP calls using the G.728 codec can be routed to a device with this call route type.
g723-call-type	When using the IPDC protocol, VoIP calls using the G.723.1 codec can be routed to a device with this call route type.
frgsm-call-type	When using the IPDC protocol, VoIP calls using the Full-Rate GSM codec can be routed to a device with this call route type.
voip-call-type	VoIP calls using the G.711 codec and transparent fax and modem calls ("G.711 fallback") can be routed to a device with this call route type.

With codec-specific call-route types (for example, g729-call-type), more call-route profiles exist per slot card. For example, the 48-port model slot card has 11 call-route profiles because it supports 11 different types of resources (7 of the 11 call-route profiles are dedicated to audio codecs as listed in Table 2-4).

Use the callroute -ih command to view the call-route profiles created for each of the following MultiDSP slot cards:

- **48-port model**
When a universal gateway has only the 48-port model slot card installed, the callroute-ih command displays these call-route profiles:

admin> **callroute -ih**

slot	#	cost	source	type	tg	sa	phone
1:04:00/0	3	40	0:00:00/0	voice-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	digital-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	phs-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	voip-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	v110-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	g729-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	g728-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	g723-call-type	0	0	
1:04:00/0	3	40	0:00:00/0	frgsm-call-type	0	0	

- **96-port model.**

When a universal gateway has only the 96-port model slot card installed, the callroute-ih command displays these call-route profiles:

admin> **callr -ih**

slot	#	cost	source	type	tg	sa	phone
1:05:00/0	3	30	0:00:00/0	voice-call-type	0	0	
1:05:00/0	3	30	0:00:00/0	digital-call-type	0	0	
1:05:00/0	3	30	0:00:00/0	phs-call-type	0	0	
1:05:00/0	3	30	0:00:00/0	voip-call-type	0	0	
1:05:00/0	3	30	0:00:00/0	v110-call-type	0	0	
1:05:00/0	3	30	0:00:00/0	g729-call-type	0	0	

- **240-port model.**

When a universal gateway has only the 240-port model slot card installed and has been hashed for voip only, the callroute-ih command displays these call-route profiles:

admin> **callr -ih**

slot	#	cost	source	type	tg	sa	phone
1:06:00/0	3	20	0:00:00/0	voice-call-type	0	0	
1:06:00/0	3	20	0:00:00/0	digital-call-type	0	0	
1:06:00/0	3	20	0:00:00/0	phs-call-type	0	0	
1:06:00/0	3	20	0:00:00/0	voip-call-type	0	0	
1:06:00/0	3	20	0:00:00/0	v110-call-type	0	0	
1:06:00/0	3	20	0:00:00/0	g729-call-type	0	0	

- **288-port model.**

When a universal gateway has only the 288-port model slot card installed and has been hashed for voip only, the callroute-ih command displays these call-route profiles:

admin> **callr -ih**

slot	#	cost	source	type	tg	sa	phone
1:07:00/0	3	20	0:00:00/0	voice-call-type	0	0	

slot	#	cost	source	type	tg	sa	phone
1:07:00/0	3	20	0:00:00/0	digital-call-type	0	0	
1:07:00/0	3	20	0:00:00/0	phs-call-type	0	0	
1:07:00/0	3	20	0:00:00/0	voip-call-type	0	0	
1:07:00/0	3	20	0:00:00/0	v110-call-type	0	0	
1:07:00/0	3	20	0:00:00/0	g729-call-type	0	0	

- **288-port model configured for 480 ports.**

When a universal gateway has only the 288-port model slot card configured to use 480 ports installed (madd3-voip-480), the call route-ih command displays these call-route profiles:

```
admin> callr -ih
```

slot	#	cost	source	type	tg	sa	phone
1:05:00/0	3	10	0:00:00/0	voip-call-type	0	0	



Note The call-route types for specific codecs (for example, g729-call-type) as defined in Table 2-2 are not supported when the universal gateways are under control of H.323 signaling. H.323 uses H.245 for codec negotiation between endpoints and therefore, call routes cannot specify codecs. For all codecs, only the voip-call-type call-route type can be used with H.323.

Depending upon whether you want the MultiDSP slot card to process VoIP or data calls, delete the call types as follows:

To process this call type	Delete call-route profiles
VoIP calls (voip-call-type)	any-call-type, digital-call-type, v110-call-type
Data calls (digital-call-type)	any-call-type, voip-call-type

For example, if you want a MultiDSP slot card to process only VoIP calls, delete the profiles when the call-route-type parameter is set to digital-call-type or v110-call-type, and any-call-type profiles for that MultiDSP slot card.



Note For all locations except Japan, the phs-call-type call-route profile need not be deleted for MultiDSP slot cards processing voice calls. PHS calls are only supported by PSTNs in Japan.

To remove call-route profiles, do the following:

- 1 Use the show command to identify all the MultiDSP (madd-card) slot cards installed in your TAOS unit:

```
admin>show
```

```
Shelf 1 ( standalone ):
```

{ shelf-1 slot-1 0 }	UP	8e1-card
{ shelf-1 slot-2 0 }	UP	ether3-card
{ shelf-1 slot-3 0 }	UP	madd-card
{ shelf-1 slot-4 0 }	UP	madd-card
{ shelf-1 slot-5 0 }	UP	madd-card

```
{ shelf-1 slot-6 0 }      UP      madd-card
{ shelf-1 slot-7 0 }      UP      madd-card
{ shelf-1 slot-8 0 }      UP      madd-card
admin>
```

- 2 Delete the call-route profiles for each call type you do not want a MultiDSP slot card to accept. To delete the call-route profile for v110-call-type processing on the MultiDSP slot card in slot 3, enter the following command:

```
admin> delete call-route { { {1 3 0} 0} 4}
Delete profile CALL-ROUTE/{ { { shelf-1 slot-3 0 } 0 } 4 }? [y/n] y
CALL-ROUTE/{ { { shelf-1 slot-3 0 } 0 } 4 } deleted
admin>
```

Repeat this procedure for each call-route profile associated with an excluded call type.



Note Modification of the call-route profiles are made after the TAOS unit is initialized. Once the call-route profile changes are committed, save the new configuration to flash memory or a TFTP server. The saved image can be retrieved to restore this configuration in the event that a TAOS unit must be re-initialized.

Configuring preferred-source routing

Using preferred-source routing causes a TAOS unit to direct calls from the designated ingress device (such as, T1 or E1 slot cards) to a specific MultiDSP slot card. This can be used to limit the calls a MultiDSP slot card accepts for processing to a specific T1 or E1 channel and can also be used for routing data calls.

Preferred-source routing is implemented by assigning the address of a T1 or E1 channel to the preferred-source parameter in the call-route profiles for each data-call type configured for a MultiDSP card. The assigned address identifies the shelf, slot, and connection associated with a specific T1 or E1 trunk.

To configure preferred-source routing, enter the following:

- 1 Use the show command to identify all the T1 or E1 cards installed in your TAOS unit:

```
admin>show
Shelf 1 ( standalone ):
{ shelf-1 slot-1 0 }      UP      8e1-card
{ shelf-1 slot-2 0 }      UP      ether3-card
{ shelf-1 slot-3 0 }      UP      madd-card
{ shelf-1 slot-4 0 }      UP      madd-card
{ shelf-1 slot-5 0 }      UP      madd-card
{ shelf-1 slot-6 0 }      UP      madd-card
admin>
```

- 2 For each MultiDSP slot card, change the value assigned to the preferred-source parameter in its call-route profile for digital-call-type. To route calls received through any T1 or E1 line connected on slot 1 to the MultiDSP card in slot 4, enter the following command:

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

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

You may configure a routing using all the T1 or E1 connections on the ingress card, as in the example, or specify an individual trunk by identifying a specific port on the ingress card, for example:

```
admin>set preferred-source={1 1 4} 0}
```

Repeat this procedure until all T1 or E1 trunks are mapped to MultiDSP slot cards.



Note Make this modification after the TAOS unit is initialized. Once these changes are committed, save the new configuration to flash memory or a TFTP server. The saved image can be retrieved to restore this configuration in the event that an TAOS unit must be re-initialized.

Using automatic trunk routing (optional) for outbound voice calls

Trunk routing of outbound VoIP calls controls allocation of egress T1 or E1 trunks. A TAOS unit that connects a VoIP call to the destination telephone number can automatically route calls to the PSTN using a trunk group selected by the TAOS unit that initiated the call.

To utilize this trunk routing method:

- Trunk groups must be enabled on both TAOS units used to connect the call.
- Both TAOS units should have the same number of T1 or E1 trunks available for connecting VoIP calls.
- Both TAOS units must utilize the same trunk numbering scheme.

When trunk prefixing is enabled, the TAOS unit obtains the trunk group number of the ingress T1 trunk from the trunk-group setting in the T1 line profile, and prefixes it to the detected DNIS, the destination telephone number. The TAOS unit modifies the Q.931 Called Party Number information element (IE) in an H.225/Q.931 SETUP message, sending the DNIS number prefixed by the incoming trunk number to the TAOS unit which connects the voice call.

When the destination TAOS unit dials the call, it connects the call to the PSTN using a trunk assigned to the requested trunk group.

Enabling trunk groups

To enable automated trunk group processing of VoIP calls, you must configure the following:

Parameter	Setting
use-trunk-groups (system profile)	This parameter enables the use of trunk groups for all network lines. When this parameter is enabled (yes), all channels must be assigned a trunk group number for outgoing calls.

Parameter	Setting
num-digits-trunk-groups (system profile)	This parameter sets a limit of the number of digits (that is, 1-4) that may be used to designate trunk groups. The value assigned this parameter limits size of the values assigned to the trunk-group parameter to one through four place numbers.
trunk-group (t1 or e1 profile)	This parameter assigns a channel to a trunk group. In a t1 or e1 profile, the default is 9. Individual channels (1 - 9999) may be assigned to different trunk groups.
trunk-prefix-enable (voip profile)	This parameter enables outbound routing of VoIP calls over trunk groups designated by the ingress TAOS unit when set to yes. The ingress TAOS unit sends the trunk group address as part of the dial string for the destination telephone number.

Configuring egress call routing

A TAOS unit can be used as an egress MultiVoice Gateway, that is, used only for connecting calls to the switched telephone network, or as both an egress and an ingress gateway, both accepting calls from and connecting calls to the switched telephone network.

Configuring egress calls only

When egress calls use trunk group routing and a TAOS unit is used only as an egress MultiVoice Gateway, you control trunk group assignments by assigning a nonzero value to the trunk-group parameter in the call-route profile for a E1, T1, or T3 slot card. Using trunk-group=0 in the call-route profile configures the slot card for egress for any VoIP call routed for any trunk group. Since the MultiVoice Gateway is only processing outbound calls to the switched telephone network, assigning the trunk group at the slot level lets MultiVoice perform equal-cost routing of VoIP calls out to the switched telephone network.

For example, if a TAOS unit has three T1 slot cards installed in slot 11, slot 12 and slot 13, equal-cost routing of VoIP calls is achieved by assigning the T1 trunks on each slot to their own trunk group. For the T1 slot card in slot 11 of the TAOS unit, all eight T1 trunks are assigned to trunk group 11 using the trunk-group parameter in the call-route profile as follows:

```
tnt45> read call-route { { {1 11 0} 0 } 0 }
CALL-ROUTE/{ { { shelf-1 slot-11 0 } 0 } 0 } read

tnt45> list
[in CALL-ROUTE/{ { { shelf-1 slot-11 0 } 0 } 0 }
index* = { { { shelf-1 slot-11 0 } 0 } 0 }
trunk-group = 11
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = trunk-call-type
```

Similarly, all T1 trunks on slot 12 would be assigned to trunk group 12, and all T1 trunks on slot 13 would be assigned to trunk group 13. When use-trunk-groups = yes in the system profile, the MultiVoice Access Manager can send instructions to the

TAOS unit to connect a call to the switched telephone network using trunk group 11, group 12, or group 13.

Configuring egress and ingress calls on T3 slot cards

When a TAOS unit is used as both an egress and ingress MultiVoice Gateway and T3 slot cards are used for the trunk connection to the switched telephone network, you assign trunk group numbers for the egress trunk group to the trunk-group parameter in the `t1:line-interface:channel-config:channel-config[n]` profile, and set `trunk-group=0` in the `call-route` profile of the T3 slot card.

When one T3 slot card provides both the ingress and egress connection to the switched telephone network, equal-cost routing of VoIP calls is achieved by assigning T1 trunks to different trunk groups. This provisions the TAOS unit to use different trunks on the T3 slot card for ingress and egress call processing.

For example, if a TAOS unit had a T3 slot card with 28 T1 trunks installed in slot 12, equal-cost routing of VoIP calls is achieved by assigning trunks 1 through 14 to trunk group 12 and trunks 15 through 28 to trunk group 13, at the DS0 level. For each DS0 in trunk group 12 set the trunk-group parameter in the `t1:line-interface:channel-config:channel-config[n]` profile as follows:

```
tnt45> list channel-config
[in T1/{ shelf-1 slot-12 1 }:line-interface:channel-config]

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 `use-trunk-groups = yes` in the system profile, the MultiVoice Access Manager can send instructions to the TAOS unit to connect a call to the switched telephone network using trunk group 12. All trunks in trunk group 13 would be available for processing ingress calls from the switched telephone network.

Configuring egress and ingress calls on several T1 or E1 slot cards

When a TAOS unit is used as both an egress and ingress MultiVoice Gateway and more than one T1 or E1 slot card is used for trunk connections to the switched telephone network, you assign trunk group numbers for the egress trunk group to the trunk-group parameters in both the `call-route` and the `t1:line-interface:channel-config:channel-config[n]` profiles to the egress trunk number. Equal-cost routing of VoIP calls is achieved by assigning the T1 trunks on each slot card to their own trunk groups.

For example, if a TAOS unit has two T1 slot cards installed in slot 12 and slot 13, all eight T1 trunks in slot 12 could be assigned to trunk group 12 as follows:

```
tnt45>list channel-config
[in T1/{ shelf-1 slot-12 1 }:line-interface:channel-config]

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 }
```

Similarly, you assign the T1 slot card in slot 13 to trunk group 13 in its call-route profile. Each DS0 on the trunks on slot 13 would be assigned to trunk group 13. When use-trunk-groups = yes in the system profile, the MultiVoice Access Manager can send instructions to the TAOS unit to connect a call to the switched telephone network using either trunk group 12. The TAOS unit can accept ingress calls from the switched telephone network using trunk group 13.

Configuring egress and ingress calls on a single T1 or E1 slot card

When a TAOS unit is used as both an egress and ingress MultiVoice Gateway and only one T1 or E1 slot card is installed for trunk connections to the switched telephone network, you assign trunk group numbers for the egress trunk group to the Trunk-Group parameters in both the call-route and the t1:line-interface:channel-config:channel-config[n] profiles to the egress trunk number. Equal-cost routing of VoIP calls is achieved by assigning the T1 trunks on each slot card to their own trunk groups.

For example, T1 trunks 1 through 4 could be assigned to trunk group 90, and T1 trunks 5 through 8 to trunk group 91. In the call-route profile, use trunk-group = 90, as illustrated by the following example:

```
tnt45> list  
[in CALL-ROUTE/{ { { shelf-1 slot-12 0 } 0 } 0 }]  
index* = { { { shelf-1 slot-12 0 } 0 } 0 }  
trunk-group = 90  
phone-number = ""  
preferred-source = { { any-shelf any-slot 0 } 0 }  
call-route-type = trunk-call-type
```

When multiple trunk groups are used with trunks on a single E1 or T1 slot card, the value assigned to the trunk-group parameter in the call-route profile should match the value used for the first trunk group assigned to the DS0s connected to the slot card (such as, T1 trunks 1 through 4).

When use-trunk-groups = yes in the system profile, the MultiVoice Access Manager directs the TAOS unit to connect calls to the switched telephone network using the trunk group in the call-route profile, in this case, trunk group 90. The TAOS unit can accept ingress calls from the switched telephone network using trunk group 91.

Priority-based call routing

Priority-based call routing improves call-routing efficiency and flexibility when a single TAOS unit supports a mixture of different MultiDSP slot card models and each model supports different audio codecs.

To configure priority-based call routing, you set a parameter called cost in the appropriate call-route profile.

Priority based call routing

A single universal gateway can support a mixture of the following MultiDSP slot card models in a single chassis:

- 48-port model (TNTV-SL-ADI-C)

- 96-port model (APX8-SL-96DSP)
- 240-port model (APX-SL-DSP-3-L)
- 288-port model (APX-SL-DSP-3)



Note The 288-port model can be configured to use 480 ports for G.711, VoIP-only traffic (see “Configuring 480 ports for G.711-encoded VoIP-only calls” on page 2-65).

Using cost parameter settings in the call-route profile, calls can be routed to a slot card according to its cost value. The lower the cost value of a call route, the higher its priority for selection as the destination slot card for a call.

For example, each MultiDSP slot card model provides a different type of audio codec support. Suppose we have installed a 48-port slot card, a 96-port slot card, and a 288-port slot card in a universal gateway.

- The 48-port model supports these codecs: G.711, G.729(A), G.723.1, Full-rate GSM, Real-time Fax (T.38), and transparent fax/modem.
- The 96-port model and 288-port model support G.711, G.729(A), Real-time Fax (T.38), and transparent fax/modem.

The 288-port model has more ports than the 96-port model, so if a G.711 call is placed, it should be routed to the 288-port model because it has the lowest cost value (see Table 2-3).

Default cost values for MultiDSP slot cards

The default cost value for each slot card can be changed by editing the cost parameter in the appropriate call-route profile for a particular resource (as defined by the call-route-type parameter).

The default cost parameters per MultiDSP slot card are as follows:

Table 2-3. Default cost values

MultiDSP slot card	Default cost of call route
48-port model	cost = 40
96-port model	cost = 30
288-port model	cost = 20
240-port model	cost = 20
480-port model (a 288-port slot card configured with 480 ports)	cost = 10



Note All VoIP call routes for a specific slot card initially activates with the above values.

How calls are routed

For each audio codec, the following table illustrates how calls are routed when using the default cost value in the call-route profile:

Table 2-4. How Calls are Routed Using Cost Values

Audio codec	Slot card order (with lowest cost value first)
G.711	1 480-port model (a 288-port slot card configured with 480 ports). 2 288-port model, 240-port model. 3 96-port model. 4 48-port model.
G.729(A)	1 288-port model, 240-port model. 2 96-port model. 3 48-port model.
Rt-Fax	1 288-port model, 240-port model. 2 96-port model. 3 48-port model.
G.728	1 48-port model.
G.723.1	1 48-port model.
Full-Rate GSM	1 48-port model.

Resetting the slot card

After making changes to any call-route profiles, verify that there are no active calls being processed by the slot card. Then reset the slot card or reset the entire universal gateway. To reset a slot card located in shelf 1, slot 8, proceed as follows:

1 Check to see if the slot card is currently processing active calls:

```
admin> modem -i | grep "1 8"
Modems allocated/in-use:
  Modem { 1 8 3 } ( Up Assign UP UP ENABLE )
```

2 While waiting for active calls to be discontinued, prevent new calls from being routed into this slot card by disabling the modems:

```
admin> mmdisable 1 8
```

3 Keep checking the status of the current calls until all calls are no longer being processed:

```
admin> modem -i | grep "1 8"
You should see the following message before resetting the slot card:
Modems allocated/in-use:
  Modem { 1 8 3 } ( Up Assign UP UP ENABLE )
```

4 Bring the slot down with the following command:

```
admin> slot -d 1 8
```

5 Remove the leftover profiles from the system with the following command:

```
admin> slot -r 1 8  
Slot 1/8, state change forced
```

6 Activate the slot card with the following command:

```
admin> slot -u 1 8
```

7 To show status of the slot card, enter the following command:

```
admin> sh  
Controller { left-controller } (PRIMARY):  
                Req'd  Oper   Slot Type  
{ shelf-1 slot-1 0 }  UP    UP    8t1-card  
{ shelf-1 slot-2 0 }  DOWN  RESET ether3-card  
{ shelf-1 slot-7 0 }  DOWN  RESET t3-card  
{ shelf-1 slot-8 0 }  UP    UP    madd3-voip-480
```

Configuring IP routing for H.323 call processing

There are two methods for implementing IP routing of MultiVoice RTP packets for H.323 VoIP call processing:

- Host routing method, which requires configuring static routes from each Ethernet interface on an TAOS unit to each Ethernet interface on all the other TAOS units in a network that can connect VoIP calls. This method is recommended for small networks, where the network does not provide core support for equal-cost multipath routing. This method requires:
 - Development of an IP addressing scheme
 - Creation of multiple static IP routes on each APX to provide equal-cost multipath routing to all the other APX systems that can connect VoIP calls
 - Defining trunk groups for egress call processing (optional)
- Network routing method, which requires configuring one default route from each Ethernet interface on a TAOS unit to a network switch or router that performs route management, regardless of how many other TAOS unit there are on the network. This method is recommended for networks, where the network provides core support for equal-cost multipath routing. This method requires:
 - Development of an IP addressing scheme
 - Creation of at least one IP route on each TAOS unit to the gateway router/switch used by a TAOS unit to connect with the packet network.
 - Defining trunk groups for egress call processing (optional)

Depending upon the network design, using either the host routing or the network routing method enables equal-cost multipath routing of VoIP calls across the packet network. Equal-cost multipath routing maximizes use of available Ethernet interfaces, packet network channels, etc., to route VoIP calls across the aggregated bandwidth of the packet network between MultiVoice Gateways.

IP addressing schemes

An appropriate IP addressing scheme is required on each TAOS unit to ensure that VoIP packets are properly routed across the packet network. The MultiVoice network administrators should adhere to the following rules when assigning IP addresses to TAOS network interfaces:

- The soft IP address should be unique.
- The IP addresses assigned to individual Ethernet interfaces on shelf controllers and slot cards should be unique.
- The system-ip-addr parameter address and Ethernet 3 card IP address should be on different logical subnets.

Following those configuration rules aids in routing VoIP call data through the Ethernet card interfaces of a TAOS unit, rather than the shelf controllers. Sending call data directly to the shelf controllers causes calls to be rejected, generating a log message similar to the following:

```
LOG warning, Shelf 1, Slot 13, Time: 10:35:25--  
[1/13/93/0] Invalid RTP path (madd->shelf) [MBID 470]  
[V: aa239039-f22c-f002-1d31-0d9dc]
```

Packet routing for H.323 VoIP calls

When two TAOS units involved in an H.323 VoIP call are setting up the VoIP packet connection via H.323 signaling, they use a destination address value equal to the destination's system-ip-addr setting to send voice packets to each other. Proper IP address assignment and route setup are necessary to force RTP packets generated on the DSP card to go directly to an Ethernet slot card rather than the shelf controller. When assigning IP addresses, the following rules apply for all configurations to ensure that VoIP packet routing bypasses the shelf controller:

- Assign the IP addresses on the Ethernet cards in a TAOS unit to logically different subnets.
- Assign the IP address in the system-ip-addr parameter on a TAOS unit to a logically different subnet from any of the Ethernet slot card IP addresses.
- Enable IP Route and IP Port caching in the ip-global profile. For example:

```
admin> read ip-global  
IP-GLOBAL read  
  
admin> set iproute-cache-enable = yes  
admin> set iproute-cache-size = 0 (0 = unlimited size)  
admin> set ipport-cache-enable = yes  
admin> write  
IP-GLOBAL written
```

Configuring host routes

Host route configuration is simple because it doesn't require a network core that supports equal-cost multipath routing. However, host routing requires a more complex configuration on the TAOS unit. Host routing is typically used for environments with a small number of gateways (for example, demo and test environments) since this configuration doesn't use intermediate routers to provide equal-cost multipath routing across the IP network.

The host route method of configuration establishes a host route for every possible destination MultiVoice Gateway for each Ethernet slot card in that TAOS unit. While this can become unwieldy for a network with many MultiVoice Gateways, it simplifies the IP network configurations for networks using few MultiVoice Gateways.

For example, the following tables illustrate the IP addressing scheme for a TAOS unit-173 MultiVoice Gateway, which allows it to route VoIP calls to the TAOS unit-186 MultiVoice Gateway. This is a “back-to-back” configuration.

The IP addresses in Table 2-5 are used as logical network gateways by TAOS unit-173 for sending and receiving VoIP call data across the IP network. The logical network gateways are associated with network ports on the Ethernet-3 slot cards that provide the physical network connection from TAOS unit-173 to the packet network.

Table 2-5. IP address table for TAOS unit-173

System IP address	Ethernet interfaces	IP address
192.168.35.173	{ { 0 0 0 } 0 }*	192.168.35.173/24
	{ { 1 3 1 } 0 }	208.168.25.173/24
	{ { 1 4 1 } 0 }	208.168.15.173/24

* This is the soft IP address by which the TAOS unit is known to the network.

TAOS unit-173 uses the IP addresses in Table 2-6 to define the destination IP address for sending VoIP call data across the network to TAOS unit-196. The host routes are configured by creating two IP Route profiles to TAOS unit-196 on TAOS unit-173. In each IP Route profile, the system IP address for TAOS unit-196 is assigned to the Dest-Address parameter and one of the IP addresses associated with ports on the Ethernet-3 cards in TAOS unit-196, that provide the physical network connection to the packet network, is assigned to the gateway-address parameter.

Table 2-6. IP Routing table for host routes from TAOS unit-173 to TAOS unit-196

dest-address parameter*	gateway-address parameter†
192.168.35.196/32	208.168.25.196
192.168.35.196/32	208.168.15.196

* Using the 32-bit subnet address fully qualifies the IP address, making this a host route.

† This is the Ethernet port IP address of the destination TAOS unit.

The first ip-route profile would be similar to the following:

```
admin> list
[ in IP-ROUTE/tnt_196_1 ]
name* = tnt_196_1
dest-address = 192.168.35.196/32
gateway-address = 208.168.25.196
```


When a VoIP call is established between TAOS unit-173 and TAOS unit-196, call data is transmitted across the packet network using the IP addresses of the Ethernet card ports on these two TAOS units (for example, 208.168.25.173/24 and 208.168.25.196).

For TAOS unit-196, the IP addresses in Table 2-7 are used as logical network gateways to send/receive VoIP call data across the IP network and are associated with network ports on this TAOS unit system's Ethernet-3 cards.

Table 2-7. Host route IP address table for TAOS unit-196

System IP address	Ethernet interfaces	IP address
192.168.35.196	{ { 0 0 0 } 0 }*	192.168.35.196/24
	{ { 1 3 1 } 0 }	208.168.25.196/24
	{ { 1 4 1 } 0 }	208.168.15.196/24

* This is the soft IP address by which the TAOS unit is known to the network.

TAOS unit-196 uses the IP addresses in Table 2-8 to define the destination IP address it uses for sending VoIP call data across the network to TAOS unit-173.

Table 2-8. Host route IP Route table for TAOS unit-196

dest-address parameter*	gateway-address parameter†
192.168.35.173/32	208.168.25.173
192.168.35.173/32	208.168.15.173

* Using the 32-bit subnet address fully qualifies the IP address, making this a host route.

† This is the Ethernet port IP address of the destination TAOS unit.

Configuring network routes

Although configuring network routes requires smarter logic in the IP network, it's much simpler to configure the TAOS unit. The general idea here is to have only one default route for each Ethernet slot card in each TAOS unit, regardless of how many destination gateways or end points exist. For this to work the following rules apply:

- The value of system-ip-addr assigned each TAOS unit must:
 - Be unique.
 - Be on a logically different subnet than any IP address assigned to any Ethernet card in any MultiVoice network.
- No two Ethernet slot card IP addresses may reside on the same logical subnet.
- Routers in the IP network must also have equal-cost multipath routes, so that VoIP packets will get routed to the IP interface on an Ethernet slot card on the destination APX in an equal load-balanced fashion.

For example, the following tables illustrate the IP addressing scheme you use to allow TAOS unit-173 and TAOS unit-196 to connect VoIP calls between them, across an IP network which supports equal-cost multipath routing, using two equal-cost routes.

The IP addresses in Table 2-9 are used as logical network gateways by the TAOS unit-173 to send/receive VoIP call data across the IP network. These are associated with network ports on the Ethernet-3 cards that provide the physical network connection to the packet network.

The value assigned to the `system-ip-addr` parameter is used as the network IP address for TAOS unit-173 itself. The MultiVoice administrator can set the value of the `system-ip-addr` parameter to either the soft IP address configured for the TAOS unit or the IP address of the Ethernet interface on the shelf controller. For this illustration, the `system-ip-addr` parameter for TAOS unit-173 uses the soft IP address.

Table 2-9. Network route IP address table for TAOS unit-173

Ethernet interfaces	IP address [*]
System-Ip-Addr [†]	Anything
{ { 1 3 1 } 0 }	208.168.25.173/24
{ { 1 4 1 } 0 }	208.168.15.173/24
{ { any-shelf any-slot 0 } 0 }	208.168.35.173/32 [‡]

^{*} This IP address can't match the subnet of any Ethernet card IP address or System-Ip-Addr assigned across the network.

[†] This IP address must be on a logically different subnet from any other Ethernet card IP address assigned across the network.

[‡] This is the soft IP address associated with the TAOS unit itself. It will be used for mapping the host route back from the network router.

The IP addresses in Table 2-10 identify the router(s) that direct VoIP calls to/from the IP network for TAOS unit-173. These routers provide the first/last hop on the IP network for calls involving TAOS unit-173. Each network route is configured by creating an `ip-route` profile using the default value for the `dest-address` parameter (`dest-address=0.0.0.0/0`) and one of the IP addresses associated with a network gateway router, that provides the connection between TAOS unit-173 and the packet network, is assigned to the `gateway-address` parameter.

Table 2-10. Network route IP Route table for TAOS unit-173

dest-address parameter	gateway-address parameter [*]
0.0.0.0	208.168.25.1
0.0.0.0	208.168.15.1

^{*} This is the IP address of the network router used for connecting calls with destination TAOS units.

A network route ip-route profile would be similar to the following:

```
admin> list
[in IP-ROUTE/NorthAmerica1]
name* = NorthAmerica1
dest-address = 0.0.0.0/0
gateway-address = 208.168.25.1
```

The IP addresses in Table 2-11 are used by the network router to connect TAOS unit-173 with any destination MultiVoice Gateway or end point. These addresses point back from the network gateway router to TAOS unit-173. The network route method of configuration needs at least two equal-cost host routes pointing back to TAOS unit-173. These pointers should use the soft IP address created for TAOS unit-173 and one of the IP addresses associated with ports on the Ethernet-3 cards in TAOS unit-173.

Table 2-11. Network route IP Route table for network router

Destination IP address*	gateway address†
208.168.35.173/32	208.168.25.173
208.168.35.173/32	208.168.15.173

* Using the 32-bit subnet address fully qualifies the host IP address for the route back to TAOS unit-173. This should match the soft IP address defined for this TAOS unit.

† This is the IP Address of the Ethernet card on TAOS unit-173 used to point back to TAOS unit-173 from the network gateway router.

Any intermediate router between the network gateway router and the destination MultiVoice Gateway or end point should be configured to route VoIP calls meant for IP address 208.168.35.173 to the network gateway router. The router should then equally distribute the packets over the two Ethernet subnets pointing to TAOS unit-173.

The IP addresses in Table 2-12 are used as logical network gateways by TAOS unit-196 to send and receive VoIP call data across the IP network. These are associated with network ports on the Ethernet-3 slot cards that provide the physical network connection to the packet network.

The value assigned to the system-ip-addr parameter is used as the network IP address for TAOS unit-196 itself. The MultiVoice administrator can set the value of the system-ip-addr parameter to either the soft IP address configured for the TAOS unit or the IP address of the Ethernet interface on the shelf controller. For this illustration, the system-ip-addr parameter for TAOS unit-196 uses the soft IP address.

Table 2-12. Network route IP address table for TAOS unit-196 (Page 1 of 2)

Ethernet interfaces	IP address*
system-ip-addr†	Anything
{{ 1 3 1 } 0 }	208.168.25.196/24

Table 2-12. Network route IP address table for TAOS unit-196 (Page 2 of 2)

Ethernet interfaces	IP address*
{ { 1 4 1 } 0 }	208.168.15.196/24
{ { any-shelf any-slot 0 } 0 }	208.168.35.196/32 [‡]

* This IP address can't match the subnet of any Ethernet card IP address or system-ip-addr assigned across the network.

† This IP address must be on a logically different subnet from any other Ethernet card IP address assigned across the network.

‡ This is the soft IP address associated with the TAOS unit itself. It will be used for mapping the host route back from the network router.

The IP addresses in Table 2-13 identify the router(s) that direct VoIP calls to/from the IP network for TAOS unit-196. These routers provide the first/last hop on the IP network for calls involving TAOS unit-196. Each network route is configured by creating an ip-route profile using the default value for the dest-address parameter (dest-address=0.0.0.0/0) and one of the IP addresses associated with a network gateway router, that provides the connection between TAOS unit-196 and the packet network, is assigned to the gateway-address parameter. This router provides the first/last hop on the IP network for calls involving TAOS unit-196.

Table 2-13. Network route IP Route table for TAOS unit-196

dest-address parameter	gateway-address parameter*
0.0.0.0	208.168.45.1
0.0.0.0	208.168.55.1

* This is the IP address of the network router used for connecting calls with destination TAOS units.

A network route ip-route profile for TAOS unit-196 would be similar to the following:

```
admin> list
[in IP-ROUTE/NorthAmerica2]
name* = NorthAmerica2
dest-address = 0.0.0.0/0
gateway-address = 208.168.55.1
```

The IP addresses in Table 2-14 are used by the network router to connect TAOS unit-196 with any destination MultiVoice Gateway or end point. These addresses are used to point back from the router to TAOS unit-196, using its soft IP address.

Table 2-14. Network route IP Route table for network router (Page 1 of 2)

Destination IP address*	Gateway address [†]
208.168.65.196/32	208.168.45.196

Table 2-14. Network route IP Route table for network router (Page 2 of 2)

Destination IP address [*]	Gateway address [†]
208.168.65.196/32	208.168.55.196

* Using the 32-bit subnet address fully qualifies the host IP address for the route back to TAOS unit-196. This should match the soft IP address defined for this TAOS unit.

† This is the IP Address of the Ethernet card on TAOS unit-196 used to point back to TAOS unit-196 from the network gateway router.

Creating static routes

Both the host route method and network route method utilize static routes to send VoIP calls across the packet network. To create static routes for either host or network routes:

- 1 Assign an IP address to the first port on the Ethernet card in shelf 1, slot 3 of TAOS unit-173:

```
admi n> read ip-inter { { 1 3 1 } 0 }  
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } read  
admi n> set ip-address = 208.168.25.173/24  
admi n> write  
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } written
```
- 2 After assigning an IP address to at least one Ethernet port on each TAOS unit in the VoIP network, assign the appropriate IP address to the Gateway-Address parameter which points to an Ethernet port on a distant TAOS unit, to configure a static route between them. For example:

```
admi n> new ip-route zone1  
IP-ROUTE/zone1 read  
admi n> set dest-address = 197.88.10.2/32  
admi n> set gateway-address = 201.10.10.1  
admi n> write  
IP-ROUTE/zone1 written
```

For each of the VoIP static routes, the following values are applied to these parameters in the ip-route profile:

Table 2-15. Static route parameters

Parameter	Specifies	
	Host Route	Network Route
dest-address	This is the fully qualified IP address assigned to the system-ip-addr parameter in the ip-global profile of a destination gateway or end point. This IP address must include the host port identifier (such as, 197.88.10.2/32).	This is always 0. 0. 0. 0. The network router completes the connection to the appropriate IP address on the destination gateway or end point.
gateway-address	This IP address identifies a port on one of the Ethernet slot cards installed on the destination gateway/end point.	This IP address identifies the network router used to contact an TAOS unit which resides on another subnet of the network.

Using multipath routes for VoIP

Using multipath static routes for VoIP traffic across the IP network distributes VoIP traffic across the aggregated bandwidth of multiple Ethernet interfaces. This increases the number of simultaneous calls that can be processed between destinations and reduces call wait times and the number of rejected calls. Each multipath route requires static routes that meet the following criteria:

- Static routes have the same destination address and subnet mask, but different gateway addresses (such as different Ethernet port IP addresses, on different Ethernet slot cards).
- The routes have the same route metric.
- The routes have the same route preference.

If more than one VoIP call comes in for the same destination TAOS unit, the local TAOS unit will check all routes within a multipath route, on a call-by-call basis, and selects the first available route it finds for each call. (For additional information on IP routing, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.)

Configuring routes for IPDC VoIP call processing

Both APX and MAX TNT support IPDC 0.12-controlled VoIP calls over InterMachine trunks (IMTs) for SS7 calls originating from the PSTN. IPDC message tags define all the VoIP parameter values used for processing VoIP calls, overriding the default voip profile (voip { 0 0 }). When initiating an IPDC VoIP call, tag values determine voice

encoding type, packet loading, IP and RPT ports, etc. The default voi p profile (voi p { 0 0 }) value applies only when a specific parameter value is not specified by an IPDC message.

Routing is controlled from the signaling gateway (for example, Lucent Softswitch), which issues instructions for establishing the TDM/IP/RTP connection between the TAOS units involved in the call. Once this connection is established, the TAOS units pass RTP packets, bidirectionally, across the packet network.

Configuring IP routing for IPDC call processing

There are two methods for implementing IP routing for IPDC VoIP call processing:

- Using RTP listen IP addresses selected by the TAOS unit
- Using RTP listen IP addresses selected by the signaling gateway

When the TAOS unit selects its own listen IP address using RMCP/AMCP messages (see “Using RMCP/AMCP messages to route VoIP calls” on page 2-39), VoIP packet routing and configuration is managed in the same way as H.323 VoIP call processing. See “Packet routing for H.323 VoIP calls” on page 2-29 for details.

When the signaling gateway is configured to perform equal-cost routing across multiple IP addresses (each associated with the Ethernet slot cards in the TAOS unit), each Ethernet port must be assigned IP addresses residing on different logical subnets. In this instance, the signaling gateway determines what IP address to use for the call, with based weighting algorithms used by the media gateway controller application.

Packet routing for IPDC VoIP calls controlled from the signaling gateway

To load balance IPDC VoIP calls across Ethernet slot cards (have the signaling gateway allocate IP addresses in an equal fashion) all Ethernet slot card IP addresses must reside on a different logical subnet within the same TAOS unit. Since routing is controlled by the media gateway controller application on the signaling gateway, this is the only configuration required on the TAOS unit. For this to work, the following rules apply:

- The value of the system- i p- addr parameter for each TAOS unit must:
 - Be unique
 - Be on a logically different subnet from any IP address assigned to any Ethernet card in any MultiVoice network
- No two Ethernet slot card IP addresses assigned to the same TAOS unit may reside on the same logical subnet
- The TAOS unit’s IP address must be assigned to SS7-signal packets

The Ethernet IP address configuration, illustrated by Table 2-16, is an example of how IP addresses should be assigned to Ethernet cards to allow equal-cost routing to be done by the signaling gateway.

Table 2-16. Ethernet IP address table for TAOS unit-173

System IP address	Ethernet interfaces	IP address
192.168.35.173	{ { 0 0 0 } 0 }*	192.168.35.173/24
	{ { 1 3 1 } 0 }	208.168.25.173/24
	{ { 1 4 1 } 0 }	208.168.15.173/24
	{ { 1 5 1 } 0 }	208.168.5.173/24

* This is the soft IP address assigned to the TAOS unit.

When VoIP data is passed across the packet network between two TAOS units, the source address contained in the SS7 signaling transport packets is used to establish the return path for VoIP call data sent back to the originating TAOS unit. This source address is the IP address where intermediate network routers send data in response to SS7 VoIP data transmissions. To achieve equal-cost routing for IPDC VoIP calls, that source address must be the IP address (that is, the value assigned to the `system-ip-addr` parameter) of the originating TAOS unit.

For example, the following commands set the system address to the address of a port on an Ethernet card in slot 12:

```
admi n> get ip-interface { { 1 12 1 } 0 } ip-address
[in IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 }:ip-address]
ip-address = 1.1.1.1/24
admi n> read ip-global
IP-GLOBAL read
admi n> set system-ip-addr = 1.1.1.1
admi n> write
IP-GLOBAL written
```

In addition, you must make sure that VoIP calls can always find a route to the next-hop MultiVoice Gateway on the path to the destination MultiVoice Gateway. The route can be learned dynamically or configured as a static route. Many sites choose to configure default routes for VoIP traffic, so that RTP packets are never dropped because of lack of routing information. For example, the following commands configure a default route named VoIP to a next-hop MultiVoice Gateway at 2.2.2.2:

```
admi n> new ip-route voip
IP-ROUTE/voip read
admi n> set gateway = 2.2.2.2/24
admi n> write
IP-ROUTE/VoIP written
```

The IP address of the TAOS unit is assigned to the SS7 signal packets by setting the value of the `use-system-ip-address-as-source` parameter, in the **ss7-systemprofile**, to yes. This inserts the IP address of the originating TAOS unit in the SS7 signaling

transport packets before transmission across the packet network. See “Using the ss7-gateway profile” on page 2-46.

Using RMCP/AMCP messages to route VoIP calls

The request modify call parameters (RMCP) and accept confirm call parameters (AMCP) messages are used to modify parameters for RCCP/ACCP controlled (VoIP) calls. The messages can be used to modify the following parameters:

- VoIP encoding type (G.711, G.729, and so forth) with Tag 0x70. Note that TAOS also supports G.723 (5.4 Kbps) encoding for SS7 VOIP calls. Following are the supported values for VOIP encoding:

Encoding type	Value
G.711 μ -law	0x00
G.723	0x04
G.711 a-law	0x08
G.729	0x12

- Packet Loading (frames/packet) with Tag 0x73. Values depend on VoIP encoding type.
- Destination Port Type with Tag 0x65. Note that for IPDC 0.12 VoIP calls, the only supported values for Source (0x65) and Dest Port (0x66) Type tags are SCN (0x00) and RTP (0x01) respectively.
- Listen IP address with Tag 0x5D.
- Listen RTP port with Tag 0x5E.
- Send IP address with Tag 0x5F.
- Send RTP port with Tag 0x60.

The table below shows the tags supported for the RMCP message:

Tag	Parameter Description	R / O status
0x65	Source port type (PSTN only)	Required
0x07	Source module number	Required
0x0D	Source line number	Required
0x15	Source channel number	Required
0x66	Destination port type (RTP only)	Required
0x70	VoIP encoding type (new G.723 value supported)	Optional
0x73	Packet loading (value depends on VOIP encoding type)	Optional
0x5D	Destination listen IP address (see Note below)	Optional
0x5E	Destination listen RTP port number (see Note below)	Optional
0x5F	Destination send IP address (see Note below)	Optional
0x60	Destination send RTP port number (see Note below)	Optional



Note The last four tags in the table are required if values are nonzero. In addition, if an IP address tag is present, the matching port tag must also be present.

This requirement also applies to the same tags in ACMP messages listed in the table below. RCCP and ACCP messages have been modified to use the same requirements regarding these tags.

The table below shows the tags supported for the AMCP message:

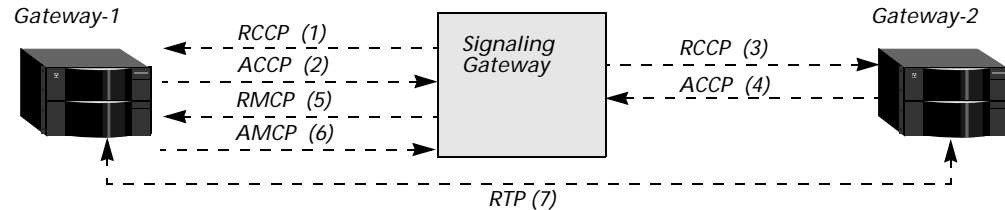
Tag	Parameter Description	R / O status
0x65	Source port type (PSTN only)	Required
0x07	Source module number	Required
0x0D	Source line number	Required
0x15	Source channel number	Required
0x66	Destination port type (RTP only)	Required
0x70	VOIP encoding type (new G.723 value supported)	Required
0x73	Packet loading (value depends on VOIP encoding type)	Required
0x5D	Destination listen IP address	Optional
0x5E	Destination listen RTP port number	Optional
0x5F	Destination send IP address	Optional
0x60	Destination send RTP port number	Optional

Tags 0x70 and 0x73 are required in ACMP messages because RMCP also queries the information for a VoIP call.

Send IP address and Send RTP port tags

With RMCP support of Tags 0x5F and 0x60, the TAOS unit can allocate its own listen IP addresses and RTP ports. The exchanges used in this process are shown in Figure 2-1:

Figure 2-1. Example IPDC message exchanges



IPDC messages to establish RTP listen addresses and ports are exchanged as follows:

- 1 The signaling gateway sends an RCCP message to Gateway-1, in which the RTP port [n] is either not specified or is 0, but with no IP address or RTP port tags.
- 2 Gateway-1 returns its RTP listen IP address and RTP port to the signaling gateway in an ACCP message, using tags 0x5D and 0x5E.
- 3 The signaling gateway sends an RCCP message to Gateway-2, in which the Destination listen IP address and Destination listen RTP port number obtained from Gateway-1 are specified.
- 4 Gateway-2 returns its RTP listen IP address and RTP port to the signaling gateway in an ACCP message, using tags 0x5D and 0x5E.
- 5 The signaling gateway sends an RMCP message to Gateway-1, in which the Destination listen IP address and Destination listen RTP port number obtained from Gateway-2 are specified.
- 6 Gateway-1 returns an AMCP message to the signaling gateway.
- 7 RTP communication commences between the Gateway-1 and Gateway-2.

Related routing issues

For all VoIP calls, it is important to avoid routing RTP traffic through the TAOS unit's shelf-controller. For that reason, when allowing the TAOS unit to allocate its own RTP address, you must set the system-ip-addr parameter in the ip-global profile to an interface address other than the default zero address (which defaults to the shelf-controller Ethernet port). For example, the following commands set the system address to the address of a port on an Ethernet card in slot 12:

```
admin> get ip-interface { { 1 12 1 } 0 } ip-address
[in IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 }:ip-address]
ip-address = 1.1.1.1/24
admin> read ip-global
IP-GLOBAL read
admin> set system-ip-addr = 1.1.1.1
admin> write
IP-GLOBAL written
```

In addition, it is important that VoIP calls can always find a route to the next-hop MultiVoice Gateway on the path to the destination MultiVoice Gateway. The route

can be learned dynamically or configured as a static route. Many sites choose to configure default routes for VoIP traffic, so RTP packets will never be dropped due to lack of routing information. For example, the following commands configure a default route named voip to a next-hop gateway at 2.2.2.2:

```
admin> new ip-route voip
IP-ROUTE/voip read
admin> set gateway = 2.2.2.2/24
admin> write
IP-ROUTE/voip written
```

Reporting IPDC VoIP call statistics

A TAOS unit operating as a network access server (NAS) can report VoIP call statistics in the output of the NAS messaging interface. IPDC VoIP call statistics are reported once a call is cleared. The source that originates call clearing can be either the signaling gateway or the TAOS unit.

Supported tags for reporting statistics

IPDC 0.12 statistics tags are reported when the signaling gateway or a TAOS unit clears calls under the following conditions:

- The access server initiates a call teardown using an RCR message
- The access server acknowledges a call teardown using an ACR message for packet-based calls

Table 2-17 shows statistic-related tags from IPDC 0.12 that are currently supported by the MultiVoice Gateway with their descriptions:

Table 2-17. Supported Statistics Tags (IPDC 0.12) (Page 1 of 2)

Tag	Description
0x91	Number of Real-Time Protocol (RTP) audio packets sent and received by the APX.
0x92	Number of RTP audio packets that failed to reach the APX, determined by missed sequence numbers.
0x93	Number of audio bytes in the RTP payload sent by the APX.
0x94	Number of audio bytes received in the RTP payload that failed to reach the APX. Because the number of bytes per packet is variable, this value can only be estimated based upon an average packet size multiplied by the number of non-received packets. The control server can estimate this value with the information supplied.
0x9D	Number of RTP audio packets received.
0x9E	Number of audio bytes received in the RTP payload.

Table 2-17. Supported Statistics Tags (IPDC 0.12) (Page 2 of 2)

Tag	Description
0xA3	Estimated interarrival jitter (in milliseconds), which is computed as follows: $J = J + (D - J) / 16$ where $D = R(i) - R(i-1) - T $, $R(i)$ is the arrival time of the received packet i , and T is the theoretical difference of departure time between two consecutive packets at the source. For example, T is 5 ms for G711 1 frame per packet, T is 10 ms for G729 1 frame per packet, and T is 40 ms for G729 4 frames per packet.

Unsupported tags for reporting statistics

Table 2-18 shows statistics-related tags from IPDC 0.12 that the MultiVoice Gateway does not support:

Table 2-18. Unsupported Statistics Tags (IPDC 0.12)

Tag	Description
0x95	Number of signaling packets sent and received.
0x96	Number of signaling packets dropped.
0x97	Number of signaling bytes sent and received.
0x98	Number of signaling bytes dropped.
0x99	Estimated average latency.
0x9F	Number of signaling packets received.
0xA0	Number of signaling bytes received.

Call statistics reporting

IPDC 0.15 specifies that the statistics tags are optional, and they are reported in the following cases of call clearing.

- The packet statistics information should be included when the access server initiates a call teardown via RCR message.
- The packet statistics should be included for packet-based calls when the access server acknowledges a call teardown via ACR message.

The TAOS unit reports the statistics in the above two cases when the statistics are available.

ss7nmi debug-level command

The TAOS unit reports VoIP call statistics in the output of the `ss7nmi debug-level` command. When the command is entered with the `-s` option, the results displayed include the number of release channel request (RCR) and release channel completed (ACR) messages sent with and without VoIP call statistics, and the number of unknown SS7 VoIP messages. In the following example, new statistics reported for IPDC VoIP calls are shown in bold type:

```
admin> ss7nmi -s
SS7 NAS Messaging Interface (NMI) statistics:
    Initialized successfully:                Yes
    Total number of internal errors:         0
    Level of diagnostics:                   0
Signaling Layer:
    Current link state:                     UP
    Last generated transaction ID:           182
    Timer T305 (RST1):                     1000 ticks - idle
    Number of protocol version errors:       0
    Number of 'message reject' received:     0
    Number of bad packets received:         0
    Number of unknown messages:             0
    Number of unknown SS7Voip messages:    0
    Number of resource conflicts:           0
    Number of release race conditions:       0
    Number of RCR with stats sent:         0
    Number of RCR without stats sent:      0
    Number of ACR with stats sent:        36076
    Number of ACR without stats sent:     0
Data Transport Layer:
    Number of link fail-overs:              0
    Number of persistent errors:            0
    Last error:                            No Error
    Last error timestamp:                   [09/02/1999 00:00:00]
```

Verifying IP route configuration

To verify the IP route configuration, check the Ethernet port caches and IP caches for each IP interface defined for an TAOS unit.

Verifying VoIP port caches

After creating routes for VoIP packet processing, run the `Ipportmap` command on the TAOS unit to verify the routing between a port on the Ethernet card and a destination TAOS unit. This command must be entered while calls are in progress, as in the following example:

- 1 Open a session with an Ethernet card on the TAOS unit. For example, if the Ethernet card is in Shelf 1, slot 2 of your TAOS unit:

```
admin> open 1 2
ether-1/2>
```
- 2 With a call in progress, enter the `ippportmap` command to verify port mappings:

```
ether-1/2> ipportnap -m
Port  Proto  Addr                Shelf/Slot          Refcnt
1469  UDP      192.168.35.131/32  1/6/0/0            12503
```

When the ports are mapped properly, the output displays the following information in these fields:

Field	Output
Addr	This is the fully qualified destination IP address of the TAOS unit that is using the network port on this Ethernet card to route VoIP packets.
Shelf/Slot	This is the shelf and slot address of the DSP card on the local TAOS unit which processes VoIP packets sent and received across the network.
Refcnt	This is the total number of packets received from the distant TAOS unit. The Refcnt field continues to increment while the call is in progress.

Verifying VoIP route caches

Enter the `ipcache` command to verify internal packet routing between an Ethernet card and a MultiDSP slot card on the TAOS unit. This command must be entered while calls are in progress, as in the following example.

- 1 Open a session with a the MultiDSP slot card. For example, if the DSP card is in shelf 1, slot 6 of your TAOS unit:

```
admin> open 1 6
madd-1/6>
```

- 2 With a call in progress, enter the `Ipcache` command to verify that the proper IP route cache was created:

```
madd-1/6> ipcache cache
Hash Address          Gateway                Shelf/Slot Type    MTU  Switched
142  192.168.35.173  208.168.15.173        1/2    STATIC  1500  512
Forward Stats: To Slots 256, To Shelf 1
Mem Usage: Allocated 1k bytes
Free block count 24
```

When packet routes have been properly cached on the DSP slot card, the output display the following information in these fields:

Field	Output
Address	This is the IP address of the far-end TAOS unit that is sending VoIP packets to the local TAOS unit.
Gateway	This is the IP address of the network router, or the Ethernet card on the far-end TAOS unit, which is used to establish the packet network connection to the far-end TAOS unit.

Field	Output
Shelf/Slot	This is the shelf and slot address of the Ethernet card on the local TAOS unit which is used to establish the packet network connection with the far-end TAOS unit.

Trunk configuration

Trunk configuration controls how network signals are processed by the TAOS unit for VoIP calls. For calls originating from SS7 networks, the TAOS unit is configured to let the signaling gateway (manage network signal processing. For calls processed using H.323, the TAOS unit is configured to detect and respond to call progress signals from a PBX/PSTN.

Interoperating with an SS7 signaling gateway using IPDC

For every TAOS unit that interoperates with a signaling gateway, you must configure the following:

- IP interface to the SS7 signaling gateway running IPDC.
- IPDC messaging interface (SS7 profile).
- T1 line settings for SS7.

For more details on configuring the SS7 interface see the *APX 8000/MAX TNT Physical Interface Configuration Guide*.

Using the ss7-gateway profile

The signaling gateway and TAOS unit communicate over a TCP/IP link. The messaging interface can be a single or dual TCP connection between the TAOS unit and the signaling gateway. When the messaging interface initializes, it opens TCP connections to the specified addresses and ports of the signaling gateway. The TAOS unit keeps the TCP connections open as long as the unit is up and the IPDC messaging interface is enabled. Following are the parameters (shown with default settings) for configuring the messaging interface:

```
[in SS7-GATEWAY]
enabled = no
control-protocol = ipdc-0.X
primary-ip-address = 0.0.0.0
primary-tcp-port = 0
secondary-ip-address = 0.0.0.0
secondary-tcp-port = 0
bay-id =
system-type = IASCTNT1B
transport-options = { 0 1000 3000 30000 7 6 }
use-system-ip-address-as-source = yes
```


Parameter	Setting
enabled	Whether the interface is enabled or disabled the interface. When set to no (the default), the interface is disabled. When set to yes, the interface is enabled if the primary-ip-address and primary-tcp-port also have valid values. Changing the setting from yes to no closes the signaling links but does not disconnect active SS7 calls.
control-protocol	The interface control protocol used for communications between the TAOS unit and the signaling gateway. The specified protocol provides call control for setting up, tearing down, and managing calls between the PSTN and the TAOS unit. The TAOS unit must be licensed for the appropriate code for the required control protocol to communicate with the signaling gateway. For VoIP, the TAOS unit must be licensed for IPDC 0.12, and the value of Control-Protocol should be set to ipdc-0.X.
primary-ip-address	IP address and TCP port to use as the primary IPDC interface.
primary-tcp-port	These settings are required to enable the messaging interface.
secondary-ip-address	IP address and TCP port to use as the secondary IPDC interface. Typically, the primary and secondary address and
secondary-tcp-port	port configurations point to the two Ethernet interfaces of the signaling gateway.
bay-id	This is an alphanumeric string which identifies the TAOS unit to the media gateway controller application. The content of this field is sent by TAOS unit to the signaling gateway during the device registration process. This parameter is not used with IPDC.
system-type	A device identifier used by the signaling gateway to identify the TAOS unit. This parameter is used for registration purposes only. The content of this field must be recorded on the signaling gateway.
transport-options	This subprofile tunes SS7 L2 timers.
use-system-ip-address-as-source	This parameter assigns either the TAOS unit IP address or signaling gateway address as the source address for SS7 signaling transport packets. The value identifies the IP address of the destination where intermediate network routers should direct data in response to SS7 VoIP/data transmissions. When this parameter is set to yes, the default, SS7 signaling transport packets are assigned the TAOS unit's IP address as their source, or outgoing physical interface address. When this parameter is set to no, SS7 signaling transport packets are assigned the signaling gateway IP address.

Transport-options subprofile

The transport-options subprofile allows users to make occasional changes in the operation of SS7 L2 (level 2) timers. The level 2 portion of the message transfer part

(MTP Level 2) provides link-layer functionality. It ensures that the two end points of a signaling link can reliably exchange signaling messages. It incorporates such capabilities as error checking, flow control, and sequence checking.

These timers manage the wait/response intervals for these various singling link processes. Changing these values are useful when customers need to use nonstandard values during system integration and for fine-tuning of their network. This subprofile contains the following fields:

```
[in SS7-GATEWAY: transport-options]
device-id = 0
t1-duration = 1000
t2-duration = 3000
t3-duration = 30000
windows-size = 7
ack-threshold = 6
```

Parameter	Setting
device-id	The logical SS7 command control device where these values apply. This is currently not used.
t1-duration	The value of the ACK delay timer in milliseconds. This timer specifies the maximum delay for an acknowledgement when an I-frame is received. Default value is 1000 (1 second). The value must be less than T2 on the peer. Valid values range from 0-2147483647.
t2-duration	The value of the transmission time-out timer in milliseconds. This timer specifies how long this end point should wait for an acknowledgement. Default value is 3000 (3 seconds). The value must be greater than T1 on the peer. Valid values range from 0 - 2147483647.
t3-duration	Value of the persistent error timer in milliseconds. This timer specifies the maximum duration of attempts to reestablish a link before the transport layer flushes the data queues and sends an error indication up. Default value is 30000 (30 seconds). Valid values range from 0-2147483647.
window-size	The maximum number of sequentially numbered data packets that can be sent while pending acknowledgement at any given time. Default value is 7. Valid values range from 1-63.
ack-threshold	The threshold for triggering an acknowledgment while receiving data packets. As soon as the specified number of packets is received, an ACK is sent back regardless of the value set for the T1 timer. The value of this parameter may not be greater than the window size. Default value is 6. Valid values range from 1-63.

Configuring an IP interface to the signaling gateway

For information about configuring LAN and WAN IP interfaces, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*. That guide also describes standard methods you can use to isolate the interface, such as making the route

private or applying a route filter to the interface, to be certain that only the SS7 messages cross the link between the TAOS unit and the signaling gateway.

Configuring T1 or E1 lines as SS7 data trunks

To configure T1/E1 lines for SS7, you must set the following parameters, shown with sample settings:

```
[in T1/{ shelf-1 slot-1 7 }:line-interface]
signaling-mode = ss7-data-trunk
incoming-call-handling = internal-processing
[in E1/{ shelf-1 slot-10 1 }:line-interface]
signaling-mode = ss7-data-trunk
incoming-call-handling = internal-processing
```

Parameter	Setting for SS7 data trunks
signaling-mode	Must be set to ss7-data-trunk. A line configured as an SS7 data trunk carries no signaling, so it provides 24 (T1) or 32 (E1) 64-kbps channels. When you specify ss7-data-trunk signaling, the line is registered with the IPDC and the IPDC takes control of the line, telling the TAOS unit when to bring calls up or down.
incoming-call-handling	Must be set to internal-processing. Specifies how the TAOS unit processes incoming calls on this line. This value is the same for both H.323 and IPDC VoIP call processing.

Example of configuring a T3 profile

To configure lines of a T3 card as SS7 data trunks, you must first configure the T3 profile as in the following example:

```
admin> read t3 {1 1 1}
T3/{ shelf-1 slot-1 0 } read
admin> set enabled = yes
admin> set frame-type = m13
admin> set line-length = 0-225
admin> write
T3/{ shelf-1 slot-1 1 } written
```

After configuring the T3 line, configure the individual T1 lines that constitute the T3 line as explained in the next section.

Example of configuring a T1 data trunk

The following commands configure a T1 line as an SS7 data trunk, enabling IPDC to control the line:

```
admin> read t1 {1 1 7}
T1/{ shelf-1 slot-1 7 } read
admin> set line-interface enabled = yes
admin> set line-interface signaling-mode = ss7-data-trunk
admin> set line-interface incoming-call-handling = internal-processing
admin> write
T1/{ shelf-1 slot-1 7 } written
```

Example of configuring an E1 data trunk

The following commands configure an E1 line as an SS7 data trunk, enabling IPDC, from the signaling gateway, to control the line:

```
admi n> read e1 {1 10 1}
E1/{ shelf-1 slot-10 1 } read
admi n> set line-interface enabled = yes
admi n> set line-interface signaling-mode = ss7-data-trunk
admi n> set line-interface incoming-call-handling = internal-processing
admi n> write
E1/{ shelf-1 slot-10 1 } written
```

Configuring PRI Tunneling in IPDC (IPDC 0.15)

PRI tunneling allows ISDN layer 3 signaling to be tunneled to a signaling gateway. The external signaling gateway controls the T1/E1 PRI lines terminating on a MultiVoice Gateway.

When the TAOS unit acts an access gateway or trunking gateway, the T1/E1 PRI lines must be made visible to an external signaling gateway. The external signaling gateway uses IPDC for call control on these lines.

In this tunneled PRI signaling scheme, a MultiVoice Gateway handles layer 1 and layer 2 of PRI signaling. All layer 3 Q.931 messages on the D-channel are tunneled to the external gateway by means of an IPDC TUNL message. The bearer channels on the PRI lines are controlled by IPDC call setup and teardown messages.

Requirements

To support PRI tunneling, a TAOS unit requires the following:

- IPDC signaling must be enabled on the TAOS unit (that is, xcom-ss7 must be set to enabled in the base profile).
- The IP address and TCP port to use as the IPDC interface to the SS7 signaling gateway must be specified. Typically, the primary and secondary address and port configurations point to the two Ethernet interfaces of the SS7 signaling gateway. Assign the appropriate IP address to the primary-ip-address parameter and the appropriate port number to the primary-tcp-port parameter in the ss7-gateway profile.
- The signaling-mode parameter must be set to tunneled-pri-signaling in the line-interface subprofile of an t1 or e1 profile. This value allows an external signaling gateway using IPDC to perform call control on T1/E1 lines terminating on a TAOS unit. The TAOS unit recognizes and responds to ISDN signaling, with local B channels controlled by an external signaling gateway. All layer 3 Q.931 messages are tunneled to the gateway configured in the ss7-gateway profile.



Note Only one signaling type can be used on a MultiVoice Gateway or channelized T1/E1 slot card. Only ISDN network terminated (NT) emulation for T1 and T3 lines that are connected to NI-2 and 5ESS/4ESS ISDN switch types are supported.

Reporting PRI tunneling status

The status command reports an active tunneled PRI trunk, using the symbol, "i". This symbol identifies DS0 connections that use ISDN PRI with layer 3 tunneled signaling to the signaling gateway, as illustrated by the following:

```

0 Connections, 0 Sessions | TNT22 Status
                          | Serial number: 9021340  Version: 9.0a0e0
                          |
                          | Rx Pkt: 27763
                          | Tx Pkt: 14688
                          |   col:    2
                          |
                          | 04/06/2000 18:29:42  Up: 0 days, 02:30:20
                          | -----
                          | T-PRI 1/01/01 LA i-----s
                          |           ^

```

Using tunlpri command options

The `tunlpri` command is used to report the status of calls processed using tunneled PRI signaling. This command uses the following syntax:

```
admin> tunlpri -s
```

Using the `-s` option, the `tunlpri` command displays module statistics. To enable tunneled PRI diagnostics, use the following `diag` command to set the desired level for debugging tunneled PRI operations:

```
diag tunlpri level
```

Following are the values you can specify for *level*:

Debug level Specifies

0x00	Diagnostic output is disabled. No debugging information is collected.
0x01	Report errors only. Collect only high level error information as errors occur.
0x02	Show basic debugging traces. Collect session logs.
0x04	Dump Tunnel messages. Collect the IPDC TUNL messages sent to and received from the SoftSwitch.
0x08	Show detailed debugging traces. Collect full session logs, including low-level processing information for tunneled PRI signaling.

The following example illustrates the output of the `tunlpri` command when debug level four (0x04) is specified:

```

admin>tunlpri -s
Tunneled PRI Module statistics:
Interface initialized and ready:      Yes
Current level of diagnostics:        15
Message count:
Received from L2 :                    1068
Sent to L2      :                     754
Received from Tunl:                   945
Sent to Tunl    :                     996

```

```
Errors:
Errors at startup:          0
Warnings:                  0
Module usage errors:       0
NULL pointers:             0
Control Bus errors:        72
Buffer pools errors:       0
Protocol errors:           0
Total:                     72
APX6>
```

Modifications to the ss7nmi command

The ss7nmi debug-level command reports TUNL message statistics when entered as follows:

```
admi n> ss7nmi -m
```

When the command is entered with the -m option, the results displayed include the number of tunneled PRI (TUNL) messages sent or received by the TAOS unit. The ss7nmi debug command includes the following options specifically for IPDC Tunneling debugging:

Options	Specifies
-m	Show TUNL message statistics
-mr	Reset TUNL message statistics
-n	Show active NLCBs (transactions)
-r [address]	Show the status of the SS7 circuit(s). When address is specified, show only status for the selected circuit.
-rc	Toggle, enable or disable, resource backtrace collection. By default, this option is disabled.
-rd [address]	Show detailed status of circuit(s). When address is specified, show only status for the selected circuit.
-s	Show SS7 interface statistics
-sr	Reset SS7 interface statistics

To enable tunneled PRI diagnostics, use the following di ag command to set the desired level for tracing tunneled PRI messaging:

```
di ag ss7nmi level
```

Debug level	Specifies
0x00	Diagnostic output is disabled. No debugging information is collected.
0x01	Report errors only. Collect only high level error information as errors occur.

Debug level	Specifies
0x02	Show signaling link states. Collect information on SS7 link-state changes.
0x04	Show NLCB/transaction states. Collect information on NCLB statuses and transactions state changes.
0x08	Show signaling semantics. Collect information on signaling types associated with each call.
0x10	Display contents of NMI packets. Collect information from network management information packets.
0x20	Show call control interface details. Collect information on the interface used to set up, monitor and tear down each call.
0x40	Show internal task events. Collect information on the low-level processes used for call control.
0x80	Show memory usage. Collect information on the memory allocated by the TAOS unit to process calls.
0x100	Show resource allocation details. Collect information on how TAOS unit resources are allocated for each call.
0x200	Show tunnel basic errors. Collect only high-level tunneling PRI error information as errors occur.
0x400	Show tunnel basic debug. Collect only high-level tunneling PRI debugging information for calls as they occur.
0x800	Dump Tunnel messages. Collect the IPDC TUNL messages sent to and received from the SoftSwitch.
0x1000	Show detailed debugging traces. Collect full session logs, including low-level processing information for tunneled PRI signaling.

The following example illustrates the output of the `ss7nmi -m` command, reporting the TUNL messaging statistics:

```
admin>ss7nmi -m
```

IPDC message processing statistics:

Message code	Received	Sent
RCR (0x0011):	152802	0
ACR (0x0012):	0	152802
RCCP (0x0013):	152847	0
ACCP (0x0014):	0	152847
RMS (0x0041):	1	0
NMS (0x0042):	0	24
RLS (0x0043):	28	0
NLS (0x0044):	0	29
NCS (0x0046):	0	7

TUNL	(0x007a):	611460	611480
RTE	(0x007d):	111	0
ARTE	(0x007e):	0	111
NSUP	(0x0081):	0	1
ASUP	(0x0082):	1	0

Data collection was started: [04/08/2002 17:24:01]

Configuring trunk signaling for H.323 VoIP networks

For every TAOS unit that operates in a H.323 VoIP network and connects to the PBX and PSTN, you must configure the T1 line settings to detect and respond to call progress signaling for H.323 VoIP calls. Set the following parameters, as shown with sample settings:

```
[in T1/{ shelf-1 slot-1 1 }:line-interface]
signaling-mode = inband
robbed-bit-mode = inc-w-200
default-call-type = voip
collect-incoming-digits = yes
t1-inter-digit-timeout = 6000
[in T1/{ shelf-1 slot-1 2 }:line-interface]
signaling-mode = isdn
default-call-type = digital
```

```
[in E1/{ shelf-1 slot-1 1 }:line-interface]
signaling-mode = r1-inband
robbed-bit-mode = inc-w-200
default-call-type = voip
number-complete = 7 digits
caller-id = get-caller-id
e1-inter-digit-timeout = 6000
[in E1/{ shelf-1 slot-1 3 }:line-interface]
signaling-mode = isdn
default-call-type = digital
```


Parameter	Setting
signaling-mode	<p>Type of signal received from the T1 trunk. Set this parameter to:</p> <ul style="list-style-type: none">• <code>inband</code> for non-PRI T1 trunks using inband with robbed bit signaling. When using inband signaling (T1, MF R2), audible tones are used to transmit DNIS/ANI across the trunk.• <code>isdn</code> for T1/PRI trunks. When using ISDN signaling, DNIS/ANI are transmitted in the ISDN call setup message.• <code>dtmf-r2-signaling</code> for R2 signaling trunks. When using DTMF R2 signaling, a DSP is allocated to detect DTMF tones for inbound and outbound calls (see “Enabling DTMF R2 signaling for E1 lines” on page 2-57 for details).• <code>inband-fgd-in-fgd-out</code> for Feature Group D (FGD) signaling on T1 inband trunks. Call signaling data is received and sent in FGD format (see “Enabling and debugging Feature Group D signaling support for T1 lines” on page 2-58 for details).• <code>inband-fgd-in-fgc-out</code> for Feature Group D (FGD) signaling on T1 inband trunks. Call signaling data is received in FGD format and sent in FGC format (see “Enabling and debugging Feature Group D signaling support for T1 lines” on page 2-58 for details).• <code>inband-fgc-in-fgc-out</code> for Feature Group D (FGD) signaling on T1 inband trunks. Call signaling data is received and sent in FGC format (see “Enabling and debugging Feature Group D signaling support for T1 lines” on page 2-58 for details).• <code>inband-fgc-in-fgd-out</code> for Feature Group D (FGD) signaling on T1 inband trunks. Call signaling data is received in FGC format and sent in FGD format (see “Enabling and debugging Feature Group D signaling support for T1 lines” on page 2-58 for details).
robbed-bit-mode	<p>Type of robbed bit-signaling received from an inband T1 trunk. Set this parameter to <code>inc-w-400</code> or <code>inc-w-200</code> for trunks supporting DNIS/ANI.</p>

Parameter	Setting
default-call-type	Default calltype for incoming calls, when using non-PRI T1 trunks (inband with robbed-bit signaling), or when the TAOS unit is configured for single-staged dialing. Set the value of this parameter to voip if all calls received are processed as VoIP calls. For T1 configurations that don't provide DNIS (in-band), this method is required to map an incoming call as a VoIP call. If other call types (such as, modem calls) are received over this trunk, set the value to digital.
collect-incoming-digits (T1)	Enables/disables collection of the Dialed Number Identification Service (DNIS) string for the destination telephone number and Automatic Number Identification (ANI) string of the calling telephone number for an incoming call. For trunks supporting DNIS/ANI, set the value of this parameter to yes. This parameter is ignored when signal-mode=isdn. If two-stage dialing is being used with ISDN signaling, then the two-stage dialing parameter must be set to yes.
caller-id (E1)	Note If DNIS/ANI is present on the T1, you must set this parameter to yes, otherwise the H.323 signaling layer identifies the DNIS/ANI digits as part of the destination phone number dialed by the user. If DNIS/ANI is not desired, provision the PSTN switch/PBX not to send DNIS/ANI.
t1-inter-digit-timeout e1-inter-digit-timeout	How long the TAOS unit waits after receiving the last digit before declaring DNIS/ANI collection complete, when using inband signaling (T1, MF R2). The TAOS unit waits until this interval has elapsed to ensure it has received all audible tones used to transmit DNIS/ANI across the trunk. It may be set to a value between 100 and 6000msec. This parameter defaults to 3000msec. (3 seconds) and works with the Number-Complete parameter when time-out processing is implemented (for details, see "Enabling collections of variable length dial strings without EOP" on page 2-61). Note The call-inter-digit-timeout parameter in the voip profile is used to control collection of keypad generated DTMF entered by the caller, when using two-stage dialing. It has no effect on the collection of DNIS/ANI for T1 signaling.
number-complete	In the E1 profile, the condition that the MultiVoice Gateway uses to determine the length of the dial string. Up to 15 digits can be collected for R2 dial strings without waiting for end-of-pulse (EOP) signaling. Time-out processing can also be implemented by setting this parameter to time-out (see "Enabling collections of variable length dial strings without EOP" on page 2-61 for details).



Note For robbed-bit interfaces, if the default `t-call-type` is `voip` in the `t1` profile, then the bearer capability in the setup message is altered to indicate that this is “packetized voice.”

In-bound calls received on all channels of this T1 will be processed by the TAOS unit as VoIP calls.

Enabling DTMF R2 signaling for E1 lines

MultiVoice Gateway can process Dual Tone Multi-Frequency (DTMF) tones over R2 signaling trunks to provide support for processing either country-specific R2 signaling (MFC-R2) or DTMF signaling over trunks that support standard R2 signaling.

MultiVoice Gateways can support DTMF R2 signaling generated by smaller European network switches and PBXs. MultiVoice implements DTMF tone processing using the R2 signaling standard defined by the International Telecommunications Union Telecommunication sector standard (ITU-T) Q.400, *Specifications of Signaling System R2 Definition and Function of Signals -- Forward Line Signals*.

A channelized E1 slot card uses one of the following channelized associated signaling (CAS) types:

- R1
- R2 or any R2 variant
- DTMF-R2



Note Only one signaling type can be used on an TAOS unit channelized E1 slot card.

To support DTMF-R2 detection, MultiVoice requires the following:

- Connection to E1 trunks that are attached to a switch that supports the ITU-T R2 signaling standard.
- The switch must generate and/or relay the high-frequency/low-frequency tone combinations generated by normal touchtone dialing to the MultiVoice Gateway.
- R2 signaling must be enabled on the MultiVoice Gateway. Verify that the R2 signaling parameter is enabled—check the base profile for `r2-sigaling-enabled=yes`.

Detection of DTMF R2 signals is enabled from the `e1` profile.

DTMF tone detection

When processing tones for DTMF R2 signaling, the MultiVoice Gateway performs as follows:

- Upon detection of an inbound call, allocate a DSP for detecting DTMF tones, capturing DTMF digits as they are received from the switch.
- Upon receipt of an outbound call (from the packet network), allocates a DSP for generating DTMF tones, sending the first DTMF tone for 70ms, followed by 70ms of silence. This tone-silence sequence is repeated until all digits are sent to the telephone switch.



Note A DSP can successfully generate and detect test tones for E1 SS7 continuity testing without impacting detection and processing of E1-R2 signaling. Specifically, the required frequency for the E1 SS7 continuity check, 1780+-20Hz and 2000+-20Hz with the sending tone level of -12+-1dbm0, as defined in ITU

Telecommunication sector standard (ITU-T) Q.724, *Specifications of Signalling System No. 7 - Telephone user part* (1988), International Telecommunications Union, are detected by the DSP. The DSP differentiates between tones in this same frequency ranges which are used for E1-R2 signaling and the E1 SS7 continuity check.

The following is an example of how to enable DTMF R2 signaling on an APX or MAX TNT E1 line slot card.

```
admin> read e1 { 1 1 7 }  
E1/{ 1 1 7 } read  
  
admin> set signaling-mode=dtmf-r2-signaling  
  
admin> set collect-incoming-digits=no  
  
admin> set e1-inter-digit-timeout=3000  
  
admin> write  
E1/{ 1 1 7 } written
```

Using Signaling-Mode parameter for DTMF R2 signaling on E1 lines

One of the settings for the `signaling-mode` parameter in the `e1` profile enables DTMF R2 signaling detection and processing in the `e1` line profile. Setting the value of the `signaling-mode` parameter to `dtmf-r2-signaling` value enables the TAOS unit to recognize and respond to the DTMF R2 signal set during voice and data calls. Once selected, DTMF R2 detection is enabled with the next VoIP call.

The following dependencies apply when `signaling-mode=dtmf-r2-signaling`:

- `collect-incoming-digits` must be enabled (`collect-incoming-digits=yes`).
- Assigning a lower value (such as 600 to 3000) to the `e1-inter-digit-timeout` parameter improves call setup times. Assigning a higher value (such as 3001 to 6000) improves detection of DTMF.
- DTMF R2 detection is only supported when R2 signal processing is enabled for the TAOS unit. The Base profile should contain the following setting:

`r2-signaling-enabled=yes`

Enabling and debugging Feature Group D signaling support for T1 lines

MultiVoice supports a subset of the Telecordia requirements for Feature Group D (FGD) signaling for Voice over IP processing, such as passing Automatic Number Identification II (II) information, Calling-Party-Number and Called-Party-Number as MFR1 tones on inc-wink signaled trunks. A MultiVoice Gateway can manage interworking between Access Tandem carriers and traditional toll service carriers for VoIP calls. It also provides basic support for trunk-side access with Equal Access dialing capability, pre subscription, and enhanced signaling options for Automatic Number Identification as specified by Requirement GR-690-CORE, *Exchange Access Interconnection FAS 20-24-0000* (Oct. 1995), Telecordia Systems (formerly Bellcore).

Feature Group D access service with equal access multifrequency signaling is characterized by two-stage outpulsing when connection is made through the access tandem. The first stage provides information to the AT for selection of a carrier and the route to take to that carrier. The second stage provides the carrier with both the calling-party-number (and, optionally, ANI) and the Called-Party Number (address or destination number). Overlap outpulsing is used to transmit this information using multifrequency signaling.

Pass-through of equal access signaling can be enabled for T1 inband trunks from the T1 line profile. When FGD signaling is enabled, MultiVoice Gateways can recognize and process the single-dialed access carrier destination, (such as: 1,2025551212 or 1,1010220,2025551212). To support access carrier billing, a MultiVoice Gateway passes the Calling-Party-Number, ANI information digits and Called-Party-Number. The ANI information digits, a two-digit code, classifies the Calling-Party-Number by tariff type (such as coin, 800 service, or POTs).

MultiVoice also manages interworking when connecting VoIP calls between Access Tandem networks and traditional toll service networks. An egress MultiVoice Gateway can be configured to receive Calling-Party Number, ANI information digits, and Called Party-Number from an Access Tandem switch and connect that call to a switched telephone network that supports Feature Group C (FGC), that is, traditional toll service and switching. FGC includes automatic number identification of the calling party, answerback, and disconnection supervision. FGC service predates the breakup of the Bell System.

T1 profile

Feature Group D licensed software for MultiVoice Gateways adds FGD signaling options to the `signaling-mode` parameter in the `t1` profile to enable inband signal processing of FGD signals, and interworking of MultiVoice networks between Access Tandem carriers and traditional toll-service carriers.

fgd-signaling-enabled parameter

Following installation of TAOS, each MultiVoice Gateway must be loaded with licensed software code to enable processing of Feature Group D signaling. When enabled, `fgd-signaling-enabled` parameter appears in the base profile.

During manufacturing or software upgrade of MultiVoice Gateways, the installation binaries used to install TAOS on the TAOS unit asks if FGD support should be enabled. FGD support can only be enabled or disabled by reinstalling the licensed software on the TAOS unit.

When support for FGD is enabled, the `fgd-signaling-enabled` parameter is added to the base profile, as illustrated:

```
admin> read base
BASE read (read-only)

admin> list
[in BASE]

shelf-number = 1
software-version = 8
software-revision = 0
software-level = ""
manufacturer = dba-ascend-mfg
....
fgd-signaling-enabled = yes
```

Using the signaling-mode parameter to configure FGD signaling

The `signaling-mode` parameter in the `t1:line-interface` subprofile identifies the type of call signal received from the ingress switched telephone network and the type of call signals passed to the egress switched telephone network. New values may be assigned to the `Signaling-Mode` which enable processing of FGD inband signaling for connecting Equal Access calls, and support interworking between Access Tandem and traditional toll service networks.

The `signaling-mode` parameter may be assigned the following values to enable FGD signaling support:

Parameter	Setting
<code>inband-fgd-in-fgd-out</code>	Configures the MultiVoice Gateway to expect to receive call signaling data in FGD format, and connect VoIP calls to the egress switched telephone network, sending call signaling data in FGD format.
<code>inband-fgd-in-fgc-out</code>	Configures the MultiVoice Gateway to expect to receive call signaling data in FGD format, and connect VoIP calls to the egress switched telephone network sending call signaling data in FGC format.
<code>inband-fgc-in-fgc-out</code>	Configures the MultiVoice Gateway to expect to receive call signaling data in FGC format, and connect VoIP calls to the egress switched telephone network sending call signaling data in FGC format.
<code>inband-fgc-in-fgd-out</code>	Configures the MultiVoice Gateway to expect to receive call signaling data in FGC format, and connect VoIP calls to the egress switched telephone network sending call signaling data in FGD format.

Changes made to the `signaling-mode` parameter take effect with the next VoIP call. The following example illustrates how to enable a MultiVoice Gateway to receive call signaling data in FGD format and send call signaling data to the egress switched telephone network in FGC format signalling using the `signaling-mode` parameter.

```
admin> read t1 { 1 1 1 }
T1/{ 1 1 1 } read
admin> list line
[in T1/{ shelf-1 slot-1 1 }:line-interface]
enabled = yes
frame-type = esf
encoding = b8zs
signaling-mode = inband
.....
ss7-continuity = { loopback single-tone-2010 }
admin> set signaling-mode=inband-fgd-in-fgc-out
admin> write
T1/{ 1 1 1 } written
```

For the `signaling-mode` parameter to include FGD signaling options, the MultiVoice Gateway must have licensed software code for FGD processing.

Feature Group D signaling timing

To ensure wideranging interoperability with available access tandem switches, MultiVoice uses the middlerange Feature Group D Signaling Timing.

- Wait up to 210 msec for first wink from the Access Carrier. Requirement GR-690-CORE specifies a range of 140-290 msec.
- Wait up to 5 seconds to receive the first digit. After sending the first wink on receipt of an off hook, the MultiVoice Gateways waits for 5 seconds before reporting a time-out error if the first digit signal is not received.
- Wait up to 4 seconds for a wink from the Access Carrier. Requirement GR-690-CORE specifies Access Tandem switches wait for up to 4 seconds for this signal.

Debugging Feature Group D signaling

To collect debugging information for Feature Group D inband signal processing on a TAOS unit, enter the following commands:

```
TnT01> open 1 1          (where the T1 slot card is)
TnT01> fgdtoggle         (turn on fgd signalling debugging)
TnT01> debug on
```

The debug command displays information similar to the following for Feature Group D signal processing.

```
-----
0 Connections, 0 Sessions | TNTFGD Status
                          | Serial number: 9340872 Version: 9.0a0e0
                          |
                          | Rx Pkt:    1057139
                          | Tx Pkt:    163995
                          | Col:       2244
                          |
                          | 02/29/2000 17:50:27 Up: 7 days, 00:17:30
                          | "T3 Tru+ 1/03/00 LA la la la la la la la
                          | "T3 Fiv+ 1/03/01 LA F-----
                          | "T3 CDX" 1/03/02 LA F-----
                          |
                          | ^
                          | |
                          | +-- display (F) for FGD line
                          |
                          |
-----
```

Enabling collections of variable length dial strings without EOP

The MultiVoice Gateway collects variable-length dial strings without using end-of-pulse (EOP) signaling. In certain areas outside the continental United States where E1 MFC-R2 signaling is used for switched network operations, the length of E.164 addresses vary. End-of-pulse (EOP) detection is not efficient, since the network may be unable to complete the call as a result of network conditions.

Collection of up to 15-digits

MultiVoice Gateways are compatible for use on European telephone systems that use E.164 addresses that are up to 15 digits long, without waiting for an end-of-pulse signal.

Previously, MultiVoice Gateways could be configured to collect dial strings of up to only 11 digits. For European networks using dial strings that were 12 digits or longer, a MultiVoice Gateway could only be configured to wait for the end-of-pulse signal to confirm it received all the dialed digits.

The number of configurable digits to 15 for the E1 line number-complete parameter is set in the e1:line-interface sub-profile.

The number-complete parameter enables detection and collection of up to 15 digits for inbound dialed telephone numbers on MultiVoice Gateways using E1 trunks supporting inband CMF R2.

The parameter now accepts values from 0-digits through 15-digits, end-of-pulse, and time-out as valid entries.

The following example illustrates how to enable the collection of 15 digit dial strings on a TAOS unit:

```
admin> read e1 { 1 1 7 }  
E1/{ 1 1 7 } read  
  
admin> set number-complete=15-digits  
  
admin> write  
E1/{ 1 1 7 } written
```

The following dependencies apply to this parameter:

- The number-complete parameter defaults to N/A when the signaling-mode parameter is assigned any of the following values:
 - e1-kuwait-signaling
 - isdn
 - p7
 - dpnss
 - none

Time-out processing

A MultiVoice Gateway can be configured to time-out, followed by pulse signals, as specified by ITU-T Recommendation Q.442, *Specifications of Signalling (sic) System R2 interregister Signalling (sic), Pulse Transmission of Backward Signals A-3, A-4, A-6 or A-15* (1993), International Telecommunications Union.

Using time-out allows a MultiVoice Gateway to delay processing of a dialed number string, even after receiving the last digit, to allowing the resources on the switched network additional time to become available, before continuing with call processing.

To implement this feature, modify entries for the number-complete and inter-digit-time-out parameters.

The number-complete parameter sets the condition the MultiVoice Gateway uses to determine the length of the dial string. For E1 MFC-R2, the MultiVoice Gateway

continues to collect digits until the on/off pulsing using to transmits the dial string is complete.

The `number-complete` parameter now accepts the following value:

Parameter value	Description
<code>time-out</code>	Configures the MultiVoice Gateway to reset the network idle timer after the initial digit is received, and then wait for silence. Once silence is detected, wait the interval specified by the <code>inter-digit-time-out</code> parameter for next digit. The MultiVoice Gateway continues to collect digits, while waiting for the network idle timer to expire before continuing with call processing.

The following illustrates how to configure a MultiVoice Gateway to determine the length of a dial string using time-out processing.

```
admin> read e1 { 1 1 1 }
E1/{ 1 1 1 } read

admin> list line
[in E1/{ shelf-1 slot-1 1 }:line-interface]

enabled = yes
frame-type = esf
encoding = b8zs
signaling-mode = inband
.....
ss7-continuity = { loopback single-tone-2010 }

admin> set number-complete=time-out
admin> write
```

E1 MFC-R2 signaling is country specific. The `signaling-mode` parameter, and the `country` parameter in the system profile, must be set for the country-appropriate signaling in order for the MultiVoice Gateway to properly detect dialed digits.

In the `e1:line-interface` subprofile, the `inter-digit-time-out` parameter controls how long a MultiVoice Gateway will wait after receiving the last digit of a dial string before declaring DNIS/ANI collection complete. When using inband signaling (T1, MF R2), a TAOS unit waits until this interval has elapsed to ensure it has received all audible tones used to transmit DNIS/ANI across the trunk.

The `inter-digit-time-out` parameter accepts values between 100 and 6000msec. This parameter defaults to 3000msec (3 seconds). For configurations supporting E1 MRC R2 signaling, the `inter-digit-time-out` parameter accepts values between 200 and 6000msec.

The following illustrates how to configure the interdigit timer on a MultiVoice Gateway to wait one second (1000msec) in between dialed digits before continuing with call processing.

```
admin> read e1 { 1 1 1 }
E1/{ 1 1 1 } read
```

```
admin> list line
[in E1/{ shelf-1 slot-1 1 }:line-interface]
enabled = yes
frame-type = esf
encoding = b8zs
signaling-mode = inband
.....
ss7-continuity = { loopback single-tone-2010 }
admin> set inter-digit-time-out=1000
admin> write
```

E1 MFC-R2 signaling is country specific. The signaling-mode parameter in the e1 profile and the country parameter in the system profile must be set for the country-appropriate signaling for the MultiVoice Gateway to properly detect dialed digits.

Processing ANI and DNIS for H.323 VoIP

Regardless of whether a TAOS unit is configured for single stage-dialing or two-stage dialing, the master DSP or slave DSP parses the dual-tone multifrequency (DTMF) tones in the following order, based on how the tones were processed by the PSTN/switch:

```
CLID*DNIS
DNIS
CLID*DNIS*
```

When the local TAOS unit connects with the destination TAOS unit involved in a call, the reported DNIS and ANI/CLID, which are included as part of the call setup message(s), are used as follows:

String	Description
ANI/CLID	<p>The Automatic Number Identifier or Calling Number Identification string of the caller's telephone:</p> <ul style="list-style-type: none">• At the destination gateway, this number identifies the origin of the call. Once received by the destination gateway, the number is exported for use by gateway applications, passed back to the calling gateway to confirm call setup, etc.• At the local gateway, this number is collected then forwarded to the destination gateway and the MultiVoice Access Manager, where it may be used for authentication, call reporting, third-party billing applications, etc.• At the destination gateway, this number is passed to the PSTN and used for initiating local switched network services that process CLID (such as Caller ID, call waiting, last number redial, etc.).

String	Description
DNIS	<p>The Dialed Number Identification Service string that identifies the called telephone:</p> <ul style="list-style-type: none">• At the destination gateway, this number is the destination telephone number dialed by the MultiVoice Gateway.• At the local gateway, this number is the dial string entered by the caller for the destination telephone number.

Configuring 480 ports for G.711-encoded VoIP-only calls

The MultiDSP 288-port slot card (APX-SL-DSP-3) in an APX 8000 or APX 1000 supports the following modes:

- 288 ports of universal port traffic (that is, simultaneous V.110 and V.92 modem, High-Level Data Link Control (HDLC), Personal Handyphone System (PHS), T.38 Fax, VoIP with G.711, G.729(A) audio codecs). This is the default mode.
- 480 ports of G.711 VoIP-only calls for H.323 and IP device control (IPDC) protocols.

Sites that use the G.711 codec in their networks have the option to configure 480 ports, which lowers the cost of network equipment and operation.

To support 480 ports of G.711 VoIP-only traffic, the following conditions must be met:

- The universal gateway must be an APX 8000 or APX 1000 unit.
- The MultiVoice software license for each universal gateway must be enabled. Additional software licenses or hardware are not required.
- The frames-per-packet parameter in the voi p profile must be set to 4 or greater. The maximum number of frames per packet you can set is 10. If a number lower than 4 is set, the value is automatically reset to 4 and a log message is generated.



Note The value specified for the frames-per-packet parameter (4 - 10) must be supported by all MultiDSP slot cards in the chassis. If using the IPDC protocol, the softswitch should use four frames per packet for all calls.

Transparent fax and modem

Regular modem (for example, v.90/v.92) and T.38 fax capability are not supported in the 480 port configuration. However, when configured for 480 ports, the slot card uses two frames per packet for transparent fax and modem.

The slot card can handle only a maximum of 96 transparent fax and modem calls per quadrant. When using priority-based call routing (see “Priority-based call routing” on page 2-25), all G.711 calls are routed to the slot card. Even if other MultiDSP slot cards also handle transparent fax, Lucent recommends allowing only a maximum of 96 transparent calls per quadrant.

Compatibility with other MultiDSP slot cards

When using IPDC and the slot card is configured for 480 ports of G.711 VoIP-only traffic, the MultiDSP 288-port slot card can coexist with 48-port and 96-port MultiDSP universal port slot cards that use other codecs.

However, when using H.323 and the slot card is configured for 480 ports of G.711 VoIP-only traffic, only G.711 is supported by all MultiDSP universal port slot cards.

New value for subtype parameter

When the slot card is activated initially, the system checks for the presence of a `madd-slot-config` profile.

If the profile exists, the system examines the subtype parameter to determine the number of ports the slot card supports. If the profile does not exist, then the slot card operates with the default 288 universal ports.

The values for the subtype parameter are:

Parameter Value	Description
480-voip-ports	Configures the slot card for 480 ports.
288-univ-ports	Configures the slot card for 288 ports. Default mode.

Configuring the slot card for 480 ports

To configure the MultiDSP 288-port slot card for 480 ports, create a new `madd-slot-config` profile and specify a value for the subtype parameter.

The following example configures the slot card that resides in shelf 1, slot 8:

```
admin> new madd-slot-config { 1 8 0 }
MADD-SLOT-CONFIG/{ shelf-1 slot-8 0 } read
admin> list
[in MADD-SLOT-CONFIG/{ shelf-1 slot-8 0 } (new)]
slot-address* = { shelf-1 slot-8 0}
subtype = 288-univ-ports

admin> set subtype = 480-voip-ports
admin> wr
```

Resetting the slot card

After making changes to the `madd-slot-config` profile, verify that there are no active calls being processed by the slot card. Then reset the slot card or reset the entire universal gateway. To reset a slot card located in shelf 1, slot 8, proceed as follows:

1 Check to see if the slot card is currently processing active calls:

```
admin> modem -i | grep "1 8"
Modems allocated/in-use:
  Modem { 1 8 3 } ( Up Assign UP UP ENABLE )
```

2 While waiting for active calls to be discontinued, prevent new calls from being routed into this slot card by disabling the modems:

```
admin> mmdisable 1 8
```

3 Keep checking the status of the current calls until all calls are no longer being processed:

```
admin> modem -i | grep "1 8"
```

You should see the following message before resetting the slot card:

Modems allocated/in-use:

```
Modem { 1 8 3 } ( Up Assign UP UP ENABLE )
```

4 Bring the slot down with the following command:

```
admin> slot -d 1 8
```

5 Remove the leftover profiles from the system with the following command:

```
admin> slot -r 1 8
```

Slot 1/8, state change forced

6 Activate the slot card with the following command:

```
admin> slot -u 1 8
```

7 To show status of the slot card, enter the following command:

```
admin> sh
```

Controller { left-controller } (PRIMARY):

	Reqd	Oper	Slot Type
{ shelf-1 slot-1 0 }	UP	UP	8t1-card
{ shelf-1 slot-2 0 }	DOWN	RESET	ether3-card
{ shelf-1 slot-7 0 }	DOWN	RESET	t3-card
{ shelf-1 slot-8 0 }	UP	UP	madd3-voip-480

Reverting to universal port mode

To revert to using 288 universal ports, use the following commands. The example assumes that the slot card has been installed in shelf 1, slot 8:

```
admin> read madd-slot-config { 1 8 0 }
```

```
MADD-SLOT-CONFIG/{ shelf-1 slot-8 0 } read
```

```
admin> list
```

```
[in MADD-SLOT-CONFIG/{ shelf-1 slot-1 0 } (new)]
```

```
slot-address* = { shelf-1 slot-8 0 }
```

```
subtype = 480-voip-ports
```

```
admin> set subtype = 288-univ-ports
```

```
admin> wr
```

After making changes to the madd-slot-config profile, reset the slot card or reset the entire universal gateway (see “Resetting the slot card” on page 2-66 for details).

In-call DTMF detection for IPDC

You can configure your TAOS unit to allow Softswitch to direct the MultiVoice Gateway to perform in-call DTMF detection and notification while a packet call is in progress. This is accomplished by modification of the RCCP, RMCP, and NTN messages. Any DTMF digits entered during the call while DTMF detection is enabled are still played out to the other party.



Note In-call DTMF detection is supported for packet calls, but not for time-division multiplexing (TDM) calls. Also, this feature requires obtaining a pre-paid billing application.

IPDC messages that support in-call DTMF detection

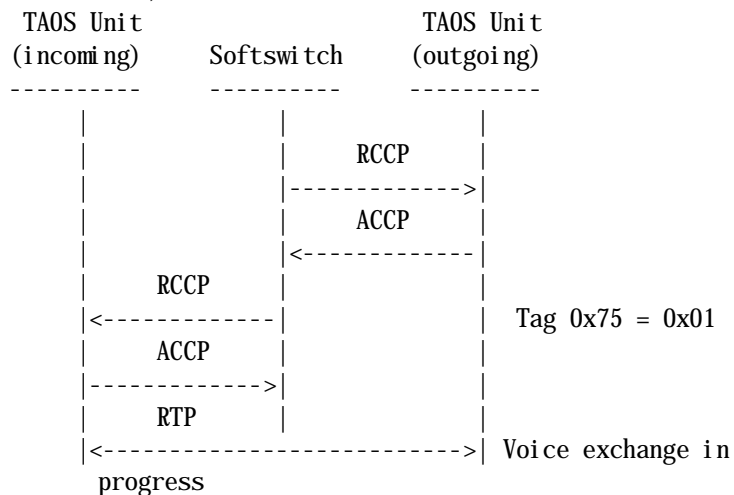
Following are IPDC messages (as defined in IPDC specification *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15*) that support in-call DTMF detection and notification.

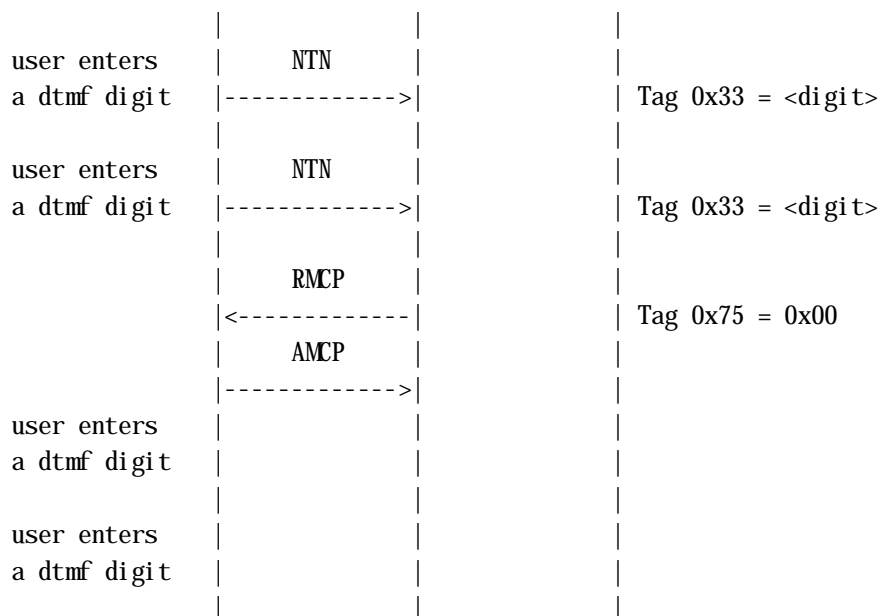
Table 2-19. IPDC messages supporting in-call DTMF detection and generation

IPDC message	Tag	Tag values
RCCP	0x75 (Constant DTMF Tone Detection)	<ul style="list-style-type: none"> 0x00 - DTMF tone detection off 0x01 - DTMF tone detection on <p>If a tag is missing, DTMF tone detection is off.</p>
RMCP	0x75 (Constant DTMF Tone Detection)	<ul style="list-style-type: none"> 0x00 - DTMF tone detection off 0x01 - DTMF tone detection on <p>If a tag is missing, there is no affect on the current state of detection.</p>
NTN	0x49 (Tone Type)	<ul style="list-style-type: none"> 0x01 - DTMF tone
NTN	0x33 (Tone String)	This tag contains the DTMF digit that was detected. The length of this tag value is 1.

Call Flow

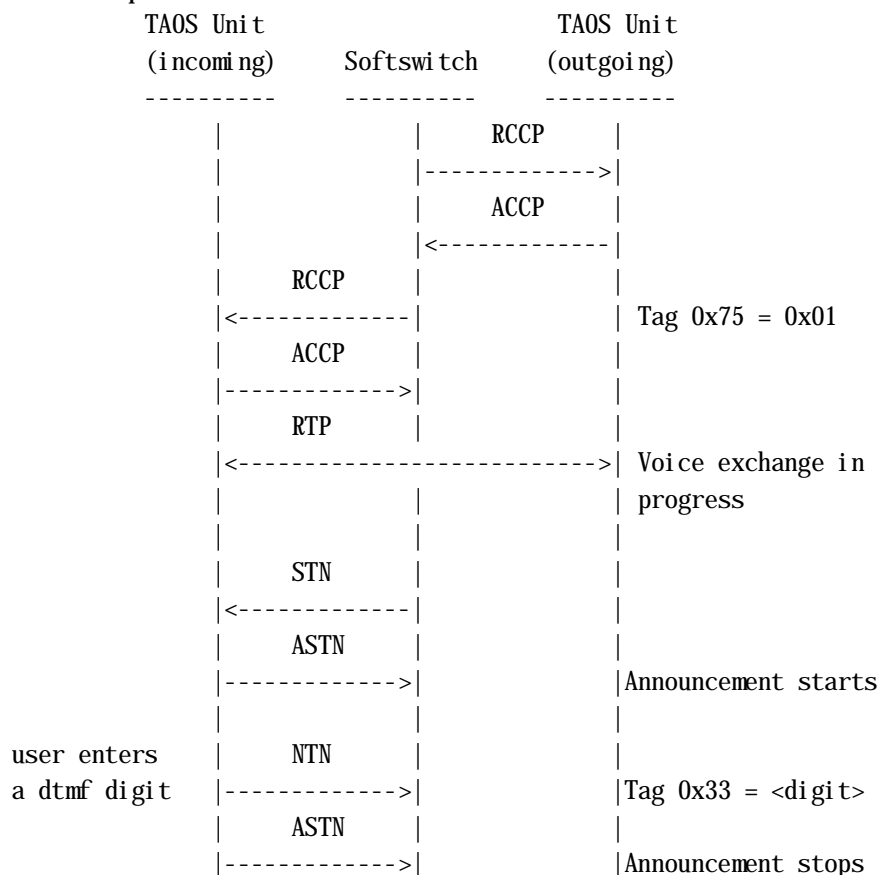
In the following call flow, a packet call is setup with DTMF detection enabled. After two DTMF digits are entered, the call is modified to disable DTMF detection.





Interaction with break-in voice announcements

If in-call DTMF detection is enabled and a break-in announcement is played (see “Break-in voice announcements in IPDC” on page 4-6 for details), the first DTMF entered will stop the announcement:



An RMCP that is received by the MultiVoice Gateway while a break-in announcement is playing is rejected. An MRJ will be sent with Tag 0xFE (Cause Code) set to 0x65 (Message Not Compatible With Call State).



Note 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

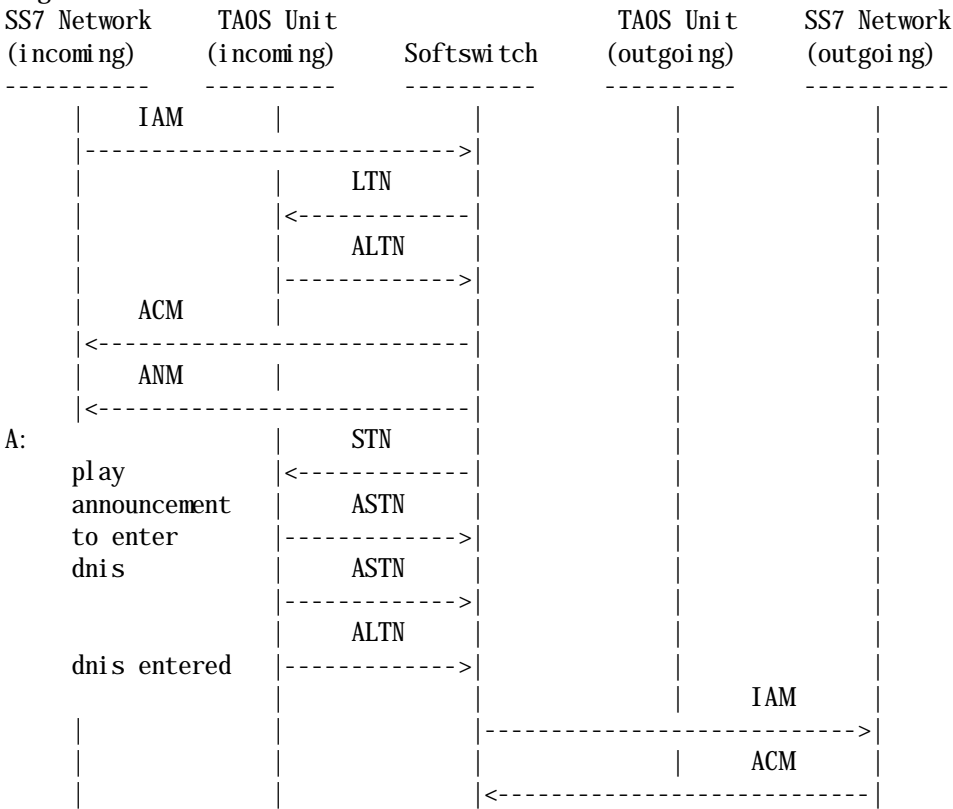
In-call DTMF detection can be combined with existing IPDC support on the MultiVoice Gateway to provide a call re-origination application.

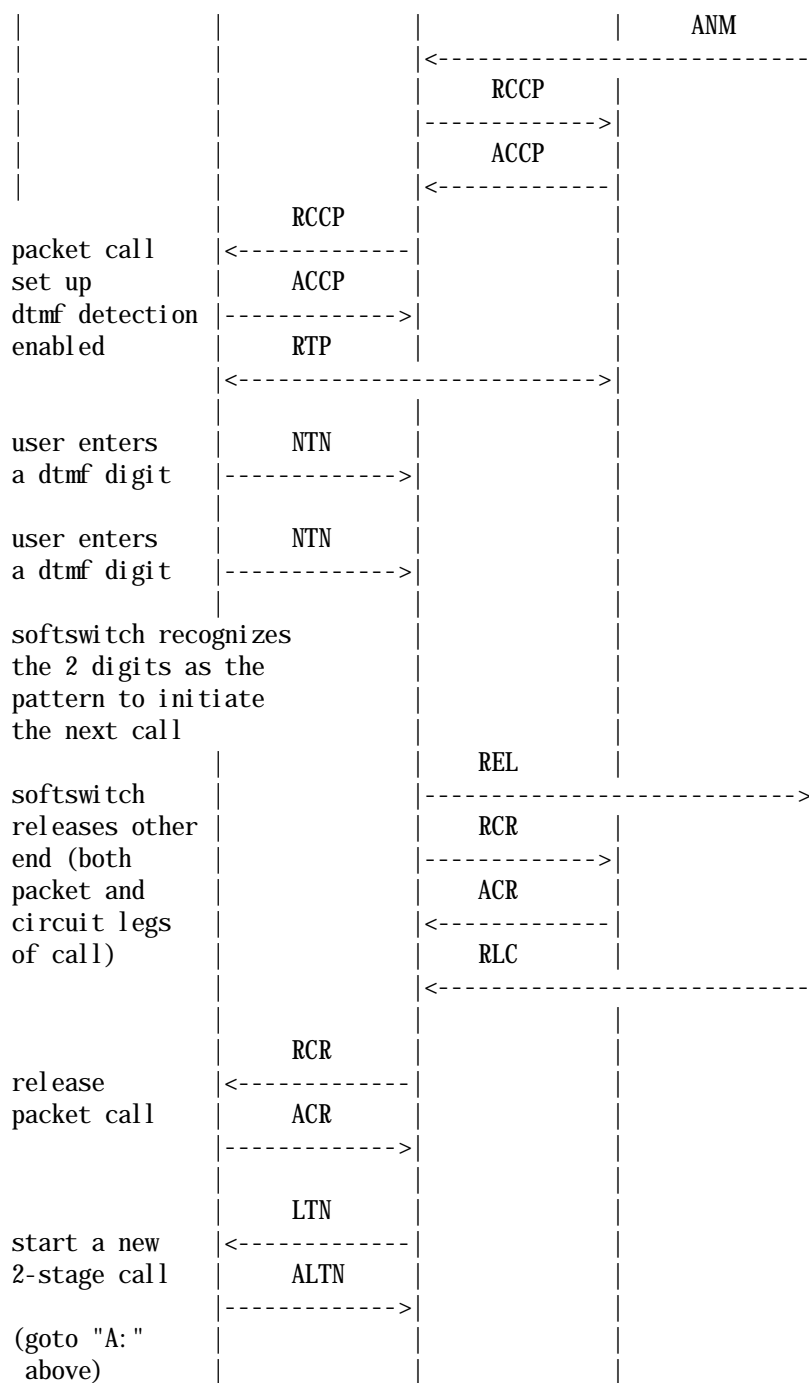
Using in-call DTMF detection, the MultiVoice Gateway forwards DTMF received during an active packet call to the Softswitch. The DTMF is sent in the NTN message, one digit per message. The Softswitch monitors the received DTMF stream for a pattern (for example, **9) that indicates that the calling party 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.



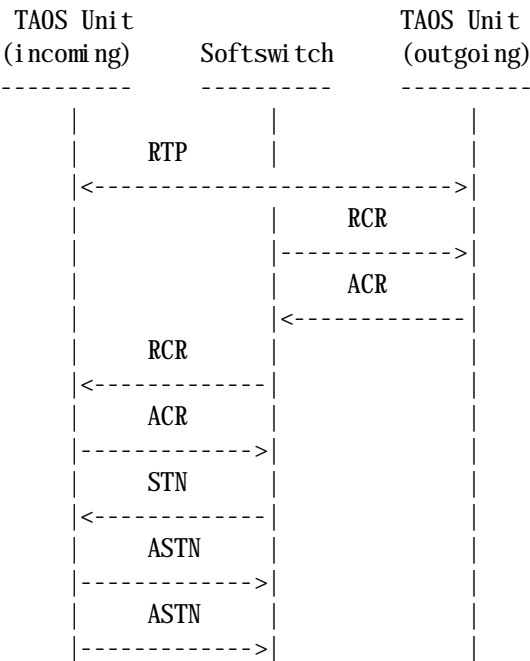


Note Call re-origination when signaled over SS7 VoIP does not use the voip profile parameters sequential-call-enable and next-call. These parameters are used when call re-origination is signaled over H.323 VoIP.

End-of-call break-in voice announcements

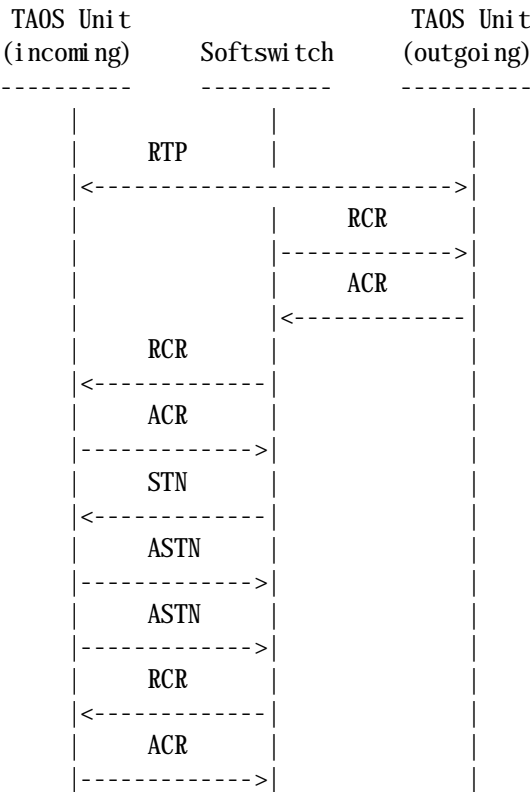
This section illustrates call flows for the special case of playing a break-in voice announcement at the end of a call. Such an announcement could be played either before or after the call is released, with VoIP call persistence enabled or disabled.

- End-of-call break-in announcement is played after call release, with VoIP call persistence mode disabled.



The STN results 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.

- End-of-call break-in is played after call release, with VoIP call persistence mode enabled.

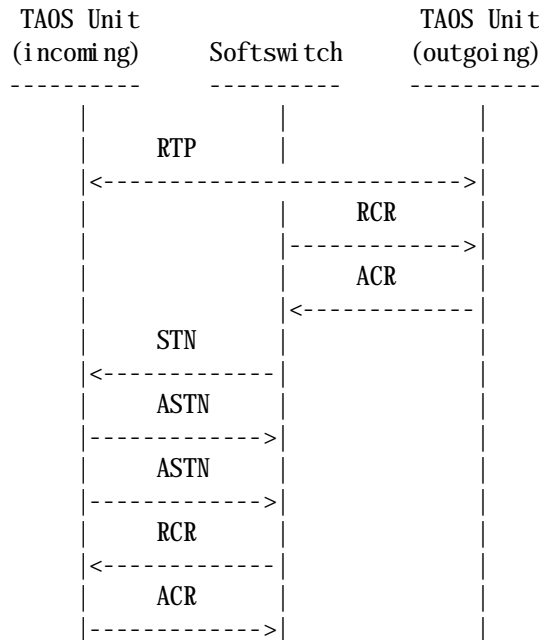


The STN results in the setup of a new VoIP call route. A second RCR is required to destroy the VoIP call route setup by the STN to play the break-in announcement.



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 at the start of the next call. The VoIP call route that was set up for the break-in announcement is then re-used.

- End-of-call break-in is played before call release, VoIP call persistence mode enabled or disabled.



This messaging is possible with support for break-in announcements. The STN utilizes the existing VoIP call route for the call. This reduces gateway processing, but adds extra seconds to the call.

DTMF payout for IPDC

TAOS supports Dual Tone Multi-Frequency (DTMF) digit payout signalled by the IPDC STN message. It plays the DTMF digits utilizing a Digital Signal Processor (DSP) on the line card or a MultiDSP card. A DSP on the MultiDSP card can be associated with a VoIP call route, so Softswitch can direct a MultiVoice Gateway 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 the following sections.

IPDC messages that support DTMF playback

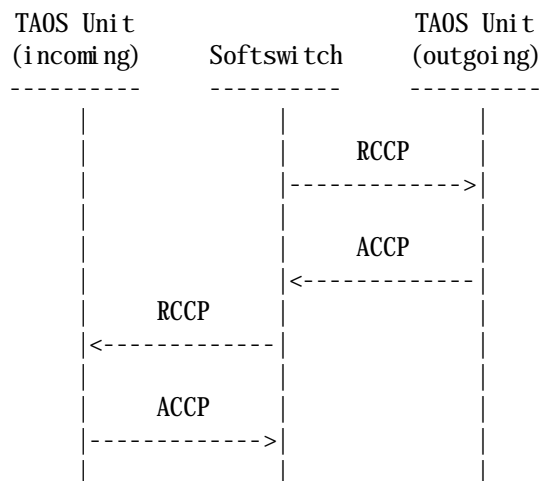
Following are IPDC messages (as defined in IPDC specification *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15*) that support DTMF playback.

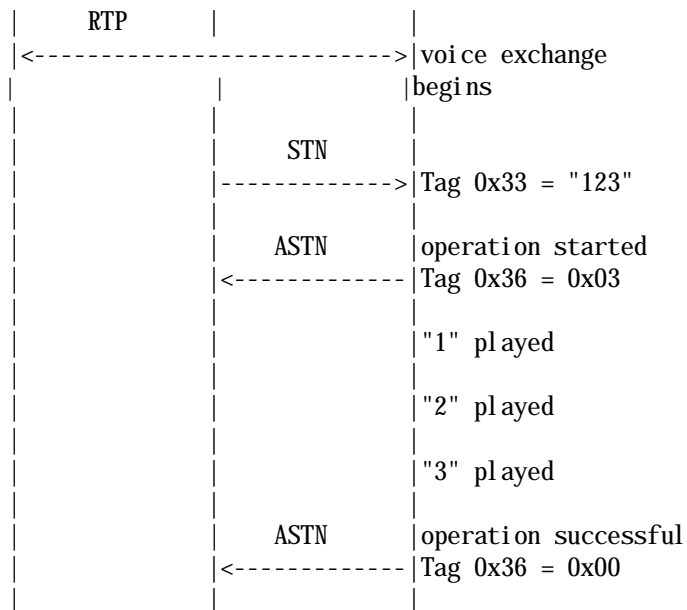
Table 2-20. IPDC messages supporting DTMF playback

IPDC message	Tag	Tag values
STN	0x49 (Tone Type)	Specify 0x01 (DTMF tone) to play DTMF digits.
	0x4A (Apply/Cancel Tone)	The following value is supported: 0x00 (Apply tone)
	0x32 (Num Tones)	The value associated with this tag indicates the number of DTMF digits to be played out.
	0x33 (Tone String)	The value associated with this tag contains the DTMF digits to be played out.
ASTN	0x36 (Completion Status)	The following values are returned:
		<ul style="list-style-type: none">• 0x00 (Operation successful)• 0x01 (Operation failed)• 0x03 (Operation started)

Basic call flow for DTMF digits played during a packet call

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 MultiVoice Gateway at the far end play three DTMF digits: 1, 2 and 3.





Call flow for out-of-band DTMF transport

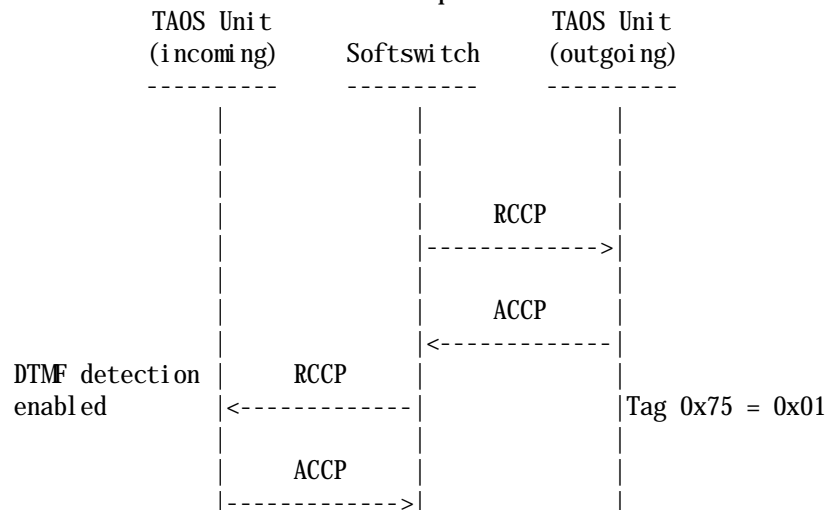
The following call flow illustrates how DTMF payout is used in conjunction with in-call DTMF detection to achieve true out-of-band DTMF transport using IPDC signalling.

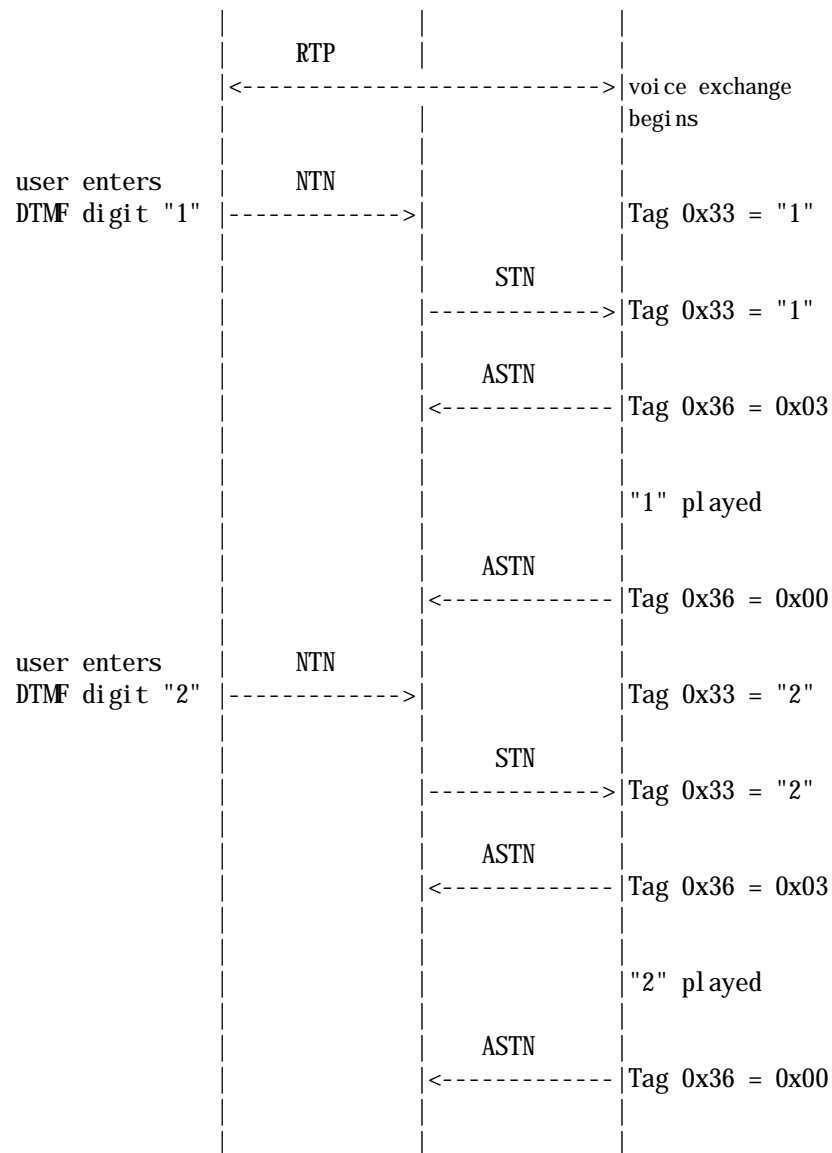
In this example, the call originator enters two DTMF digits, 1 and 2, after the voice exchange has begun. When performing out-of-band DTMF transport, it is necessary to remove the entered DTMF from the RTP stream. To do so, set the voip profile on the MultiVoice Gateway as follows:

```

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:





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 (that is, 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 2-21. 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"> STN while a VoIP call is performing pre-call DTMF detection. STN while a VoIP call is playing a pre-call voice announcement. STN while a VoIP call is playing a break-in voice announcement.
ASTN with Tag 0x36 (Completion Status) = 0x01 (Operation Failed)	<ul style="list-style-type: none"> STN with Tag 0x4A (Apply/Cancel Tone) = 1 (Cancel)

IPDC country-specific call-progress tone payout for VoIP

IPDC defines a specification for playing tones, such as DTMF or arbitrary frequencies towards the PSTN. TAOS provides a means for signaling one of several call progress tones (for example, dial tone, alerting, busy, network busy and unobtainable) using a MultiDSP slot card.

You can also configure the unit to generate a country-specific call progress tone. Country-specific call progress tones can be played as

- Local (to the calling party) payout of remote country-specific call progress tones, which is explained in this section.
- Carry back the call progress tones via RTP, which is already supported in the current IPDC VoIP implementation in TAOS using existing IPDC messaging.

STN message that supports country-specific call-progress tones

A tone type that has been added to the STN (Send tones or announcement) message includes a country identifier.tone string that identifies one of the call progress tones. TAOS uses the tone string and country identifier to generate a country-specific call progress tone.

The STN message that supports generating country-specific call-progress tones is defined in IPDC specification *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15*.

Tag 0x49 (tone type)

The proprietary tag value of 0x41 (Call Progress Tone) has been added to the tone type tag 0x49. The tag value minimizes conflict with any future tag values that might be added in the future by the IPDC community at large. Value 0x41 signals that the STN message contains a request to apply or cancel a call progress tone.

Associated with this value for tag 0x49 is a set of additional values used to indicate the type of call progress tone to play. These values are specified in tag 0x33 (tone string) whenever 0x49 has value 0x41, as follows:

Call progress tone	Tag 0x33 value
Dial tone	"1"
Alerting tone	"2"
Busy tone	"3"
Network busy tone	"4"
Unobtainable tone	"14"

The next available non-proprietary tag value for tag 0x49 is 0x08.



Note TAOS also provides support for two other call progress tones (that is, pin tone and error tone). However, these tones are not country-specific and are relevant only for the H.323 VoIP implementation in TAOS.

Tag 0xC1 (Country Identifier)

The proprietary tag, 0xC1, has also been added to the STN message whenever the STN message contains a request to apply or cancel a call progress tone (that is, when tag 0x49 has the value 0x41).

The following table lists the value of the 0xC1 tag generated in the STN message according to the setting of the country parameter in the system profile:

Parameter setting	Tag 0xC1 value
argentina	0x01
australia	0x02
belgium	0x03
china	0x04
costa rica	0x05
finland	0x06
france	0x07
germany	0x08
hong kong	0x09
italy	0x0A
japan	0x0B
korea	0x0C
mexico	0x0D
netherlands	0x0E
new zealand	0x0F
singapore	0x10
spain	0x11
sweden	0x12

Parameter setting	Tag 0xC1 value
switzerland	0x13
uk	0x14
us	0x15
brazil	0x16

The value of tag 0xC1 is used as the country of origin when determining the frequency, duration, and cadence of the call progress tone. If tag 0xC1 is omitted, the value of the country parameter in the system profile is used as the country of origin.

STN/ASTN usage

The semantics of the STN and ASTN (Completion result of STN command) messages remain the same as for the other tones and announcements.

- To start a call progress tone, send an STN message with tag 0x4A set to 0x00 (Apply Tone).
- To stop a call progress tone, send an STN message with tag 0x4A set to 0x01 (Cancel Tone).

All of the above five call progress tones play continuously until explicitly canceled.



Note If the universal gateway is unable to accept an STN call progress tone request, it responds with an ASTN with status 0x01 (operation failed).

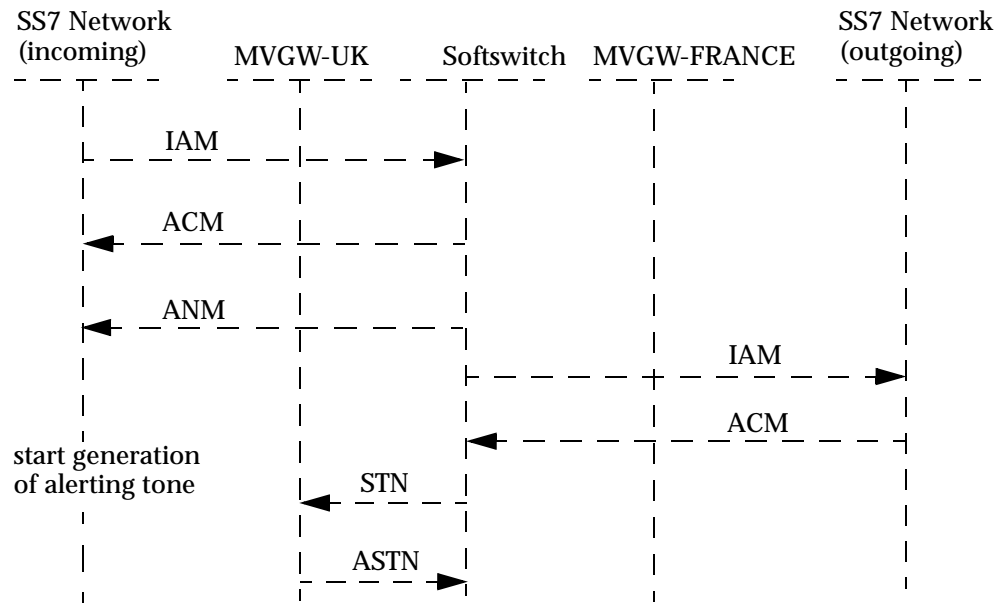
Sample Call Flows — ringing, then answered scenario

If your network consists of two universal gateways, one in the United Kingdom (MVGW-UK) and one in France (MVGW-FRANCE), with one Softswitch, and the calling party is in the UK and the called party is in France, to allow the calling party to hear an alerting tone specific to France, Softswitch sends MVGW-UK an STN with tag 0xC1 = 0x07, tag 0x49 = 0x41, tag 0x33 = "2", tag 0x4A = 0x00 and other tags as required for STN.

Softswitch received tag 0xC1 = 0x07 from MVGW-FRANCE when MVGW-FRANCE sent an NSUP to the Softswitch.



Note The NSUP message is unsupported.



Message contents:

Softswitch->MVGW: (STN - apply "alerting" call progress tone)

Protocol=0x4b, Correlator (4): 00000000

Message: 0x0073

Tag ID=0x07, Data (2): 00 01

Tag ID=0x0d, Data (2): 00 01

Tag ID=0x15, Data (2): 00 01

Tag ID=0x49, Data (1): 41

Tag ID=0x4a, Data (1): 00

Tag ID=0x32, Data (1): 01

Tag ID=0x33, Data (1): 32

Tag ID=0xc1, Data (1): 07

MVGW->Softswitch: (ASTN - command started)

Protocol=0x4b, Correlator (4): 00000000

Message: 0x0074

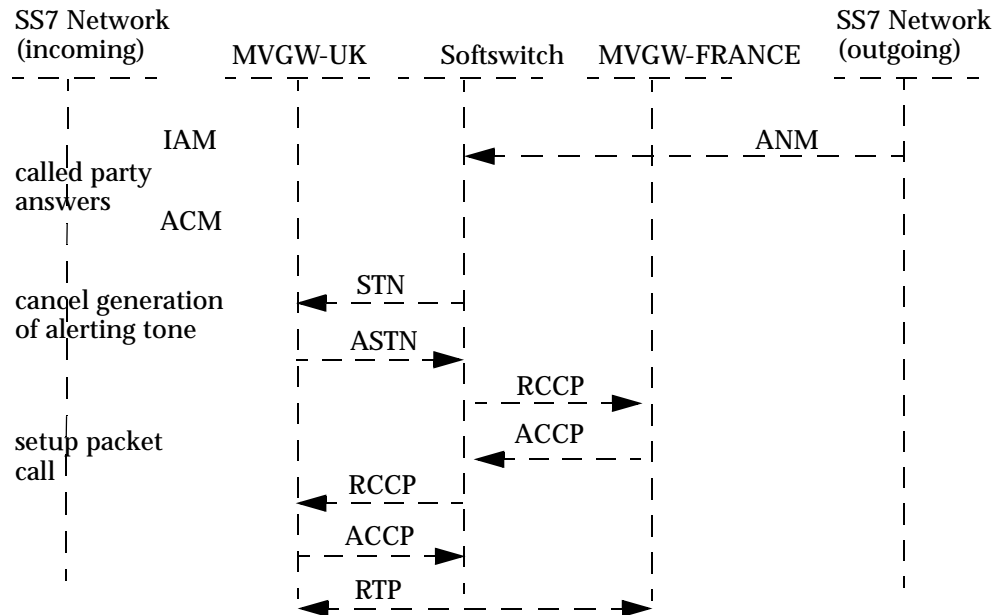
Tag ID=0x07, Data (2): 00 01

Tag ID=0x0d, Data (2): 00 01

Tag ID=0x15, Data (2): 00 01

Tag ID=0x36, Data (1): 03

When the called party answers, Softswitch stops the alerting tone by sending MVGW-UK an STN with the same tags as above except tag 0x4A = 0x01. The packet call can then be set up.



Message contents:

Softswitch->MVGW: (STN - cancel "alerting" call progress tone)

```

Protocol=0x4b, Correlator (4): 00000000
Message: 0x0073
Tag ID=0x07, Data (2): 00 01
Tag ID=0x0d, Data (2): 00 01
Tag ID=0x15, Data (2): 00 01
Tag ID=0x49, Data (1): 41
Tag ID=0x4a, Data (1): 01
Tag ID=0x32, Data (1): 01
Tag ID=0x33, Data (1): 32
Tag ID=0xc1, Data (1): 07
  
```

MVGW->Softswitch: (ASTN - command completed)

```

Protocol=0x4b, Correlator (4): 00000000
Message: 0x0074
Tag ID=0x07, Data (2): 00 01
Tag ID=0x0d, Data (2): 00 01
Tag ID=0x15, Data (2): 00 01
Tag ID=0x36, Data (1): 00
  
```

Sample Call Flows — busy, then hangup scenario

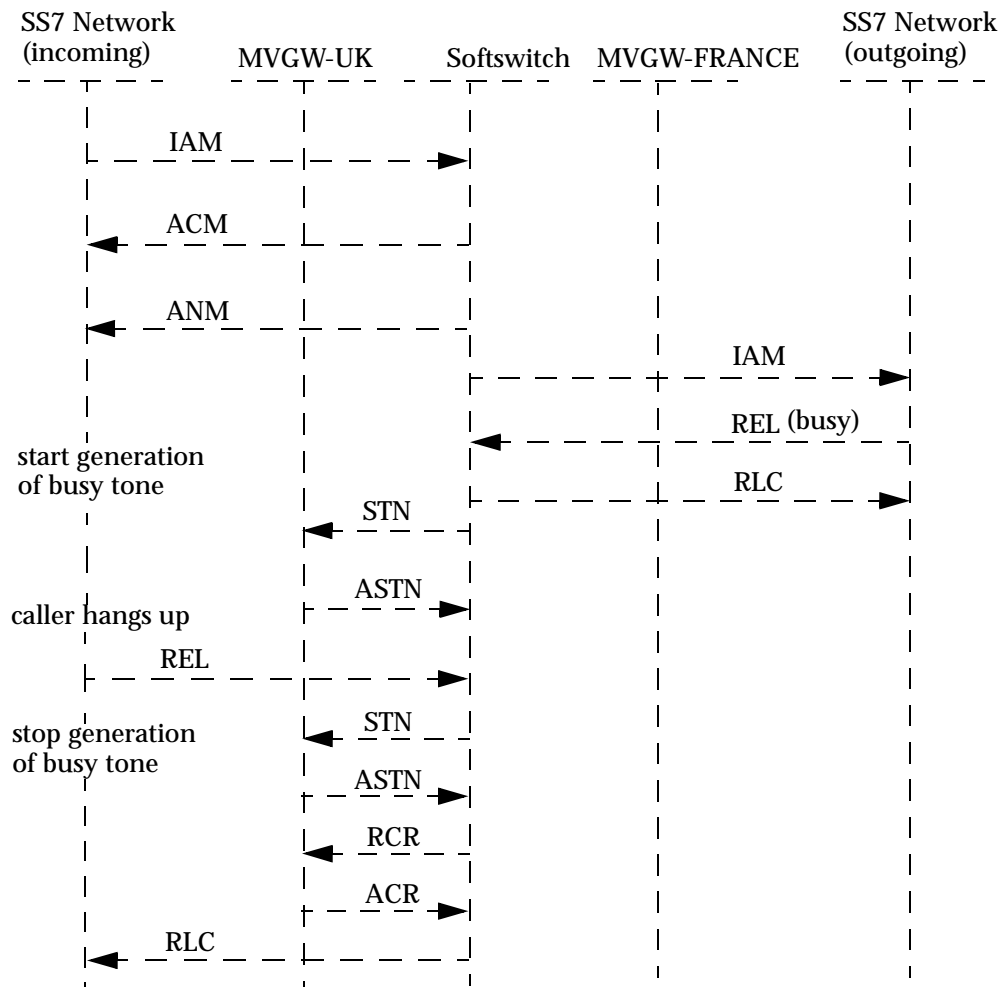
If call setup never progresses to the point where a packet call is actually setup (that is, an RCCP is sent and accepted by the universal gateway), but at least one call progress tone has been generated, and it is time to take down the call, then when VoIP call persistence is enabled on the gateway, it is necessary for the Softswitch to send the

gateway an RCR at the end of the call so that the gateway may free the resources that were used to generate the call progress tone or tones.

To see if Voip call persistence is enabled, check the setting of the `ss7voip-call-persistence` in the voip profile:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> list
[in VOIP/{ 0 0 }]
...
ss7voip-call-persistence = yes
...
```

In the following call flow, the called party is busy. The Softswitch directs the universal gateway to generate a busy tone specific to France. After a short while, the calling party hangs up. Since VoIP call persistence is enabled, the Softswitch must send the gateway an RCR to allow it to free the resources associated with call progress tone generation when VOIP call persistence is enabled.



The RCR allows the universal gateway to free the resources (for example, MultiDSP slot card) associated with the VoIP call route that was setup for the call progress tone generation when the first STN was received.



Note If VoIP call persistence was disabled, the RCR would not be needed.

VoIP Call Configuration

3

The voi p profile	3-1
Creating DNIS-specific voi p profiles	3-7
Configuring call-performance parameters	3-8
Configuring H.323 call management parameters	3-23
Using H.323 authentication	3-70

The voi p profile

The voi p profile configures call-performance features and manages H.323 call processing. The following VoIP call-performance features are configured through the voi p profile:

- The type of voice compression and coding to use for VoIP calls.
- Enabling use of a fixed or dynamic jitter buffer.
- Enabling silence detection and comfort noise generation.
- Adjust the relative lever of silence suppression.
- Modifying the Type-of-Service (ToS) byte for UDP packet processing.
- Modify the maximum number of calls a TAOS unit processes.

The following H.323-specific functions are configured through the voi p profile:

- The IP address of the H.323 gatekeeper —MultiVoice Access Manager (MVAM).
- The IP address for a secondary H.323 gatekeeper (MVAM).
- Adjust the frequency and time intervals when a TAOS unit must register with MVAM.
- Enable Personal Identification Number (PIN) collection for authentication by MVAM.
- Enable single-stage dialing.
- Enable progress tone cut-through from the distant PSTN on the local TAOS unit.
- Adjust the amount of time a caller has to dial a telephone number.
- Support for multiple logical gateways.
- Configure voice announcements in place of call-progress tones.
- Enable rerouting of blocked calls back out over the PSTN.

- Enable out-of-band pass through of PSTN call-progress tones.
- Block Caller ID.
- Configure the call interdigit timer.
- Delay alerting the PSTN about active calls until the connection is completed across the MultiVoice network.
- Enable transparent modem signaling.

The MultiVoice call configuration options are located in the voi p profile:

Parameter	Setting
voi p-index*	Identifies the voi p profile by telephone number. This subprofile uses the telephone number (DNIS) associated with an inbound trunk and the called destination to control routing and processing of VoIP calls. The default voi p profile, voi p { 0 0 }, is a system wide profile used for processing all VoIP calls. Each DNIS-specific VoIP profile can contain settings which apply only to calls received on the associated trunk.
gk-ml g-control	Provides support for partitioning a single MultiVoice Gateway into multiple logical gateways. Partitioning call control lets the H.323 Gatekeeper perform call-specific administration on a call-by-call basis.
gatekeeper-ip	Identifies the H.323 gatekeeper associated with this TAOS unit. This gatekeeper, usually running MVAM, performs H.323 registration, admission and status reporting for this MultiVoice Gateway.
	Note After changing the default value of 0. 0. 0. 0 to an IP address, you need to reset the TAOS unit.
vpn-mode	Enables or disables H.323 call authentication on a TAOS unit. When authentication is enabled, a TAOS unit prompts for a user- entered Personal Identification Number (PIN).
packet-audi o-mode	Selects the default audio coder/decoder (codec) used to process analog voice, received from the public switched telephone network (PSTN) and packetized voice, for transmission across the packet network.
frames-per-packet	Sets the number of voice frames transmitted in a single RTP packet, across the IP network, between two MultiVoice Gateways.
tos-options subprofile	Sets the requested Type-of-Service (ToS) processing priority for RTP packets sent across the IP network between two MultiVoice Gateways.

Parameter	Setting
silence-det-cng	Setting this parameter to yes enables silence suppression. When enabled, the sending side of the call uses silence suppression during background noise conditions. On the receiving side, suppressed sections will always be filled in with locally generated noise. During those silent periods, the local TAOS unit will generate background (comfort) noise to assure the caller that the call is still connected.
gatekeeper-ip-sec	Identifies a secondary H.323 gatekeeper associated with this TAOS unit. This gatekeeper, usually running MVAM, performs H.323 registration, admission and status reporting for this TAOS unit, if the TAOS unit can't register with the gatekeeper specified by the gatekeeper-ip parameter.
gatekeeper-keepalive	Sets the time interval between attempts a TAOS unit makes to reregister with a system running MVAM, following the initial registration. This value equals the wait time, in seconds, between each attempt to reregister.
registration-retries	Sets the number of attempts a TAOS unit makes each time it executes keepalive registration. Since a MultiVoice Gateway may not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a gateway makes during a registration cycle.
registration-retry-timer	Sets the time interval between each registration attempt a TAOS unit makes with MVAM. This sets the pause, in seconds, between each registration attempt specified by the registration-retries parameter.
primary-retries	Sets the number of attempts a TAOS unit makes whenever it tries to reregister with the MultiVoice Access Manager at gatekeeper-ip after registering with the gatekeeper at gatekeeper-ip-sec. Since a MultiVoice Gateway may not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a gateway makes during a reregistration cycle.
ena-adap-jitter-buffer	Changes the jitter buffer mode to either adaptive or fixed for VoIP calls. When the adaptive mode is selected, the jitter buffer will range in size between the values set for max-jitter-buffer-size and one packet.
max-jitter-buffer-size	Sets the maximum jitter buffer size for VoIP calls when the TAOS unit is configured to perform adaptive call jitter buffering. When using adaptive mode, the jitter buffer may increase to accommodate the entered number of audio packets, based on the incoming packet arrival statistics (jitter).

Parameter	Setting
initial-jitter-buffer-size	Sets the initial jitter buffer size for VoIP calls when the TAOS unit is configured to perform adaptive call jitter buffering. When using either adaptive or fixed mode, the jitter buffer is set to initial-j i t t e r - b u f f e r - s i z e at start-up.
maxcalls	Sets the maximum number of VoIP calls a TAOS unit can process simultaneously, by limiting the number of Digital Signal Processors (DSPs) available.
cut-thru-enable-nearend	Enables or disables transmission of call-progress tones from the far-end public switched telephone network (PSTN) across the IP network to the local TAOS unit, for play out to the caller.
single-dial-enable	Enables or disables single-stage dialing for VoIP calls when MultiVoice is used to perform H.323 call processing.
h323-voice-ann-enabled	Enables or disables play out of voice announcements to report call-progress for VoIP call processing.
voice-ann-dir	Identifies the directory on the external flash memory where voice announcement files are stored for call-progress reporting.
call-inter-digit-timeout	Sets the limit on how long the TAOS unit waits for a caller to enter a single digit when using two-stage dialing, and when entering digits during a call.
silence-threshold	Sets the relative threshold for silence suppression to compensate for background noise levels when silence suppression is enabled (s i l e n c e - d e t - c n g = y e s).
dtmf-tone-passing	<p>Specifies how DTMF tones detected at the ingress gateway are transmitted to the egress gateway.</p> <p>Specify one of the following values:</p> <ul style="list-style-type: none">• inband–The near-end gateway passes PSTN-generated DTMF digits and tones as part of the voice processing stream. These tones are compressed by the selected audio codec and transported across the IP network using UDP packets.• outofband–The near-end gateway passes PSTN-generated DTMF digits and tones across the network using non-UDP packets. Once received at the far end, the digits are played out to the local PSTN/caller.• rtp–DTMF tones are transferred and passed via another channel to the decoding DSP, according to the RFC2833 standard. <p>Note Both near-end and far-end gateways must have the same setting.</p>

Parameter	Setting
rt-fax-options subprofile	Enables or disables real-time fax call processing.
call-hairpin	Enables or disables attempts to re-route blocked VoIP calls from a TAOS unit using a connection to the local public switched telephone network (PSTN).
call-keep-alive-timeout	Sets the time interval that a MultiVoice Gateway will wait before polling a remote gateway and/or client during a VoIP call, to verify that they are still functioning, and reachable over the IP network.
clid-suppress	Enables or disables blocking transmission of the Calling Line ID (CLID) associated with a call to the local PSTN by the MultiVoice Gateway. The gateway can send a blocked number message or substitute CLID received from MVAM to the PSTN.
true-connect-enable	Enables or disables a TAOS unit delay reporting a call connected to the local PSTN until both parties in a call are connected.
g711-transparent-data	Enables or disables detection of high-speed fax/modem signals on a VoIP channel, and enables fax/modem transmission in a transparent mode using the G.711 codec at 64Kbps.
allow-g711-fallback	Enables or disables fallback to the G.711 audio codec when either H.323 end point (such as, a gateway or terminal) involved in a VoIP call does not support the audio codec designated by the packet-audio-mode parameter.
allow-coder-fallback	Enables or disables fallback to a negotiated codec when either H.323 end point (such as, a gateway or terminal) involved in a VoIP call does not support the audio codec designated by the packet-audio-mode parameter.
trunk-quietse-enable	Enables or disables automatic trunk deactivation when the MultiVoice Gateway is unavailable to process calls.
early-ringback-enable	Enables or disables local generation of a ringback tone by a TAOS unit as soon as the call-setup begins on the far-end MultiVoice Gateway.
trunk-prefix-enable	Enables or disables assignment of the egress trunk group by the ingress TAOS unit. The MultiVoice Gateway prepends the trunk group number associated with the entry (ingress) T1/E1 trunk to the destination telephone number sent to the exit (egress) gateway or call signaling entity. The egress gateway connects the call to the PSTN using a DS0 assigned to the designated trunk group.

Parameter	Setting
operator-assist	Allows callers to request operator assistance during the dialing phase of a MultiVoice call. A TAOS unit can be assigned a dial string, up to five digits long, that may be entered by a caller in order to connect that caller to an operator.
sequential-call-enable	If a caller must enter a PIN to authenticate MultiVoice calls, to dial subsequent VoIP calls without reentering the PIN, as long as the connection between the PSTN and near-end MultiVoice Gateway is not terminated.
next-call	A new call can be initiated by dialing a string (for example, **9) as specified in the 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-digits (if the call is a long-distance call) number.
ss7voip-call-persistence	<p>Setting this to yes causes VoIP call route to persist across VoIP-related IPDC requests for a given call (e.g., LTN, STN, RCCP and RMCP) until the call is released (via RCR).</p> <p>Setting this to no disables the feature and 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.</p> <p>Enabling VoIP call persistence results in faster call setup and call processing times for SS7 VoIP calls initiated through IPDC.</p>
faststart-enable	Setting this to yes 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.
rtpqos-polling-enable	Setting this to yes generates RTP QoS statistics 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).
signaling-tos-subprofile	Enables configuring DSCP values for marking H.323 signaling packets.

Parameter	Setting
pstn-attribute subprofile	<p>Changes the way an egress MultiVoice Gateway manages call signaling with the switched network. For example:</p> <ul style="list-style-type: none">• Delivery of Q.931/Q.850 cause codes are transparent when received from the PSTN by the far-end MultiVoice Gateway to the near-end MultiVoice Gateway.• Bearer capabilities sent in the Q.931 Setup message by the far-end MultiVoice Gateway for outbound calls to the switched network are configurable.• Reporting of Q.931 Progress Indicator information element (IE) in the Proceeding and Alerting message by the near-end MultiVoice Gateway to the switched network is configurable.

If you are configuring a TAOS unit to work in an H.323 environment, you must provide an IP address for the gatekeeper-ip parameter to process VoIP calls. The IP address points to the computer running MVAM that performs all of the H.323 gatekeeper functions for the TAOS unit. The TAOS unit can process VoIP calls over most IP networks using the factory defaults for the remaining voip profile parameters.



Note In this release, you may not change the values contained in DNIS-specific voip profiles. The TAOS unit globally applies the values set in the default voip profile to all VoIP calls. DNIS-specific voip profiles are only used to simplify internal processing and routing of VoIP calls.

Creating DNIS-specific voip profiles

User-defined voip profiles are used to map incoming calls by identifying all calls associated with a specific Dialed Number Identification Service (DNIS) string as VoIP calls. See “Using DNIS-specific trunk mappings” on page 2-15.

For example, if a user created the following voip profiles:

```
admin> dir voip
 46 12/23/1998 09:48:55 { 0 0 }
 31 12/18/1998 09:50:06 { 8903190 0 }
 31 12/18/1998 10:07:16 { 8903190 0 }
```

The TAOS unit processes all calls from the PSTN with these DNIS strings as VoIP calls. The voip-index subprofile distinguishes between the default voip profile, voip {0 0}, and any user-created voip profiles:

```
admin> list voip-index
[in VOIP/{ 8903190 0 }:voip-index
gateway-access-number = 8903190
far-end-number = 0
```

This subprofile includes the following parameters:.

Parameter	Specifies
gateway-access-number	This is the Dialed Number Identification String (DNIS) passed from the PSTN associated with the in-bound telephone number used to access the TAOS unit. If the TAOS unit is configured to perform two-stage dialing of VoIP calls, this would be the telephone number dialed to access the TAOS unit from the PSTN.
far-end-number	This value should always be set to 0.

To set the values for these parameters, use the `new` and `write` commands to create user-defined voip profiles:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> new voip { 8903190 0 }
VOIP/{ 8903190 0 } read
admin> write
VOIP/{ 8903190 0 } written
admin> dir voip
  46 12/23/1998 09:48:55 { 0 0 }
  31 12/18/1998 10:07:16 { 8903190 0 }
```



Note You may create DNIS-specific voip profiles by changing the value of the `gateway-access-number` parameter using the `set` command; but only if no other changes have been written to the `voip { 0 0 }` profile.

Configuring call-performance parameters

The call-performance parameters control how a MultiVoice Gateway processes calls received from the PSTN. This group of parameters affects allocation of packet network bandwidth for each call, the allocation of DSP assets for each call, and subsequently, the number of VoIP calls that a TAOS unit can process simultaneously. The following voip profile parameters handle VoIP call-performance functions:

- `packet-audio-mode`
- `frames-per-packet`
- `allow-g711-fallback`
- `allow-coder-fallback`
- `silence-det-cng`
- `silence-threshold`
- `ena-adap-jitter-buffer`
- `max-jitter-buffer-size`
- `initial-jitter-buffer-size`
- `tos-options`
- `maxcalls`
- `faststart-enable`

Configuring voice compression

Voice is transmitted across an IP network as compressed audio frames, which are compressed/decompressed by the TAOS unit. The `packet-audio-mode` parameter specifies which default audio codec (coder/decoder) packs (and unpacks) analog speech into digital audio frames. You may enter any of the following values representing these supported audio codecs:

Parameter value	Specifies
<code>g711-ulaw</code>	G.711 μ -law
<code>g711-alaw</code>	G.711 a-law
<code>g729</code>	G.729(A)
<code>g723</code>	G.723.1 running at 5.3kps
<code>g723-6.4kps</code>	G.723.1 running at 6.4kps
<code>g728</code>	G.728
<code>frgsm</code>	Full-rate GSM

The default value for the `packet-audio-mode` parameter is `g711-ulaw`. The following example illustrates how to set the audio codec used for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set packet-audio-mode = g729
admin> write
VOIP/{ 0 0 } written
```

Changes to the setting take effect with the next call. The `packet-audio-mode` parameter has the following dependencies:

- TAOS units configured with 96-port MultiDSP slot cards (APX8-SL-96DSP) support using only the G.711 or G.729(A) audio codecs.
- This parameter does not prevent other supported audio codecs from being dynamically selected during call-setup.
- The `silence-det-cng` parameter is ignored when using G.711 a-law or G.711 μ -law. For details, see “Configuring silence detection and comfort noise generation” on page 3-13.
- When either G.723 or G.723-6.4kps codec is specified:
 - `silence-det-cng` may be enabled or disabled for 6.4Kbps processing only (`packet-audio-mode=g723-6.4kps`).
 - Comfort noise generation may be enabled or disabled for 5.3Kbps processing. With comfort noise enabled, the 5.3Kbps can decode silence detection and suppression packets. Silence detection/suppression cannot be selected for 5.3Kbps processing since it will not encode silence. This is in accordance with standards.
 - Comfort noise generation cannot be enabled for 5.3Kbps processing unless the adaptive jitter buffer is disabled.
 - Silence detection/suppression cannot be enabled for 6.4Kbps processing unless the adaptive jitter buffer is disabled.

- Adaptive jitter buffer processing can be enabled when silence detection/suppression is disabled.
- The actual maximum size of the adaptive jitter buffer is limited to nine frames per packet for G.723.1 both rates.

G.728 codec support

G.728 is an audio codec based on Low-Delay Code Excited Linear Prediction (LD-CELP). G.728 provides toll-quality audio at a bit rate of 16Kbps. With a frame size of only 2.5 milliseconds, G.728 also has a very low delay. Although the MultiVoice implementation of G.728 uses a frame size of 5 milliseconds, the bitstream from the audio codec is the same as described in the ITU-T standard and can thus be decoded by any G.728 decoder.

When the G.728 codec is selected, the MultiVoice Gateway attempts to determine if the G.728 codec is supported by the other gateway during H.245 capability negotiation. If both sides agree to use G.728 as the preferred codec, both gateways use G.728 to compress and decompress audio after the H.245 open logical channel message is exchanged.

Although MultiVoice uses a 5-millisecond frame for G.728 processing, it is compatible with any third-party G.728 decoder. However, if a MultiVoice Gateway attempts to communicate with a third-party VoIP gateway transmitting an odd number of 2.5 millisecond frames per IP packet, the call fails.

When you enable G.728 audio processing (`packet-audio-mode=g728`), the `silence-det-cng` parameter in the `voip` profile must be set to `no` (its default value). The following commands enable G.728 processing:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set packet-audio-mode = g728
admin> set silence-det-cng = no
admin> write
VOIP/{ 0 0 } written
```

G.723.1 codec support

When G.723.1 codec is selected

- `silence-det-cng` can be enabled or disabled for 6.4Kbps processing only by setting the `packet-audio-mode` parameters as follows:
`packet-audio-mode=g723-6.4kps`
- Comfort noise generation can be enabled or disabled for 5.3Kbps processing by setting the `packet-audio-mode` to `g723-5.3kps`. When comfort noise is enabled, the 5.3Kbps setting allows silence detection and suppression packet decoding. Silence detection/suppression cannot be configured directly for 5.3Kbps processing since it will not encode silence. This is in accordance with standards.
- Comfort noise generation cannot be enabled for the `packet-audio-mode 5.3Kbps` setting processing unless adaptive jitter buffering is disabled and the `ena-adap-jitter-buffer` is set to `no`.
- Silence detection/suppression cannot be enabled for 6.4Kbps processing unless the adaptive jitter buffer is disabled.

- Adaptive jitter buffer processing can be enabled for:
 - 6.4Kbps processing when silence detection/suppression is disabled,
 - 5.3Kbps processing when comfort noise generation is disabled.
- The actual maximum size of the adaptive jitter buffer is limited to nine frames per packet for G.723.1 both rates.

Full-Rate GSM codec support

Full-Rate GSM (Global System for Mobile Communications) is a voice encoder/decoder standard for cellular communications. Full-Rate GSM compresses the speech samples from 64Kbps PCM to 13.2Kbps, requiring less network than G.711 a-law or G.711 μ -law. It is the standard followed by European, Japanese, and Australian cellular communications systems, and is supported by certain Web phone applications.

Full Rate GSM uses a speech frame size of 160 samples (20msec) and the encoder produces 33 bytes per frame. The decoder produces 160 samples (20msec) of speech from the 33-byte encoder output.

The Full Rate GSM audio codec is defined by ETSI Recommendation GSM 06.10, *GSM Full Rate Speech Transcoding*, (Feb. 1992), European Telecommunications Standards Institute. Full Rate GSM also supports Silence Detection and Comfort Noise Generation, as defined by the ETSI Recommendation GSM 06.12, *Comfort Noise Generation*, (Feb. 1992), European Telecommunications Standards Institute and ETSI Recommendation GSM 06.12, *Discontinuous Transmission* (Feb. 1992), European Telecommunications Standards Institute.

A MultiVoice Gateway reports Full-Rate GSM during H.245 capability negotiation. If both H.323 end points (such as, a MultiVoice Gateway and a PC, or two MultiVoice Gateways) choose Full-Rate GSM as the preferred codec, then, after opening the H.245 logical channel between both H.323 end points, Full-Rate GSM is used for processing the VoIP call. Full-Rate GSM is encoded as a standard audio capability.

Configuring voice packet size

The number of compressed audio frames assigned to each RTP packet used to transport voice across the IP network is controlled by the frames-per-packet parameter. You can assign a value ranging from 1 to 10 packets. The default is 4.

The following example illustrates how to change the number of audio frames assigned to each RTP packet for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set frames-per-packet = 6
admin> write
VOIP/{ 0 0 } written
```

Assigning a lower value to the frames-per-packet parameter reduces the delay and distortion introduced into any given voice call. But using a lower value may also degrade performance as the number of RTP packets processed for a voice call increases.

Note When a different audio codec is dynamically selected during call-setup, a TAOS unit uses the default value of four frames per RTP packet to process that call.

For more information on MultiVoice packet processing see Appendix A, “MultiVoice Packet Processing.”

Configuring audio codec negotiation

Voice is transmitted across an IP network as compressed audio frames. The `packet-audio-mode` parameter in the default `voip` profile specifies the preferred audio codec used by the gateways to compress and uncompress analog speech and digital audio frames.

You can use the following parameters (shown with default values) to specify how the system behaves when the preferred codec is not supported for all VoIP, fax, and transparent modem calls:

```
[in VOIP/{ 0 0 }]
allow-g711-fallback = yes
allow-coder-fallback = yes
```

Parameter	Setting
<code>allow-coder-fallback</code>	<p>Overrides fallback to a negotiated codec when either of H.323 end points (such as a gateway or terminal) involved in a VoIP call do not support the audio codec designated by the <code>packet-audio-mode</code> parameter.</p> <p>When <code>allow-coder-fallback=no</code>, the ingress gateway rejects the call if it is unable to connect the call using the preferred codec. If this parameter is set to no, the <code>allow-g711-fallback</code> parameter has no effect.</p> <p>When <code>allow-coder-fallback=yes</code>, the ingress gateway negotiates an alternate audio codec with the destination gateway during call capabilities setup. Yes is the default setting.</p>
<code>allow-g711-fallback</code>	<p>Overrides fallback to the G.711 audio codec when either of H.323 end points (such as a gateway or terminal) involved in a VoIP call does not support the audio codec designated by the <code>packet-audio-mode</code> parameter.</p> <p>If <code>allow-coder-fallback=yes</code>, setting <code>allow-G711-fallback=no</code> prevents the ingress gateway from selecting the G.711 codec when negotiating call capabilities. In this case, the system terminates the call if G.711 is the only available choice and it is not the preferred codec.</p> <p>When <code>allow-G711-fallback=yes</code>, the ingress gateway may negotiate using the G.711 audio codec with the destination gateway during call capabilities setup. yes is the default setting.</p>

Normally, an H.323 stack advertises a list of supported audio codecs. If the preferred codec is present on a list received from a far-end gateway, that codec is always selected. Otherwise, the system selects an alternate codec that matches one from its supported list.

Modifications made to these parameters become effective with the next VoIP call.

The following example illustrates how to allow fallback to any supported audio codec, except G.711, when processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set allow-coder-fallback = yes
admin> set allow-g711-fallback = no
admin> write
VOIP/{ 0 0 } written
```

Configuring silence detection and comfort noise generation

A TAOS unit can be configured to detect periods of silence during voice calls, suppress transmission of voice packets containing silence, and generate white (comfort) noise to assure the user that a call is still connected during silent periods.

The `silence-det-cng` parameter enables or disables the feature. You can prevent silence frames from being passed across the packet network, reducing the effective bandwidth of the VoIP call. During those silent periods, the local TAOS unit generates background (comfort) noise to assure the caller that the call is still connected during these silent periods. You can assign the following values to the `silence-det-cng` parameter:

Parameter value	Specifies
yes	Silence frames are not passed across the IP network by the TAOS unit. During silent periods, while the call is still connected, the local TAOS unit will generate background (comfort) noise.
no	(Default) Silence is processed as part of the audio stream; comfort noise is not locally generated.

Changes to the parameter setting become effective with the next VoIP call.

The following example illustrates how to enable silence detection and comfort noise generation when processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set silence-det-cng = yes
admin> write
VOIP/{ 0 0 } written
```

When using silence suppression and comfort noise generation, the following apply:

- Silence compression and comfort noise generation must be enabled on both the local TAOS unit and distant TAOS unit involved in a call.
- When silence compression and comfort noise generation are enabled, the dynamic jitter buffer is not used (`ena-adap-jitter-buffer=no`).
- When either the G.723 or G.723-6.4kps codec is specified

- Comfort noise generation can be enabled for processing at a rate of 5.3Kbps. With comfort noise enabled, the 5.3Kbps processing can decode silence detection and suppression packets.
- Comfort noise generation cannot be enabled for 5.3Kbps processing unless the adaptive jitter buffer is disabled.
- Silence detection/suppression cannot be enabled for 6.4Kbps processing unless the adaptive jitter buffer is disabled.

Adjusting the relative silence threshold

The `silence-threshold` parameter adjusts the relative threshold for silence suppression to compensate for background noise levels. This parameter lets the silence floor be raised or lowered in 1dB increments, without preventing conversation at normal speech levels from getting through. This parameter allows the user to raise the silence floor from an increase of 0 dB, the nominal level, to an increase of 9dB.

The following example illustrates how to raise the relative threshold for silence suppression for processing VoIP calls:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set silence-threshold = 3  
admin> write  
VOIP/{ 0 0 } written
```

Dependencies This parameter is ignored if silence suppression is disabled (`silence-det-cng=no`).

Configuring dynamic call jitter buffers

VoIP calls are processed using packet-based jitter buffering. A unique jitter buffer is opened for each call; the buffer dynamically adjusts its size to accommodate network jitter. In essence, jitter buffer playout delay adapts to network jitter.

To configure dynamic call jitter buffers, proceed as follows:

- 1 **Enable the adaptive jitter buffer.**
- 2 **Configure the initial jitter buffer size.**
- 3 **Configure the maximum jitter buffer size.**

Enabling the adaptive jitter buffer

The `ena-adap-jitter-buffer` parameter changes the jitter buffer mode to either adaptive or fixed for VoIP calls. When the adaptive mode is selected, the jitter buffer ranges in size between the values set for `max-jitter-buffer-size` and one packet, depending on the number of late or out-of-sequence packets received during the call. You can enter either of the following values:

Parameter value	Specifies
yes	(Default) That adaptive jitter buffering is used for processing VoIP calls.

Parameter value	Specifies
no	That static jitter buffers is used for processing VoIP calls.

Changes to this value become effective with the next VoIP call.

The following example illustrates how to enable or disable adaptive jitter buffering for VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set ena-adap-jitter-buffer = yes
admin> write
VOIP/{ 0 0 } written
```

Using adaptive jitter buffering has the following dependencies:

- When `silence-det-cng=yes`, MultiVoice uses the value assigned to `initial-jitter-buffer-size` parameter to open static call jitter buffers.
- When `ena-adap-jitter-buffer=no`, MultiVoice uses the value assigned to `initial-jitter-buffer-size` to open static call jitter buffers.
- When G.723 codec is the valued for the `packet-audio-mode` parameter, the maximum jitter buffer size can't exceed nine packets (`max-jitter-buffer-size=9`).

Configuring the maximum jitter buffer size

The `max-jitter-buffer-size` parameter sets the maximum jitter buffer size for VoIP calls when the TAOS unit is configured to perform adaptive call jitter buffering. When using adaptive mode, the jitter buffer can increase to accommodate the entered number of audio packets, based on the incoming packet arrival statistics (jitter).

You may enter a value between 1 and 19 (packets). This allows the TAOS unit to expand the length of a call's jitter buffer to a size proportionate to the selected number of audio packets. This value defaults to 19. Changes to this value become effective with the next VoIP call.

The following example illustrates how to set the maximum jitter buffer size when adaptive jitter buffering is enabled for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set max-jitter-buffer-size = 19
admin> write
VOIP/{ 0 0 } written
```

Configuring the initial jitter buffer size

The `initial-jitter-buffer-size` parameter sets the initial jitter buffer size for VoIP calls when the TAOS unit is configured to perform adaptive call jitter buffering. When using either adaptive or fixed mode, the jitter buffer is set to `initial-jitter-buffer-size` at start-up. During a call, the TAOS unit adjusts each jitter buffer to accommodate the number of audio packets, based on the in-coming audio packet volume.

You can enter a value between 1 and 19 (packets). This value defaults to 2. Changes to this value become effective with the next VoIP call.



Note When using adaptive jitter buffers, the minimum jitter buffer size may be less than the value assigned to the `initial-jitter-buffer-size` parameter. Under the appropriate conditions, adaptive jitter buffers may shrink to only one frame in size from the `initial-jitter-buffer-size`.

The following example illustrates how to change the initial jitter buffer size when adaptive jitter buffering is enabled for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set initial-jitter-buffer-size = 5
admin> write
VOIP/{ 0 0 } written
```

For more information on jitter buffer processing see Appendix B, “Determining Jitter Buffer Size.”

Type of Service (TOS) or Differentiated Service Codepoint (DSCP) marking

You can set the IP Type of Service (TOS) byte in IP packets that carry signaling messages to define the type of packet marking— either TOS or Differentiated Services Codepoint (DSCP).

For detailed information about how the system supports TOS precedence (RFC 791) and DSCP (RFC 2474) marking of packets, see the *APX/MAX TNT WAN, Routing and Tunneling Configuration Guide*.

Type of Service marking

Type of Service is an eight-bit parameter found in the header of an IP datagram. In networks that support processing of IP packets based on precedence, the Type of Service byte is used to attain a certain level of UDP packet processing by manipulating values for delay, throughput, and reliability.

The `tos-options` subprofile sets the Precedence bits (bit0 - bit2) and the TOS bits (bit3 - bit6) for the Type of Service (TOS) byte use by UDP voice packets. It is divided into three fields, containing the following values:

Bits 0-2: Precedence.

Bits 3-6: TOS (performance cost).

Bit 7: Reserved for Future Use.

0	1	2	3	4	5	6	7
PRECEDENCE			TOS				0

The `tos-options` subprofile is shown below, with default values:

```
[in VOIP/{ 0 0 }:tos-options]
active = yes
precedence = 101
type-of-service = latency
apply-to = both
```

Parameter	Setting
active	Enables or disables user configuration of the Type-of-Service byte. Setting this value to yes enables operator configuration of the TOS byte. This is the default value. Setting this value to no disables this feature. Changes to this parameter take effect with the next VoIP call.
precedence	Importance of priority of the UDP packet, bit0 through bit2 of the Type-of-Service octet. This is represented by a hexadecimal value, which defines how the network processes the UDP packets. The default is 101. Changes to this value become effective with the next call.
type-of-service	Processing attribute management, bit3 through bit6 of the Type-of-Service octet. These bits denote how the network should make trade-offs between throughput, delay, reliability and cost when processing the UDP packets. This value defaults to 1 latency. Changes to this value become effective with the next call.
apply-to	How the Type-of-Service value is applied to the data flow over the IP network between the MultiVoice Gateways. This parameter has no affect on VoIP call packet processing.

Configuring precedence parameter values

The values assigned to the precedence parameter set bit0 through bit2 of the Type-of-Service octet. The impact of a selected value on UDP packet processing is IP network dependent (see RFC791). You can enter of the following values (hexadecimals), representing processing priorities, as defined by RFC791:

Parameter value	Specifies (RFC 791 definition)
000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	CRITIC/ECP (default)
110	Internetwork Control
111	Network Control

The following example illustrates how to assign a “Flash” precedence or processing priority to UDP packets used for processing VoIP calls:

```
admi n> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admi n> list tos-options
```

```
admin> set precedence = 011
admin> write
VOIP/{ 0 0 } written
```

Configuring type-of-service parameter values

The values assigned to the type-of-service parameter set bit3 through bit6 of the Type of Service octet. The impact of a selected value on UDP packet processing is network dependent (for more information, see “Use of the TOS field in Routing” in RFC1349):

Parameter value	Specifies (RFC1349 definition)
latency	Minimize delay
throughput	Maximize throughput
reliability	Maximize reliability
cost	Minimize cost
normal	Normal (network control)

The following example illustrates how to set maximized throughput for processing UDP packets used for VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> list tos-options
admin> set type-of-service = throughput
admin> write
VOIP/{ 0 0 } written
```

Differentiated Services Codepoint marking

You can use the IP TOS field in the IP header of packets that carry H.323 signaling messages to set DSCP.

Differentiated services (DS) is an architecture that provides different types or levels of service for network traffic. The differentiated services codepoint is a particular bit pattern (that is, a hexadecimal value) that can be assigned to the DSCP 6-bit field in the IP TOS byte of the IP header. This DSCP field facilitates the definition of future per-hop behaviors.

Implementors should note that the DSCP field is six bits wide. Differentiated Services compliant nodes must select per-hop behaviors by matching against the entire 6-bit DSCP field.



Note The full byte (that is, 8 bits) of the DSCP field can be specified and will be set this way in the IP TOS byte of the IP header. Even though you can set the entire 8 bit in any desired way, only the most significant 6 bits are used and matched to select a Per-Hop Behavior (PHB) by the DS domains in the network. In order to specify traditional TOS/Precedence values, as per RFC 791, the desired bit field can simply be specified as the equivalent DSCP value.

Parameters in voip profile sets DSCP in H.323 packets

You can configure DSCP values for marking H.323 signaling packets by setting the following parameters in the signaling-tos subprofile of the voip profile:

```
[in VOIP/{ 0 0 }:signaling-tos]
active = no
precedence = 000
type-of-service = normal
apply-to = both
marking-type = dscp
dscp = 00
```

Parameter	Setting
active	Enables or disables user configuration of the DSCP. Setting this value to yes enables configuration of the DSCP. This is the default value. Setting this value to no disables this feature. Changes to this parameter take effect with the next VoIP call.
precedence	Importance of priority of the UDP packet, bit0 through bit2 of the Type-of-Service octet. This is represented by a hexadecimal value, which defines how the network processes the UDP packets. The default is 000, which means Normal Priority. Changes to this value become effective with the next call.
type-of-service	Processing attribute management, bit3 through bit6 of the Type-of-Service octet. These bits denote how the network should make trade-offs between throughput, delay, reliability and cost when processing the UDP packets. This value defaults to normal. Changes to this value become effective with the next call.
apply-to	How the Type-of-Service value is applied to the data flow over the IP network between the MultiVoice Gateways. This parameter has no affect on VoIP call packet processing.
marking-type	Either precedence-tos or dscp. When set to dscp, Differentiated Services CodePoint marking (RFC 2474) can be set by entering a hexadecimal number via the dscp parameter. The differentiated services codepoint is a particular bit pattern (that is, a hexadecimal value) that can be assigned to the Differentiated Services Codepoint (DSCP) 6-bit field in the IP TOS byte of the IP header. When set to precedence-tos, the system marks packets in a manner consistent with RFC 791.

Parameter	Setting
dscp	The DSCP tag to be used in the marking of the packets (if the marking-type parameter = dscp). Hexadecimal field, 1 byte. The default value is 00 and the range is from 00 to ff hexadecimal.

For example, the following commands enable DSCP marking and specify a value of 33 for H.323 signaling packets:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set signaling-tos active = yes  
admin> set signaling-tos dscp = 33  
admin> write
```

For details about configuring DSCP marking in SS7 signaling packets, refer to your platform's *Physical Interface Configuration Guide*.

Controlling VoIP call volume

The `maxcalls` parameter controls the maximum number of VoIP calls a TAOS unit can process simultaneously, by limiting the number of digital signal processors (DSPs) available for processing VoIP calls.



Note When the `voip-max-capacity-allowed` parameter is enabled and licensed for an APX in the read-only base profile, the `maxcalls` parameter is automatically set to the maximum number of VoIP calls that can be processed (for example, 2688). (See “Base profile parameters” on page 2-2 for details.)

Limited DSP availability is useful when continued high call volumes on a network affect the call quality. Adjusting the value for `maxcalls` allows a TAOS unit to allocate more system resources to processing fewer calls, resulting in improved call quality. When active calls exceed the resources that are available to process VoIP calls, the caller hears a busy signal from the TAOS unit.

Maxcalls parameter

The following example illustrates how to limit the number of available DSPs to handle VoIP calls:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set maxcalls = 128  
admin> write  
VOIP/{ 0 0 } written
```

You may enter any number between 1 and the maximum value. On a MAX TNT, the `maxcalls` parameter defaults to 672—only values between 1 and 672 can be entered. On a APX, only values between 1 and 2688 can be entered. If an APX has only been licensed for up to 2688 calls, and it receives call attempt #2689, the call will be rejected.

Changes to this parameter become effective with the next call.



Note This value does not reflect actual VoIP call volumes achieved by the TAOS unit in either a testing or production environment.

Exceeding the maximum call volume

When the licensed call volume is exceeded, a MultiVoice Gateway displays the following warning message if debugging and the h323warn command (level 2 or higher) were enabled:

```
H323: 4: WARNING: _wanNewCall():  
... call denied due to simultaneous call capacity  
... 2689 > 2688
```

Configuring H.323 (v2) fastStart

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.

fastStart vs. standard H.245 procedure

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.

faststart-enable parameter

The faststart-enable parameter 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.

The following procedure illustrates how to enable fastStart:

```
[in VOIP/{ 0 0 } read]
admin> set faststart-enable=yes
admin> wri
```

Configuring H.323 call management parameters

A TAOS unit may be configured to use IPDC in support of an SS7 network configuration or use H.323 in support of non-SS7 networks. TAOS units use the following parameters to handle H.323 management:

- gatekeeper-ip
- gatekeeper-ip-sec
- gatekeeper-keepalive
- registration-retries
- registration-retry-timer
- primary-retries
- cut-thru-enable-nearend
- dtmf-tone-passing
- clid-suppress
- call-keep-alive-timeout
- call-inter-digit-timeout

- true-connect-enable
- single-dial-enable
- call-hairpin
- vpn-mode
- h323-voice-ann-enabled
- voice-ann-dir
- voice-ann-enc
- g711-transparent-data
- trunk-quiet-enable
- early-ringback-enable
- trunk-prefix-enable
- rtpqos-polling-enable

These parameters can be ignored or reset when using IPDC to route VoIP calls from an SS7 network. When operating in an H.323 environment, the only parameter that must be set is the `gatekeeper-ip` parameter. This identifies the location of the H.323 gatekeeper system that performs call management for the MultiVoice network.



Note The use of the H.323 `voice-ann-enabled`, `voice-ann-dir`, and `voice-ann-enc` parameters is discussed in Chapter 4, “Voice Announcement Administration.” The use of the `rt-fax-options` subprofile is discussed in Chapter 5, “MultiVoice Real-time Fax.”

H.323 gatekeeper communication

An H.323 gatekeeper manages the MultiVoice network. It provides address translation and controls access to the local area network for all TAOS units processing VoIP calls and any H.323 terminals (such as, PCs running H.323-compliant telephony software). All gatekeeper functions are performed by the MultiVoice Gatekeeper running MVAM software.

Identifying the primary gatekeeper

The `gatekeeper-ip` parameter identifies the computer running MVAM that performs all the H.323 gatekeeper functions for this TAOS unit when MultiVoice is configured to perform H.323 call processing.

MultiVoice implements the H.323 direct call model for VoIP networks, so each TAOS unit must communicate with a gatekeeper to perform call registration and admission, and report statuses (RAS). The TAOS unit sends all call request messages and call processing information to the IP address specified by `gatekeeper-ip`.

After changing the default value of 0.0.0.0 to an IP address, you need to reset the TAOS unit. Changes to this parameter take effect with the next registration cycle.



Note The `gatekeeper-ip` parameter must be configured for a TAOS unit to start processing VoIP calls in an H.323 network.

The following example illustrates how to set the IP address of MVAM that functions as the H.323 gatekeeper for this TAOS unit:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read
```

```
admin> set gatekeeper-ip = 123.123.23.1
admin> write
VOIP/{ 0 0 } written
```

The TAOS unit must be able to send packets to and receive packets from MVAM. You can verify connectivity by pinging the IP address of MVAM from the terminal server. If the pings fail, see your network administrator about possible routing problems.

Identifying a secondary gatekeeper

The `gatekeeper-ip-sec` parameter identifies a second computer running the MVAM software that performs all the H.323 gatekeeper functions for the TAOS unit when configured for H.323 call processing, if it can't register with the gatekeeper identified in the `gatekeeper-ip` parameter.

The following example illustrates how to set the IP address designating the MVAM that functions as the secondary H.323 gatekeeper for this TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set gatekeeper-ip-sec = 123.123.23.13
admin> write
VOIP/{ 0 0 } written
```

The following dependencies apply:

When an IP address is not assigned to `gatekeeper-ip-sec`, then the TAOS unit goes into a *slow poll mode* with the MultiVoice Access Manager at `gatekeeper-ip`. The TAOS unit attempts registrations at 30-second intervals with MVAM as defined by the `gatekeeper-ip` parameter. During the time the gateway is unregistered, new calls are *blocked*, which means the TAOS unit rejects any new calls.

Anytime a TAOS unit attempts to register with a gatekeeper, that gateway is effectively unregistered with any gatekeeper. During this period, calls are blocked. However, existing calls continue to operate normally.

The TAOS unit must be able to send packets to and receive packets from MVAM. You can verify connectivity by pinging the IP address of MVAM from the terminal server. If the pings fail, see your network administrator about possible routing problems.

Setting gateway registration policy

Registration is a process where the TAOS unit informs MVAM of its identity and availability to process VoIP calls. The transport address and alias address of the TAOS unit across the RAS (registration, admission and status) channel to MVAM. Sending the transport and alias addresses must take place initially before the TAOS unit can connect calls and repeats periodically.

The TAOS unit sends a Registration Request (RRQ) to MVAM. TAOS units used as MultiVoice Gateways send information about the feature set installed on the MVAM as part of each Registration Request (RRQ) message. This allows MVAM to distinguish between MultiVoice Gateways running TAOS 10.0 and previous releases to provide appropriate call processing support for each MultiVoice Gateway.

MVAM responds with either a registration confirmation (RCF) or registration reject (RRJ) message. Once registered, the TAOS unit can request address translation, admissions control and zone management services from the MVAM.

Controlling keepalive registration

Once registered with a gatekeeper, a TAOS unit re-registers with its currently registered gatekeeper every 120 seconds. This is called the *keepalive registration*. The `gatekeeper-keepalive` parameter sets the time interval between attempts to reregister with a system running MVAM, following the initial registration. The parameter value equals the wait time, in seconds, between each attempt to reregister.

You can enter any value between 1 and 65535. Changes to the `gatekeeper-keepalive` parameter become effective with the next registration cycle.

The following example illustrates how to set the keepalive time interval for a TAOS unit:

```
admi n> read voip { 0 0 }
VOIP/{ 0 0 } read
admi n> set gatekeeper-keepalive = 120
admi n> write
VOIP/{ 0 0 } written
```



Note If you change this parameter, you should also change the `registrationDuration` parameter on MVAM. Gateway registration with MVAM automatically expires within that time frame.

Detecting gatekeeper failure

At H.323 stack initialization time, a TAOS unit attempts to register with the primary H.323 gatekeeper. The H.323 stack does not initialize when the primary gatekeeper is not configured. Registration with a primary gatekeeper fails when the gateway cannot register with the primary gatekeeper after all attempts have been made. By default, a TAOS unit makes five registration attempts at 5-second intervals.

When registration with the primary gatekeeper fails, a TAOS unit attempts to register with the secondary gatekeeper if there is a valid address (non-null) configured for the `gatekeeper-ip-sec`. The TAOS unit applies the same registration policy (five registration attempts at 5-seconds intervals). Once it successfully registers with the secondary gatekeeper, the TAOS unit operates in *backup mode*.

If there is no valid address (null) configured for the `gatekeeper-ip-sec` when the primary gatekeeper fails, then the TAOS unit goes into slow-poll mode with the MultiVoice Access Manager identified by the `gatekeeper-ip` parameter setting.

Setting reregistration policy

After a TAOS unit registers with the MultiVoice Access Manager identified in the `gatekeeper-ip-sec` parameter setting, it periodically attempts to reregister with the primary MVAM identified in the `gatekeeper-ip` parameter setting. The attempts to reregister with the primary gatekeeper are initiated after every cycle of five successful registrations with the secondary gatekeeper. If the gateway cannot register with the primary gatekeeper in this mode, it performs keepalive registration with the secondary gatekeeper.

Setting the number of registration attempts for each cycle

The `registration-retries` parameter sets the number of attempts a TAOS unit makes each time it executes keepalive registration. Since a gateway might not successfully register on its first attempt, the value for this parameter represents the

number of repeated registration attempts a gateway makes during a registration cycle, until it either registers successfully or until all attempts have failed.

You can enter any value between 1 and 200 for the registration-retries parameter. Changes to this value become effective with the next registration cycle. This value defaults to 5 attempts.

The following example illustrates how to set the number of registration attempts a TAOS unit performs during a registration cycle:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set registration-retries = 5
admin> write
VOIP/{ 0 0 } written
```

Setting the interval between registration attempts for each cycle

The registration-retry-timer parameter sets the time interval between each registration attempt with MVAM. The parameter value sets the pause, in seconds, between each registration attempt specified by the registration-retries parameter.

You can specify a time between 1 and 200 seconds. Changes to this value become effective with the next registration cycle. This value defaults to 5 seconds.

The following example illustrates how to set the time interval between each registration attempt specified by the registration-retries parameter:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set registration-retry-timer = 5
admin> write
VOIP/{ 0 0 } written
```

Setting the number of reregistration attempts

The primary-retries parameter sets the number of attempts a TAOS unit makes whenever it tries to reregister with the MultiVoice Access Manager identified in the gatekeeper-ip parameter setting. Since a gateway might not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a gateway makes during a reregistration cycle, until it either registers successfully with the MultiVoice Access Manager identified by the gatekeeper-ip parameter setting or until all attempts have failed.

Setting primary-retries to zero (0) disables this feature. You can enter any value between 0 and 200. Changes to this value become effective with the next registration cycle. The default value is 1.

The following example illustrates how to set the number of registration attempts this TAOS unit will execute when attempting to reregister with MVAM at gatekeeper-ip:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set primary-retries = 5
admin> write
VOIP/{ 0 0 } written
```

Reporting trunk capacity to the gatekeeper

For all T1 or E1 trunks attached to a MultiVoice Gateway, the gateway can report the following information to MVAM:

- Trunk status at initialization
- Changes in trunk status after initialization
- Trunk profile changes after initialization
- Trunk group changes after initialization

Changes in trunk availability are reported for both VoIP and data trunk calls as part of the nonStandardData byte sent in subsequent registration request (RRQ) messages.

A MultiVoice Gateway periodically reports trunk availability to MVAM in response to an information request (IRQ) message and as part of a subsequent registration request (RRQ) message. The nonStandardData byte uses two data fields for reporting trunk status for all enabled trunks and changes to trunk status. MVAM extracts this information to determine which trunk groups have available channels for egressing VoIP calls.

When a MultiVoice Gateway is initialized, it sends a full RRQ to MVAM, reporting the status of all enabled trunks. When trunk group routing is enabled for VoIP calls, the trunk status information allows MVAM to identify available channels for egressing VoIP calls.

A lightweight RRQ reports only changes to the original trunk information. This message is issued in response to an IRQ message from MVAM and in a subsequent RRQ message. The RRQ message reports the following information:

- Any changes in trunk statuses (such as an active trunk going down, or an inactive trunk coming up), as they occur. An RRQ is sent immediately for just the changed trunk, even if that trunk is disabled.
- Any changes made in T1 or T3 profile parameter values (such as changes in signaling mode, default call type, etc.), that affect trunk availability. An RRQ is sent immediately for just the profile change. However, if the change is to the `t1:line-interface enabled` parameter, this is reported as a change in trunk status, not a profile change.
- Whenever the assigned trunk group usage changes for a trunk or channel. An RRQ is sent immediately for only the enabled trunks. Disabled trunks are NOT included in the report.
- Any changes in channel statuses (such as an active trunk going down, or an inactive trunk coming up), as they occur. Every lightweight RRQ automatically reports channel status changes when the status of any channel differs from the status previously reported. Only the channel status at the time the RRQ is generated matters. The channel status changes that occur between scheduled keepalive registrations are not reported.

In the absence of trunk or profile changes, for every lightweight RRQ sent by the MultiVoice Gateway during keepalive registration channel the status is checked and compared. Disabled trunks are also included in the RRQ sent during keepalive registration.

H.323 call signaling

During each VoIP call, a TAOS unit processes a variety of call signaling operations. These operations include

- Passing and responding to call-progress signals
- Delaying transmission of call-progress signals to the PSTN
- Passing and processing DNIS/ANI/CLID
- Performing call keepalive signaling with distant end points
- Enabling transparent processing of fax/modem signals

Controlling call-progress tones on a local gateway

For MultiVoice networks using non-PRI trunks, there is an answer supervision feature. The cut-thru-enable-nearend parameter enables call-progress tones from the distant PSTN to be passed across the IP network to the local TAOS unit. When enabled, the near-end TAOS unit in a VoIP call plays call-progress tones from the PSTN on the far-end out-dialed DS0. When disabled, the far-end TAOS unit locally generates call-progress tones. The result is that this feature allows callers at either end of a MultiVoice call to hear the call-progress tones from the distant PSTN.

Enabling call-progress tones provides answer supervision support for TAOS units using non-PRI trunks, by processing the call-progress tones from the distant PSTN. Using far-end cut-through, the tones from the PSTN on the far-end, out-dialed DS0 are passed back to the near-end gateway via RTP and made available for play before the call is actually setup. You can enter either of the following values:

Parameter value	Specifies
yes	(Default) That the near-end TAOS unit plays call-progress tones from the far-end out-dialed DS0. PSTN-generated call-progress tones are passed across the IP network, using RTP packets between gateways. The audio signals from the distant PSTN are compressed by the far-end gateway for transmission across the IP network, then decompressed by the near-end gateway and played for the caller.
no	That this feature is disabled. The near-end TAOS unit ignores the RTP audio signaling and attempts to play back local progress tones in response to Q.931 messages.

Changes to this value become effective with the next call.

The following example illustrates how to enable local call-progress tone cut-through for VoIP calls on a TAOS unit:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set cut-thru-enable-nearend = yes  
admin> write  
VOIP/{ 0 0 } written
```

The following dependencies apply to using the cut-thru-enable-nearend parameter:

- Network traffic volumes and voice quality determine when this parameter value should be modified. When call volumes increase, disabling this feature can improve call performance.
- When no is selected, callers hear silence until the local TAOS unit generates call-progress tones in response to Q.931 messages.



Note The fast H.245 (start H.245 before Q.931 CONNECT) is always used and has no impact.

Controlling transmission of call-progress tones to the PSTN

MultiVoice can delay transmission of call-progress tones to the PSTN until the call is answered. Delayed transmission avoids incurring PSTN charges for a call that is connected end-to-end across the VoIP network.

A MultiVoice Gateway can be configured through the command-line interface to delay sending the connect message to the ingress PSTN switch until the following information is received from the egress MultiVoice Gateway:

- An H.323 alerting message
- A call-progress message from the egress PSTN indicating the call has been answered

Previously, incoming VoIP calls from the PSTN were connected at the near-end gateway before any H.323 signaling was sent to the far-end gateway. As a result, a PSTN charge was incurred at the time the call connected to the near-end gateway, before the called party received and answered the call from the far-end gateway. This is called a true connect call.

True connection requires a default call type of voip on T1 or E1 trunks accepting incoming VoIP calls, as illustrated by the following:

```
[in T1/{ shelf-1 slot-10 1 }:line-interface]
default t-call-type = voip
[in E1/{ shelf-1 slot-11 1 }:line-interface]
default t-call-type = voip
```

The true-connect-enable parameter allows the operator to force the TAOS unit to delay alerting the PSTN, when applicable, and to send connect messages only when the equivalent H.323 messages are received. No PSTN charge is incurred unless the H.323 VoIP call is connected.



Note True connection does not work for E1 R2/R1 trunks. Use this feature only with T1-inband, T1-PRI, or E1-PRI trunks.

The true-connect-enable parameter may be assigned the following values:

Parameter value	Specifies
yes	An alerting message is sent to the ingress PSTN switch only when an H.323 alerting message is received on the ingress VoIP gateway, and a PSTN connect message is sent only when the H.323 VoIP call has been answered. This ensures that no charges are incurred for incomplete calls.

Parameter value	Specifies
no	(The default) An alerting message is sent to the ingress PSTN switch as soon as the connection is established with the ingress MultiVoice Gateway. This behavior results in the caller incurring a PSTN charge at the time of connection to the near-end gateway, before the called party has received and answered the call from the far-end gateway.

The following commands configure delayed PSTN alerting and connect messages (true connect signaling) on a TAOS unit:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set true-connect-enable = yes  
admin> write  
VOIP/{ 0 0 } written
```

The following dependencies apply to the true-connect-enable parameter:

- The default t-call-type parameter in the t1:line-interface or e1:line-interface sub-profile must be set to voip for T1 or E1 trunks used for incoming VoIP calls that require true connect signaling. Setting this parameter to voip causes *all* calls received on the trunk to be mapped to VoIP.
- The T310 timeout includes the time that the called party's phone is ringing, so a 10-second timeout can cause the near-end gateway to tear down the call too soon. With ISDN trunks, set T310 on the Telco switch or PBX to 30 seconds or greater when using the true connect feature.
- When the true connect feature is enabled and a VOIP call fails before the PSTN call is fully connected, the gateway is still able to send an appropriate tone or voice announcement to the caller.

Processing call failures

Call failures are reported for incoming PSTN calls by playing the appropriate tones or announcements to alert the caller of the call failure prior to connecting the call across the MultiVoice network. The ingress TAOS unit will only tear down the call after playing the proper tone or announcement to let the user know that the call failed.

Rerouting DTMF signals

Out-of-band processing of DTMF packets sends digits and tones received from the PSTN, by the near-end TAOS unit, across the network using non-UDP packets. When these packets reach the far-end TAOS unit, they are regenerated for use by the MultiVoice application or sent out to the PSTN.

DTMF tones may be degraded or distorted when they are encoded and decoded as part of the voice stream. Degradation and distortion results from the design of the audio codecs, which are intended to process speech and not DTMF tones. Consequently, DTMF input may not be detected by the far-end gateway or PSTN.

This dtmf-tone-passing parameter enables filtering the tone from the voice path and passing 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 will accept the out of band DTMF play-out commands. You can enter one of the following values:

Parameter value	Specifies
dtmf-tone-passed-inband	(Default) That the near-end TAOS unit passes PSTN-generated DTMF digits and tones as part of the voice processing stream. These tones will be compressed by the selected audio codec and transported across the IP network using UDP packets.
dtmf-tone-passed-outofband	That the near-end TAOS unit passes PSTN-generated DTMF digits and tones across the network using non-UDP packets. Once received at the far end, the digits are played out to the local PSTN/caller.
rtp	<p>DTMF tones are transferred and passed via the same channel to the decoding DSP, according to the RFC2833 standard.</p> <p>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.</p> <p>There is no negotiation of support for RFC2833 at call setup time. Therefore all machines in a network must support RFC2833 for any one of them to use it.</p> <p>Note Support for RFC2833 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)</p>

Changes to the dtmf-tone-passing parameter are effective with the next VoIP call.

To enable out-of-band DTMF processing for VoIP calls on an TAOS unit, set the dtmf-tone-passing parameter 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
```

Blocking Caller ID on a local gateway

MultiVoice administrators can block Caller ID at the destination gateway by preventing the Calling Line IDentification (CLID) string from being passed to the PSTN and the ultimate called destination. Certain carrier switches, which do not recognize the CLID sent from an inbound gateway, might subsequently reject outbound calls when they received the Caller ID from an outbound gateway. The switches expect the Caller ID to be the subscriber number configured by the subscriber-side PRI/BRI (MultiVoice supports only subscriber side ISDN).

The `clid-suppress` parameter blocks transmission of the caller's CLID to the PSTN. Blocking CLID transmission prevents switches from rejecting calls as a result of the Caller ID inconsistency and allows service providers to control and charge for Caller ID services.

You can enter either of the following values:

Parameter value	Specifies
yes	The local TAOS unit blocks transmission of the Caller ID (CLID) signals received from the distant TAOS unit, excluding from the data passed to the local PSTN.
no	(Default) That the local TAOS unit transmit the Caller ID (CLID) signals received from the distant TAOS unit, passing it to the local PSTN.

Changes to this parameter are effective with the next VoIP call.

To block outbound Caller ID on a MultiVoice Gateway, proceed as follows:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set clid-suppress = yes
admin> write
VOIP/{ 0 0 } written
```

Enabling keep alive registration between calling end points

TAOS units can determine whether a call's remote end point (such as gateway, terminal, PC, etc.) has become unreachable. A TAOS unit can subsequently terminate the connection.

The `call-keep-alive-timeout` parameter controls how often a MultiVoice Gateway polls a remote gateway or client during a VoIP call to verify that it is still functioning and reachable over the IP network. The same parameter setting specifies the time in which the remote gateway or client must respond before the call is dropped.

When the value of this parameter is set between 1 and 32767 (seconds), a keepalive packet is sent at regular intervals to the remote gateway or client. If no response is received, the call with that end point is dropped. If the call is dropped, the gateway sends a Drop Request (DRQ) message to the MVAM with the disconnect reason of "forcedDrop." When this parameter's value is 0, the default, this feature is disabled. Changes to this parameter take effect with the next VoIP call.

To enable keep alive registration on a TAOS unit for VoIP calls, proceed as follows:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set call-keep-alive-timeout = 150
admin> write
VOIP/{ 0 0 } written
```



Note Enabling keepalive registration only works with other MultiVoice Gateways and selected PC and terminal end points that are H.323 compliant. This feature is normally not used.

Enabling transparent fax/modem operations

MultiVoice Gateways can process fax/modem traffic over a VoIP channel, regardless of which audio codec is currently in use. A MultiVoice Gateway can detect a fax/modem transmission on a VoIP channel and enable fallback to the G.711 audio codec to allow transparent processing of fax/modem transmission. Detection of fax/modem is based on an algorithm that listens for an Answer tone, generated by an answering fax/modem. The Answer tone is significantly different for high-speed modems and fax terminals. The difference in Answer tones allows a MultiVoice Gateway uses to discriminate between the two types of equipment. Typically both real-time fax and transparent data can be enabled simultaneously.

To work, this feature must be enabled on MultiVoice Gateways at either end connecting the fax/modem call. Both MultiVoice Gateways must agree to transparent mode before the call bandwidth is increased to G.711 bandwidth, 64Kbps.

Using transparent modem with real-time fax

If a TAOS unit has been licensed for real-time fax, users can run either a high-speed modem with speeds greater than 2400bps or a fax terminal in the VoIP channel. This capability provides a fallback for real-time fax transmissions. Both fax terminals and high-speed modems transmit a single tone when they answer a call, but each type of equipment uses a different tone. The TAOS unit detects the type of equipment in use on the basis of its answer tone. When it detects the equipment answering the call, the TAOS unit sends H.245 request-mode messages to request a switchover from the current audio codec to either G.711 with no echo canceler (for transparent modem) or T.38 data mode (for real-time fax).

Transparent data is encoded as an audio-mode type, either G.711 μ -law (64Kbps) or G.711 a-law (64Kbps). Real-time fax (if supported) is encoded as data-mode type T.38 fax.



Note Transparent data mode introduces an H.245 request-mode message that is not backward compatible with the real-time fax feature provided by pre-TAOS 8.0 releases. To interoperate with a MultiVoice Gateway using transparent mode, all TAOS systems should be upgraded to TAOS 10.0.

Limitation for low-speed modems

Real-time fax cannot be used concurrently with low-speed modems (2400bps or less) because low-speed modems use the same answer tone as fax terminals. If a low-speed modem is used on a VoIP channel that is enabled for real-time fax, the Gateway detects a fax answer tone and requests T.38 encoding. The ingress gateway (typically the gateway on which the modem call originated) can accept the T.38

encoding request or reject the request, which causes the egress gateway to terminate the call.

G711-Transparent-Data parameter

Configure the g711-transparent-data parameter in the voip profile:

```
[in VOIP/{ 0 0 }]  
voip-index* = { 0 0 }  
gatekeeper-ip = 135.92.52.138  
gk-mlg-control = no  
vpn-mode = no  
single-dial-enable = no  
packet-audio-mode = g729  
frames-per-packet = 4  
...  
g711-transparent-data = no  
...
```

The g711-transparent-data parameter setting enables or disables transparent transmission of fax or modem signals across VoIP channels. When enabled, if a MultiVoice Gateway detects a fax or modem Answer tone in a VoIP channel, the unit transparently requests end-to-end G.711 encoding and bandwidth for the call, in a process similar to that used by real-time fax. The echo cancelers are disabled when the TAOS unit enters this mode, thus providing transparent G.711 encoding. The data is encoded transparently as an audio-mode type, either G.711 μ -law (64Kbps) or G.711 a-law (64Kbps).

The g711-transparent-data parameter accepts the following values:

Value	Specifies
yes	A MultiVoice Gateway transparently requests end-to-end G.711 encoding and bandwidth for the call upon detection of a fax or modem Answer tone in a VoIP channel.
no	(The default) A MultiVoice Gateway continues with VoIP call processing, even when a fax or modem Answer tone is detected.

The following commands enable the transparent modem feature on VoIP channels:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set g711-transparent-data = yes  
admin> write  
VOIP/{ 0 0 } written
```

The following commands enable both real-time fax and the transparent modem feature for high-speed modems:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set g711-transparent-data = yes
```

```
admin> list rt-fax-options
admin> set rt-fax-enable = yes
admin> write
VOIP/{ 0 0 } written
```

The g711-transparent-data parameter is N/A when either G.711 μ -law or G.711 a-law encoding is selected for the packet-audio-mode parameter (such as packet-audio-mode=g711-alaw).

Processing CED tones

A TAOS unit can detect two types of called station identification (CED) tones, fax and generic CED. Depending upon the type of CED tone detected, the TAOS unit will initiate a request for either transparent mode or T.38 fax mode.

The MultiVoice interface layer determines which mode to request on the basis of system configuration; initiating the request for the transparent mode or, when enabled, real-time fax. This is possible when the g711-transparent-data parameter is enabled, the TAOS unit has been licensed for real-time fax, and the rt-fax-options parameter have been enabled.

```
voip { 0 0 }
rt-fax-options = { yes }
g711-transparent-data = yes
```

In this case, when fax CED is detected, the gateway sends an H.245 RequestMode message for real-time fax using T.38. When generic CED is detected, the gateway sends an H.245 RequestMode message for G.711 with no echo canceller. It initiates a Bandwidth Request (BRQ) for bandwidth of 64Kbps.



Caution Low-speed modems (≤ 2400 bps) use the same CED as fax terminals. Running a low-speed modem on a VoIP channel when real-time fax is enabled causes the gateway to attempt a switch over to T.38 fax mode. If the ingress gateway (typically the fax/modem originate side) accepts the switch over request, then the VoIP call is changed to T.38. If the ingress gateway rejects the switch over then the call is terminated on the egress gateway.

If VoIP users run low-speed modems, then the gateway must be configured so that real-time fax is disabled and transparent data is enabled as follows:

```
voip { 0 0 }
rt-fax-options = { no }
g711-transparent-data = yes
```

Deactivating trunks used for VoIP calls

The trunk-quiet-escape-enable parameter enables MultiVoice Gateways to automatically deactivate trunks used for VoIP calls when a gateway becomes unavailable. When parameter value is yes, trunks configured to accept VoIP calls are made unavailable to the PSTN under the following conditions:

- A gateway cannot register with either a primary or secondary gatekeeper.
- A gateway's trunk connection with the PSTN is unavailable, so that gateway is forced to unregister itself from its gatekeepers.

Previously, when a Gateway could not register with the primary and secondary gatekeeper, the caller heard a fast-busy signal because the PSTN switch continued to

route calls to the trunks on that gateway. Deactivating the trunk changes the trunk state to inform the PSTN switch that those trunks are not available and forces the gateway to unregister from all known gatekeepers.

When the TAOS unit becomes unregistered, the gatekeepers route new calls to other gateways. Calls already in progress remain active until they are terminated by the caller or PSTN. When any one of the gateway's trunks comes back in service, that gateway starts registering itself with one of its gatekeepers. The gatekeeper then begins to route calls to this gateway.



Note System-wide deactivation can occur only on T1 trunks that use ISDN PRI signaling and have been configured for VoIP.

Enabling the trunk-quiesce-enable parameter

The trunk-quiesce-enable parameter enables automatic trunk deactivation whenever a MultiVoice Gateway is unable to register with either a primary or secondary MVAM, or force a MultiVoice Gateway to unregister whenever the trunk connection to the PSTN is unavailable.

Assigning the value yes to the trunk-quiesce-enable parameter causes the MultiVoice Gateway to be unavailable to accept calls whenever it becomes unregistered or it loses the connection to the PSTN. Assigning the value no, the default, allows it to continue processing call requests when unregistered or its PSTN connection goes down.

The following commands enable trunk deactivation for T1 PRI lines configured for VoIP:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set trunk-quiesce-enable = yes
admin> write
VOIP/{ 0 0 } written
```

Configuring PSTN call signaling

An egress MultiVoice Gateway can manage call signaling with the switched network by:

- Enabling transparent delivery of Q.931/Q.850 cause codes received from the PSTN by the far-end MultiVoice Gateway to the near-end MultiVoice Gateway
- Enabling configuration of the bearer capabilities sent in the Q.931 Setup message by the far-end MultiVoice Gateway for outbound calls to the switched network
- Enabling configuration of reporting the Q.931 Progress Indicator information element (IE) in the Proceeding and Alerting message by the near-end MultiVoice Gateway to the switched network configurable

MultiVoice call signal processing made is consistent with the following telecommunications standards:

- ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1) - ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993), International Telecommunications Union
- ITU Telecommunication sector standard (ITU-T) Q.850, *Usage of Cause and Locations in the Digital Subscriber Signalling (sic) System No. 1 and the Signalling (sic) System No. 7 ISDN User Part* (Mar. 1993), International Telecommunications Union

Transparent reporting of disconnect cause codes

MultiVoice provides transparent reporting of call disconnect cause codes for both the far-end MultiVoice Gateway and near-end MultiVoice Gateway using Q.931 (H.323) or Q.850 (SS7) signaling.

If the inbound PSTN connection uses PRI signalling when a VoIP call is disconnected, the near-end MultiVoice Gateway passes the Q.931 disconnect message—generated by the far-end PSTN and passed across the packet network by the far-end MultiVoice Gateway—directly to the near-end switched network. When the Q.931 disconnect message is received by the local telephone company switch, it plays the appropriate tone for the caller. The near-end MultiVoice Gateway does not play any voice announcement or tones.

If the inbound PSTN connection uses inband signalling, or the call is disconnected internally, the near-end MultiVoice Gateway responds to the Q.931/Q.850 cause codes, reporting the information to the MVAM. Then the near-end MultiVoice Gateway generates either the appropriate call-progress tone or voice announcement for the caller, depending upon the instructions it receives from MVAM.

With transparent reporting of call disconnect cause codes disabled, when a VoIP call is disconnected the near-end MultiVoice Gateway plays the appropriate voice announcement or tones for the end user. Then the near-end MultiVoice Gateway sends Q.931 disconnect message with cause code NORMAL (16). to the local telephone company switch.

Configuring bearer capabilities for outbound calls to the PSTN

An egress MultiVoice Gateway can be configured to request a specific bearer service from the switched circuit network for outbound VoIP calls. The MultiVoice Gateway can be configured to request the following bearer services from the egress switched telephone network for outbound call processing:

- Speech
- Unrestricted digital information
- Restricted digital information
- 3.1 kHz audio
- Video

Request for a specific bearer service is transmitted to the switched telephone network in the bearer service information element of the call-setup message sent by the MultiVoice Gateway. For more information see “4.5.5 Bearer capability” in ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1)—ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993). The bearer service request is configured through the TAOS administration interface. Prior to TAOS 10.0, the egress MultiVoice Gateway always requested “speech” bearer service when connecting a VoIP call to the switched telephone network.

Q.931 Call signaling progress indicator

An egress MultiVoice Gateway can be configured to forward the Q.931 progress indicator information element as part of the Alerting and Proceeding message sent to the ingress switched network. The Q.931 progress indicator information element

describes call routing events on the egress switched telephone networks used for a VoIP call.

When use of the progress indicator information element is enabled, a MultiVoice Gateway includes the call routing event descriptions in the Alerting and/or Proceeding messages sent to the ingress switched network. The progress indicator information element reports one of the following routing conditions:

- Call is not end-to-end ISDN; further call-progress information may be available in-band.
- Destination address is non-ISDN.
- Origination address is non-ISDN.
- Call has returned to the ISDN.
- Interworking has occurred and has resulted in a telecommunication service change.
- In-band information or an appropriate pattern is now available.

For more information on the use of the progress indicator information element, see “4.5.23 Progress Indicator” and “Annex G” in ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1)—ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993).

Detecting and reporting call-progress

To detect progress indicators in call alerting and proceeding messages on a near-end MultiVoice Gateway, inbound VoIP calls from the switched telephone network must be differentiated from non-VoIP calls (such as, analog).

When using inband signaling, the default `t-call-type` parameter in the `t1:line-interface` or `e1:line-interface` sub-profile specifies what call-type the MultiVoice Gateway should expect for incoming calls on this trunk, for purposes of call routing. The default `t-call-type` parameter applies to inband and PRI signaling for VoIP calls. Set `default-call-type=voip` to enable sending the progress indicator in call alerting and proceeding messages for PRI signaling.

pstn-attribute subprofile

This feature adds the `pstn-attribute` subprofile to the `voip` profile. This profile contains the following parameters:

```
admin> list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
cause-code-transparency = no
alert-progress-indicator = no-progress-indicator
proceed-progress-indicator = no-progress-indicator
bearer-capability = speech
```

cause-code-transparency parameter

The `cause-code-transparency` parameter in the `pstn-attribute` sub-profile of the `voip` profile enables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network—passed across the packet network from the far-end MultiVoice Gateway to the near-end MultiVoice

Gateway—to the local telephone company. The local telephone company switch then plays the appropriate tone or disconnect message for the caller.

The cause-code-transparency parameter may be assigned the following values:

Parameter value	Specifies
yes	Enables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network to a local telephone company switch, across a MultiVoice network. The local telephone company switch responds to these messages by playing the appropriate tones or messages for the caller.
no	(The default) Disables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network to a local telephone company switch, configuring the near-end MultiVoice Gateway to play the appropriate tones or messages for the caller.

Changes to the cause-code-transparency parameter take effect with the next VoIP call. The following example illustrates how to enable transparent delivery of disconnect cause codes:

```
tnt132>read voip { 0 0 }  
VOIP/{ 0 0 } read  
  
tnt132>list pstn-attribute  
[in VOIP/{ 0 0 }]:pstn-attribute]  
cause-code-transparency = no  
....  
  
tnt132>set cause-code-transparency = yes  
  
tnt132>write  
VOIP/{ 0 0 } written
```

The cause-code-transparency parameter has the following dependencies:

- This parameter should be enabled (cause-code-transparency=yes) whenever voice announcement reporting is enabled (h323-voice-ann-enabled = yes), for callers to hear both a busy signal and the call failure message. When voice announcements are enabled, if transparent delivery of disconnect codes is disabled (cause-code-transparency=no), callers do not hear the busy tone. Instead, the near-end MultiVoice Gateway plays the call failure message.

alert-progress-indicator parameter

The alert-progress-indicator parameter in the pstn-attribute sub-profile of the voip profile configures the type of call-progress events that are captured and reported in the Q.931 Alert message progress indicator information element by the MultiVoice Gateway. Once configured, MultiVoice Gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

The alert-progress-indicator parameter may be assigned the following values:

Parameter value	Specifies
no-progress-indicator	(The default) Disables alert reporting of call routing events on the egress switched telephone network.
none-end2end-isdn	The egress MultiVoice Gateway reports when calls are connected to a egress switched telephone network which does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF signaling.
dest-non-isdn	The egress MultiVoice Gateway reports when calls are connected to a egress switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not return call-progress signals to the MultiVoice Gateway.
orig-non-isdn	The ingress MultiVoice Gateway reports when calls are received from a local switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not provide call-progress signals to the MultiVoice Gateway.
return-to-isdn	The egress MultiVoice Gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.
interworking-occurred	The egress MultiVoice Gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
inband-info-available	The egress MultiVoice Gateway reports if inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

The following example illustrates how to set the parameter for reporting calls that are connected to a far-end switched telephone network that does not use ISDN signaling:

```
tnt132>read voip { 0 0 }  
VOIP/{ 0 0 } read
```

```
tnt132>list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
....
alert-progress-indicator = no-progress-indicator
....
tnt132>set alert-progress-indicator = none-end2end-isdn
tnt132>write
VOIP/{ 0 0 } written
```

Changes to the alert-progress-indicator parameter take effect with the next VoIP call.

proceed-progress-indicator parameter

The proceed-progress-indicator parameter, in the pstn-attribute sub-profile of the voip profile, configures the type of call-progress events that are captured and reported in the Q.931 Proceeding message progress indicator information element by the MultiVoice Gateway. Once configured, MultiVoice Gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

The alert-progress-indicator parameter can be assigned the following values:

Parameter value	Specifies
no-progress-indicator	(The default) Disables alert reporting of call routing events on the egress switched telephone network.
none-end2end-isdn	The egress MultiVoice Gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF signaling.
dest-non-isdn	The egress MultiVoice Gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling, such as a transit network or private network, that does not return call-progress signals to the MultiVoice Gateway.
orig-non-isdn	The ingress MultiVoice Gateway reports when calls are received from a local switched telephone network that does not use ISDN signaling, such as a transit network or private network, which does not provide call-progress signals to the MultiVoice Gateway.
return-to-isdn	The egress MultiVoice Gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.

Parameter value	Specifies
interworking-occurred	The egress MultiVoice Gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
inband-info-available	Assigning this value, the egress MultiVoice Gateway reports if inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

The following example illustrates how to set the parameter to report calls that are proceeding on a far-end switched telephone network that does not use ISDN signaling:

```
tnt132>read voip { 0 0 }  
VOIP/{ 0 0 } read  
  
tnt132>list pstn-attribute  
[in VOIP/{ 0 0 }]:pstn-attribute]  
....  
proceed-progress-indicator = no-progress-indicator  
....  
  
tnt132>set proceed-progress-indicator = none-end2end-isdn  
  
tnt132>write  
VOIP/{ 0 0 } written
```

Changes to the proceed-progress-indicator parameter take effect with the next VoIP call.

bearer-capability parameter

The bearer-capability parameter, in the pstn-attribute sub-profile of the voip profile, configures the request for a specific bearer service from the egress switched circuit network for outbound VoIP calls. The request is transmitted to the switched telephone network in the bearer service information element of the call-setup message sent by the MultiVoice Gateway.

The bearer-capability parameter may be assigned the following values:

Parameter value	Specifies
speech	(The default) Requests a switched network routing over a channel that supports speech bearer capability.
unrestricted-digital-info	Requests a switched network routing over a channel that supports unrestricted digital information (UDI) bearer capability.

Parameter value	Specifies
restricted-digital-info	Requests a switched network routing over a channel that supports restricted digital information (RDI) bearer capability.
audio-3100hz	Requests a switched network routing over a channel that supports digital audio bearer capability up to 3.1kHz.
video	Requests a switched network routing over a channel that supports video signaling bearer capability.

The following example illustrates how to specify digital audio bearer capability for VoIP calls:

```
tnt132>read voip { 0 0 }
VOIP/{ 0 0 } read
tnt132>list pstn-attribute
[in VOIP/{ 0 0 }]:pstn-attribute]
....
bearer-capability = speech
tnt132>set bearer-capability = audio-3100hz
tnt132>write
VOIP/{ 0 0 } written
```

Changes to the bearer-capability parameter take effect with the next VoIP call.

Multiple Logical Gateways

TAOS implements dynamic call control for H.323 VoIP calls on MultiVoice networks and provides support for partitioning a single MultiVoice Gateway into multiple logical gateways. Using this method of call control lets the H.323 Gatekeeper perform call-specific administration on a call-by-call basis.

Call-specific administration of H.323 VoIP calls is allowed for the following call control functions on the same physical MultiVoice Gateway:

- PIN prompting
- Single-stage dialing
- Two-stage dialing
- Voice announcement playback
- Configurable call timers for prepaid and credit card billing systems

MVAM analyzes call performance data (trunk group, DS0 status, and call activity) received when a gateway performs periodic keepalive registration. When MVAM responds to subsequent call requests from each gateway, the Administration Conformation (ACF) message includes any changes defined for the aforementioned call administration parameters. The gateway applies the parameter changes received from MVAM to the current call request. This information is stored as part of the nonstandard data included in registration, admission and status (RAS) messages exchanged by the gateway and gatekeeper for each call.



Caution Dynamic call control and multiple logical gateways are only supported in MultiVoice networks running TAOS 10.0 on the gateways and MVAM 3.0 on the gatekeepers. These features are not supported in MultiVoice networks where gatekeepers are running Release 2.x of MVAM.

MVAM 2.x configures all H.323 call management features globally, on each MultiVoice Gateway, using the values assigned in the Voip Options profile. A gatekeeper running MVAM 3.0 can send instructions to the ingress gateway which override global call management settings utilizing status information reported by MultiVoice Gateways. The decision to override the global call management settings can be based upon reported ingress trunk or DS0 groups, Caller ID, time-of-day, gateway, etc.

The rules used to apply overrides to H.323 call management parameters are configured on MVAM. These parameter changes are useful when partitioning MultiVoice Gateways into logical gateways. *Logical gateways*, defined on MVAM, treat selected trunk groups on a MultiVoice Gateway as if they were a unique VoIP gateway. Initially, MultiVoice Gateways must have T1, T3 and PRI trunks to support logical gateways.



Note While BRI lines can still be used for VoIP, the multiple logical gateway features are not supported on MultiVoice Gateways that use BRI.

A MultiVoice Gateway cannot identify its own logical gateways. Only the gatekeeper running logical gateways can identify the MVAM. However, a gateway must be configured to apply instructions received from MVAM when processing the current call.

H.323 Call-specific administration

H.323 call-specific administration lets MVAM override defaults for PIN authentication, dialing mode and voice announcement playback.

MVAM can enable call-specific administration on the basis of the reported DNIS, ANI, trunk group and DS0 information, or any combination of that data, which are all reported in the first ARQ from the gateway.

Dynamic PIN authentication

When multiple logical gateways are enabled on a MultiVoice Gateway, any incoming call request immediately sends an ARQ to MVAM that include the following information:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM sends an ACF message to the gateway. The gateway then processes the call as if the following VoIP parameters were set to these values:

`vpn-mode=yes`
`single-dial-enable=yes`

If MVAM or a third-party billing application used with MultiVoice requires PIN authentication for the call, an Admission Reject (ARJ) message is issued directing the gateway to set `vpn-mode=no` for this call. The gateway then resumes call handling as if

the call had just arrived from the PSTN but prompts for authentication (as if `vpn-mode=no`) before continuing with call processing.

Dynamic single-stage and two-stage dialing

When the multiple logical gateways are enabled on a MultiVoice Gateway, any incoming call request immediately sends an ARQ to MVAM that includes the following information:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM sends an ACF message to the gateway. The gateway then processes the call as if the following VoIP parameters were set to these values:

`vpn-mode=yes.`
`single-dial-enable=yes`

If MVAM or a third-party billing application used with MultiVoice requires a caller perform two-stage dialing for this call (dialing the destination telephone number after dialing into the MultiVoice Gateway), an Admission Reject (ARJ) message is issued directing the gateway to set `single-dial-enable=no` for the call. The gateway will then resume call handling as if the call had just arrived from the PSTN, but prompt the caller to enter the destination telephone number (`single-dial-enable=no`) before continuing with call processing.

Static announcement branding

When the multiple logical gateway feature is enabled on a MultiVoice Gateway, MVAM or a third-party billing application can select a set of voice announcements for playback from multiple sets of voice announcements stored on the gateway. This is known as *branding*.

By sending either an ARJ or ACF message containing an announcement directory specifier, the gateway plays voice announcements from the named directory on the PC flash card for the current call.

Executing the branding instructions, the gateway searches for the voice announcement directory using the value set in the `voice-ann-dir` parameter. When `voice-ann-dir=/current` (default) and MVAM requests a specific directory (brand) of announcements for a call, the gateway searches for those announcements starting in the `/current` directory. For example, if MVAM specifies `italian`, the gateway searches for announcements in the directory `/current/italian/`.



Note It is recommended that you use only four brands of static announcements because there are limitations in the announcement cache size. Using more than four brands degrades announcement quality and overall gateway performance.

Configurable call timers

MultiVoice supports the use of configurable call timers, controlled by MVAM or a third-party billing application that supports timed billing plans (such as prepaid phone cards or prepaid cellular accounts).

Using an ACF message, MVAM or a third-party billing application, set the following timers:

Timer	Description
Call countdown timer	<p>Sets the time remaining before a gateway disconnects the current call. When this timer expires, the gateway plays an announcement that time has expired and disconnects the call.</p> <ul style="list-style-type: none">• By default, once the timer on the gateway is set, the h323drq.au announcement file is played back for the caller upon call termination.• If the MVAM or third-party billing application uses its own countdown timer, the announcement specified in an Disengage Request (DRQ) message can be used to select a different announcement file for playback upon call termination.
Call disconnect warning timer	<p>Specifies when a call disconnect warning announcement is played for the caller. This announcement alerts the caller to the time remaining before this call is terminated.</p> <ul style="list-style-type: none">• By default, once the timer on the gateway is set, the h323bki n.au announcement file is played back for the caller when the time expires.• If the MVAM or third-party billing application uses its own disconnect warning timer, the announcement specifier in an Interrupt Request (IRQ) message can be used to select a different announcement file for playback when this timer expires.

H.323 call-specific administration messages

Call administration information is transmitted as part of the nonstandard data included in registration, admission and status (RAS) messages exchanged between the gateway and gatekeeper for each call. This data consists of a set of parameters using URL encoding, as described in RFC 1738, with each parameter composed of a set of attribute value pairs.

This nonstandard data may include the following call administration information:

- ANI/CLID
- Conference identifier
- User PIN
- Inbound or outbound trunk identification
- Enable voice announcement playback
- Select voice announcement playback
- Internal call timer and disconnect timer settings
- Call failures
- Call results

- Trunk group and DS0 status information
- Available digital signal processors (DSPs)
- Maximum number of calls a MultiVoice Gateway may support

Trunk and call status reporting

Each MultiVoice Gateway reports its current call processing status as part of a Registration Request (RRQ) message to MVAM. The RRQ message includes data on trunk, trunk group, and DS0 status. The initial RRQ message, sent to MVAM when a gateway is initialized, contains a full report on all the trunks used by the physical gateway. The RRQ messages sent during keepalive registration include only the status changes since the previous registration message.

DS0 status (in-service/out-of-service)

A MultiVoice Gateway reports trunk, trunk group, and DS0 information to MVAM for each trunk. This includes:

- Trunk group
- Physical address
- DS0 service status (in-service or out-of-service)



Note A DS0 is in service for a logical gateway when it belongs to the associated trunk group and is in the up state. Information regarding DS0 activity (in use, free) is not reported via RRQ. DS0 activity is reported separately, traced from the per-call trunk/DS0 reporting mentioned below.

Trunk groups and physical address (shelf, slot, etc.) information are provided to MVAM to allow dynamic tracking of DS0 activity and trunk group assignments, and provided for future support of DS0 selection by physical-address for outbound PSTN calls.

Full trunk and DS0 status reporting is performed only when necessary, enhancing gateway performance. Full RRQs report complete trunk and DS0 information, usually when a gateway is initialized or else when requested by MVAM. Lightweight RRQs are used to report only status changes for trunk and DS0 information. MVAM can request complete trunk and DS0 information by responding to a lightweight RRQ with a Registration Reject (RRJ) message containing the reject reason Full Registration Required.



Note Currently, trunk and DS0 status are not reported for BRI lines. Only the following information is reported for MultiVoice Gateways that use BRI:

- Number of idle VoIP ports.
- Value of maxcalls in voip profile.

Trunk and DS0 reporting (per call)

Trunk group and physical address information for the DS0 connection are reported for each call processed by a MultiVoice Gateway. This information is sent from the

gateway to the gatekeeper as nonstandard data in these registration, admission, and status (RAS) messages for the following call types:

Table 3-1. Trunk Messages

Message	Call type	Trunk or DS0 information
Admission Request (ARQ)	Inbound (from PSTN)	The trunk group and physical address of the DS0 upon which the call arrived.
Bandwidth Request (BRQ)	Outbound (to PSTN)	The trunk group and physical address of the DS0 upon which the call went out.
Disengage Request (DRQ)	Inbound (from PSTN) and Outbound (to PSTN)	The physical address of the DS0. Note For outgoing PSTN calls, the trunk group or DS0 information might not be present.
Disengage Confirmation (DCF)	Inbound (from PSTN) and Outbound (to PSTN)	The trunk group and DS0 information for gatekeeper-initiated call terminations.

Trunk and DS0 selection (per call)

Currently, MultiVoice Gateways only support trunk-group based routing for outbound PSTN calls. To do this, trunk groups must be enabled in the System profile of each gateway in the MultiVoice network. Each T1 or E1 line must also be assigned a trunk group.



Note Trunk groups should only be assigned at the T1 level.

The physical address information collected by the gateway for each DS0 is used currently by MVAM to track DS0 activity dynamically. The physical address is currently not used for DS0 to DS0 linking. In the future, both trunk group and/or physical address information will be available for DS0 selection on the gateway. When this happens, trunk groups should only be used when processing both VoIP and data calls on the same gateway. Otherwise, only gatekeeper, physical-address based, DS0 routing should be used.

gk-mlg-control parameter

The gk-mlg-control parameter in the voi p profile enables the MultiVoice Gateway to accept and process call-specific administration instructions from MVAM 3.0.

When enabled, the gateway can apply call-specific processing instructions for PIN authentication, single- or two-stage dialing, voice announcement playback, and configuring call timers for prepaid billing. Values received from MVAM or third-party billing systems override parameter settings in the voi p profile that process the current VoIP call.

Rules used for performing call-specific administration are configured on MVAM and are used when partitioning MultiVoice Gateways into multiple logical gateways. This allows MVAM to administer a single physical gateway as if it were multiple gateways, partitioning the gateway according to trunk groups, DNIS, time of day, etc.

Call-specific administration is enabled by specifying yes, enabling the processing of call-specific administration instructions. The default, no, causes reversion to global administration of VoIP calls using the values set in the voip profile.

The following example illustrates how to enable multiple logical gateway processing on a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set gk-mlg-control=yes
admin> write
VOIP/{ 0 0 } written
```

This parameter has the following dependencies:

- If gk-mlg-control=yes, the value of the vpn-mode parameter defaults to N/A
- If gk-mlg-control=yes, the value of the single-dial-enable parameter defaults to N/A

Changes to this parameter are effective with the next VoIP call.

Setting H.323 dialing options

MultiVoice offers a set of dialing options that support the following:

- Adjusting the amount of time a caller has to dial a telephone number
- Performing single-stage dialing of telephone numbers
- Rerouting blocked VoIP calls back out over the local PSTN
- Deactivate trunks used for VoIP calls
- Request operator assistance during the dialing phase
- Enable early ringback signaling
- Enable the use of trunk prefixes for routing VoIP calls out to the local PSTN
- Enabling user-entered authentication
- Determining the length of a dial string

Adjusting and troubleshooting the interdigit timer

The call-inter-digit parameter limits how long a TAOS unit waits for a caller to enter a single digit when using two-stage dialing. The customer may set the interdigit timer, for any value between 1 and 20 seconds, by changing the value of the call-inter-digit-timeout parameter.

By default, callers have 6 seconds to enter each digit of a telephone number, with a one-second decrement for each digit a caller enters. When the timer expires, the dialing is considered to be complete and the call proceeds. If callers finish dialing before the time expires, they can wait up to 16 seconds or press the pound (#) key before the gateway continues processing the call.

Setting the primary-retries parameter in the voip profile to zero (0) disables this feature. You may enter any value between 300msec and 20,000msec (0.3 seconds and 20 seconds). Changes to this value become effective with the next registration cycle. This value defaults to 6000msec.

The following example illustrates how to set the value of the interdigit timer:

```
admin> read voip { 0 0 }
VOIP/{0 0} read
admin> list call-inter-digit-timeout
[in VOIP/{ 0 0 }:call-inter-digit-timeout]
call-inter-digit-timeout = 6000
admin> set call-inter-digit-timeout = 4000
admin> write
VOIP/{ 0 0 } written
```

The following dependencies apply to adjusting the inter-digit timer:

- This timer setting is applied to PIN entries and digits dialed after entering the telephone number.
- Values below 300 milliseconds may result in dropped digits.

Troubleshooting the interdigit timer

There are two common problems that result from setting the interdigit timer value too low. They are as follows:

Trouble	Corrective action
Enabling or resetting the interdigit timer may result in dropping dialed digits.	Dropping dialed digits usually occurs if the gateway is configured to wait for a short, 300msec to 1,000msec, time interval. To correct this problem, increase the time interval to 3000msec, or higher, depending upon the frequency and severity of the problem.
Enabling the inter digit timer caused single-stage dialing to fail	Under certain circumstances, enabling the interdigit timer can cause single-stage dialing to fail. When this occurs, try increasing the time interval for single-digit collection. If that fails to correct the problem, disable the configurable interdigit timer by turning digit collection off in the Line-Interface sub-profile of the T1 or E1 profile.

Configuring single-stage dialing

The `single-dial-enable` parameter is used to enable or disable single-stage dialing of VoIP calls when MultiVoice is configured to perform H.323 call processing. You can enter either of the following values:

Parameter value	Specifies
yes	The TAOS unit extracts the Dialed Number Identification Service (DNIS) string for the destination telephone number from a single dialed entry. The destination number is passed to the distant gateway during call-setup.
no	(Default) That this feature is disabled. Callers are required to dial the TAOS unit, then wait for a subsequent dial tone before dialing the called telephone number.

The following example illustrates how to enable single-stage dialing on a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set single-dial-enable = yes
admin> write
VOIP/{ 0 0 } written
```

Single-stage dialing works with MultiVoice Gateways under the following conditions:

- You are using T1 inband trunks, and the switch (or PBX) can relay DTMF signals to the MultiVoice Gateway.
- You are using T1 PRI trunks.
- You have enabled collection of DNIS/ANI on the TAOS unit.

For additional information see “Configuring trunk signaling for H.323 VoIP networks” on page 2-54.

Using H.323 single-stage dialing without PIN authentication

Users do not need to enter a Personal Identification Number (PIN) authentication to complete a VoIP call if `vpn-mode = yes` or users are authenticated using ANI. Callers enter only the MultiVoice access number followed by the destination phone number (DNIS). For example, they can enter 997325551212. The digits specify the following:

Table 3-2. Digits

99	The access number. This can be either single or multiple digits, configurable by the service provider. This number is not forwarded to the destination gateway.
7325551212	The destination phone number. This is a real destination number (DNIS) that must be sent to destination gateway. This number could be a PBX extension (such as 3103 in a company 's private phone network) or a full public phone number as shown here.

Using H.323 use single-stage dialing with PIN authentication

Users can enter the access number, followed by the destination phone number, and be prompted to enter their PIN to complete a VoIP call if `vpn-mode = no`. Callers enter the MultiVoice access number and destination phone number (DNIS) all at one time, then hear the PIN prompt (three short beeps). The user must enter the PIN to initiate call processing. In future releases, callers hear a voice announcement "Please enter you PIN number."

Rerouting blocked calls over the local PSTN

When a TAOS unit is unable to process an incoming voice call because registration with the gatekeeper fails, it can attempt to connect the call using its local PSTN connection.

This technique of turning the call back from the MultiVoice Gateway over the PSTN is called hairpin dialing. This allows a TAOS unit to complete calls over the public switched network when it is unable to route them over the IP network.

The `call-hairpin` parameter controls whether a TAOS unit will attempt to re-route blocked calls using its local PSTN connections. You may enter either of the following values:

Parameter value	Specifies
yes	The TAOS unit connects calls using the PSTN if it cannot register with a MultiVoice Gatekeeper (MVAM).
no	(Default) The TAOS unit does not connect calls using the PSTN if it cannot register with MVAM. New call requests are rejected until it successfully registers with a gatekeeper.

Changes to this value take effect with the next VoIP call.

To enable hairpin dialing on a TAOS unit for VoIP calls:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set call-hairpin = yes  
admin> write  
VOIP/{ 0 0 } written
```



Note Hairpin dialing only works when a second DSP is available in the same TAOS unit to handle the outbound call to the PSTN. That DSP may be on the same MultiDSP slot card or a second DSP slot card installed in the same shelf of the TAOS unit.

Requesting operator assistance

Callers can request operator assistance during the dialing phase of a MultiVoice call. A TAOS unit can be assigned a dial string, up to five-digits long, that can be entered by a caller to connect that caller to an operator.

Callers can enter a set of digits (such as: *0, 09, etc.) when they need operator assistance during the dialing stage of a MultiVoice call. The digit string used to request operator assistance is defined in the `operator-assist` parameter in the `voip` profile.

When the caller enters the operator assistance digits, the TAOS unit sends them to MVAM, which translates these digits into the actual number to dial for operator assistance. MVAM sends this number to the far-end MultiVoice Gateway to connect the call to an operator.

Once the call is connected, the digit string used to request operator assistance is available for normal call processing functions, such as responding to automated attendants, AUDIX, etc.

The operator assistance option is supported for MultiVoice Gateways operating as either multiple logical gateways (`gk-ml g-control = yes`) or as a single gateway (`gk-ml g-control = no`). To provide operator assistance requires MVAM 3.1.0 be installed and running on the gatekeeper.

operator-assist parameter

The operator-assist parameter defines the dial string a caller enters when requesting operator assistance. This parameter value can be up to five digits long.

The operator-assist feature is enabled by entering a two to five-digit dial string containing an asterisk (*) in either the first or second position. This parameter accepts the asterisk (*) plus any number(s) 0 through 9 as a valid entry. By default this value is *0. This feature is disabled by assigning a NULL value to the operator-assist parameter.

The following illustrates how to set the value of the operator-assist parameter:

```
tnt17>read voip { 0 0 }
VOIP/{ 0 0 } read
tnt17>set operator-assist = *9
tnt17>write
VOIP/{ 0 0 } written
```

To disable the operator assistance feature, set the value of the operator-assist parameter value as illustrated:

```
tnt17>set operator-assist =
tnt17>write
VOIP/{ 0 0 } written
```

The operator-assist parameter has the following dependencies:

- The first or second digit of the dial string must always be an asterisk (*).
- A MultiVoice Gateway must be configured for two-stage dialing (`single-dial-enable = no`).
- The gatekeeper must be running MVAM 3.1.0.
- A translation rule must be defined in one of the ingress translation tables used by MVAM that contains the actual dialed number used to connect calls to operator assistance.

Enabling early ringback

The early-ringback-enable parameter allows a TAOS unit to generate a ringback tone locally, as soon as the call is started on the far-end gateway. Early ringback eliminates delays in call notification times, which can occur in certain VoIP network configurations (such as satellite IP networks, wireless networks, or networks using

channel-associated signaling (CAS) trunks). Delays in call notification in these network environments can cause callers to hang up before the call completes, while waiting for call-progress tones from the far-end PSTN.



Caution Early ringback is intended for use only on networks that experience long call-setup times. Its use for other network configurations is not recommended and might result in erroneous ring-to-busy and ring-to-failure announcements.

The following settings enables early ringback:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set early-ringback-enable = yes  
admin> write  
VOIP/{ 0 0 } written
```

Enabling trunk prefixing

The trunk-prefix-enable parameter enables a TAOS unit to identify and assign an egress trunk group to the destination telephone number. When received by the egress MultiVoice Gateway or call signaling entity, the trunk group prefix is used to select the egress trunk to connect the call.

With trunk prefixing, the TAOS unit is able to identify the entry (ingress) trunk number to the exit (egress) gateway or call signaling entity by prepending the ingress trunk number to the DNIS number. Trunk groups must be in use system-wide.

When trunk prefixing is enabled, the system obtains the trunk group number from both:

- The trunk-group parameter in the T1 line profile associated with the inbound trunk on the ingress MultiVoice Gateway
- The ACF message from MVAM

Once assigned, the trunk group number is prepended to the destination telephone number. The trunk group/dial string combination is sent as the Q.931 Called Party Number information element (IE) in an H.225/Q.931 SETUP message to the egress MultiVoice Gateway. The destination address value of the SETUP user-to-user information element (UUIE) is not currently encoded.

Trunk-Prefix-Enable parameter

When set to yes, the trunk-prefix-enable parameter causes an egress MultiVoice Gateway to route outbound calls to the PSTN using a preselected trunk group, assigned by either the ingress MultiVoice Gateway or MAVM. When set to no, the default, the egress MultiVoice Gateway selects trunk groups for outbound calls.

For example, the following commands enable trunk prefixing, beginning with the next VoIP call the TAOS unit receives:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set trunk-prefix-enable = yes  
admin> write  
VOIP/{ 0 0 } written
```

This parameter has the following dependencies:

- Using trunk groups must be enabled in the system profile on the egress MultiVoice Gateway (use-trunk-groups = yes).
- The size of the trunk groups must be defined (num-digits-trunk-groups = 1) in the system profile on all egress MultiVoice Gateways.
- Trunk group numbers must be assigned in both the T1 trunk and line profiles for egress T1 trunks.

Configuring PIN collection

The `vpn-mode` parameter enables or disables collection of a MultiVoice user's PIN by this TAOS unit when MultiVoice is configured to perform H.323 call processing. This parameter controls whether a user must enter a separate PIN code when placing a VoIP call.

User PINs are assigned by MVAM, whenever a new user is added to the gatekeeper's database. After a user enters a PIN, it is sent to the gatekeeper as part of the call admissions request (ARQ) from the TAOS unit. The gatekeeper then authenticates the user before continuing with call-setup.

You may enter either of the following values the `vpn-mode` parameter:

Parameter value	Specifies
yes	The TAOS unit does not prompt for a user-entered PIN. All calls are admitted without requiring user-entered authentication, as if the call were made on a virtual private network.
no	(Default) The TAOS unit prompts callers for their PINs before admitting calls. The TAOS unit presents callers with either a dial tone or prompts indicating that a user-entered PIN is required.



Note This parameter has no effect on performing Automatic Number Identification (ANI) authentication for H.323 call processing.

The following example illustrates how to disable user-entered PIN collection on a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set vpn-mode = yes
admin> write
VOIP/{ 0 0 } written
```

Enabling sequential calls for PIN authentication

Callers who must enter a PIN to authenticate MultiVoice calls can dial subsequent VoIP calls without reentering their PINs, as long as they do not terminate the connection between the PSTN and near-end MultiVoice Gateway. MultiVoice users need only authenticate once, for the initial VoIP call, to initiate many subsequent calls.

Dialing the next call without authentication is supported for MultiVoice Gateways operating as either multiple logical gateways (`gk-mlg-control = yes`) or as single gateways (`gk-mlg-control = no`).

sequential-call-enable parameter

To enable the sequential-call-enable parameter, set the value to yes, the default. To disable the feature, set the value of the sequential-call-enable parameter to No.

The following procedure illustrates how to set the value of the sequential-call-enable parameter:

```
tnt17>read voip { 0 0 }  
VOIP/{ 0 0 } read  
  
tnt17>set sequential-call-enable = yes  
  
tnt17>write  
VOIP/{ 0 0 } written
```

To disable the sequential call dialing feature, set the value of the sequential-call-enable parameter as illustrated:

```
tnt17>set sequential-call-enable = no  
  
tnt17>write  
VOIP/{ 0 0 } written
```

The new value is applied with the next VoIP call received by the MultiVoice Gateway.

The sequential-call-enable parameter has the following dependencies:

- The TAOS unit must be configured for two-stage dialing and PIN collection (vpn-mode=no).
- If the original call was an operator-assisted call, the caller is automatically disconnected.
- If the original call used single-stage dialing (not prepaid or calling card environment) the caller is automatically disconnected.

Enabling sequential dialing (H.323 caller originated disconnect)

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 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-digits (if the call is a long-distance call) number.



Note While dialing, the digits must be entered within the time limit specified in the call-inter-digit-timeout parameter. If the digits are not entered within the time limit, the user must re-enter 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.

next-call parameter

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.

Dependencies

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 MultiVoice Gateway, 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, re-entering the PIN is not required to dial the next VoIP call, as long as the connection between the PSTN and the near-end MultiVoice Gateway has not been terminated.

Example

The following example illustrates how to enable sequential dialing 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
```

Generating RTP QoS statistics

The RTP Quality of Service (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 a MultiVoice Gateways. RTP QoS information passed onto the Call Logging Server is enhanced in this feature to offer a good perspective of the QoS.

In polling, you can enable the `rtpqos-polling-enable` parameter so the i960 processor requests periodic statistics of the SARMS.


```
[VOIP/{ 0 0 } read]
admin> set rtpqos-polling-enable = yes
admin> write
```

For details on the contents of the QoS information that is collected, refer to “NavisAccess™ support for RTP payload information” on page 6-11 in Chapter 6, “Network Reporting”.

Gatekeeper CLID substitution

When MultiVoice Gateways are connecting VoIP calls, they can transmit a calling line ID (CLID) generated by the MVAM software on the gatekeeper instead of the PSTN-generated CLID collected on the trunk line. CLID substitution allows the MultiVoice network to provide the appropriate E.164 address for both the called and calling telephone numbers to the respective PSTN, and for use by external applications.

In certain configurations in which the gateways connecting the call reside in different area codes or countries, the CLID received from the PSTN must be changed to provide the appropriate calling number information to the local carrier or to call-management and billing applications.

Using a set of user configured translation tables stored on the gatekeeper, the MVAM translates the CLID received from a Gateway into the appropriate dial string, adding or removing country codes and area codes as appropriate for the respective locations of the callers. The gatekeeper then reports the revised CLID to the gateways as part of the admission confirmed (ACF) message.

Details on configuring CLID substitution are found in the *MultiVoice Access Manager User's Guide*.

Configuring two-stage dialing in SS7 networks

To support two-stage dialing in SS7 networks, the TAOS unit must perform iterative DTMF detection and voice announcement payout, prior to the setup of the actual packet or time-division multiplexing (TDM) call.

VoIP call persistence

A TAOS unit provides support for playing voice announcements. For each announcement request, the TAOS unit:

- 1 Sets up a VoIP call route.
- 2 Plays the announcement.
- 3 Tears down the VoIP call route when the announcement is over.

However, to minimize the impact on the shelf controller, *VoIP call persistence* can be configured. VoIP call persistence sets up and maintains a VoIP call route before the actual packet or TDM call is established so that the VoIP call route persists across the VoIP-related IPDC requests (for example, DTMF detection and voice announcements) for a given call.

VoIP call persistence is a Lucent-proprietary extension of IPDC. If the default behavior of the TAOS unit needs to be compliant with standard implementations of

IPDC, VoIP call persistence can be disabled. When VoIP call persistence is disabled, the VoIP call route exists for a single VoIP-related IPDC request.



Note Since VoIP call persistence introduces some nonstandard behavior into the interaction between the TAOS unit and a Lucent Softswitch (discussed below), the existing functionality is maintained for those deployments that do not use this new capability.

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 APX 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.

ss7voip-call-persistence parameter

The `ss7voip-call-persistence` parameter can be configured in the `voip` profile.

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.

Values assigned to the `ss7voip-call-persistence` parameter can be set as follows:

Parameter value	Description
yes	<p>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).</p> <p>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.</p>
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 TAOS unit 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 TAOS unit 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.

Example output from this command is as follows:

```
admin> ss7voip -s
SS7VoIP Session 14532490
=====
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).

Example output from this command is as follows:

```
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

This section describes the IPDC messages and tags that are used to support two-stage dialing in SS7 networks. 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 TAOS unit and describes how Lucent interprets those tags.

Tag	Description
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. 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 TAOS unit sends an ALTN message with Tag 0x35 set to value 0x06 (Operation Started).
0x4A	Apply/Listen or Cancel Tone — Cancel Tone. The TAOS unit 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 TAOS unit 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 TAOS unit, and describes how Lucent interprets those tags.

Tag	Description
0x35	<p>Tone Listen Completion Status.</p> <p>The TAOS unit sends 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>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

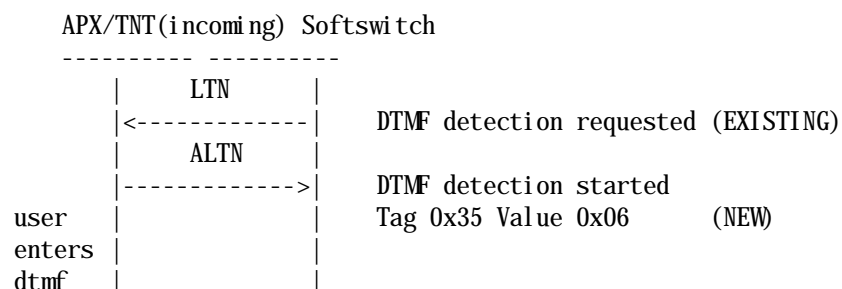
All required tags are included in the ALTN message used as an "Operation Started" acknowledgment to an LTN request. In particular, the ALTN will contain the following tags and values:

- 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 TAOS unit 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.



STN message

The following changes have been made:

Tag	Description
0x86	Announcement Treatment The value 0x00 (Continuous Play) is not currently supported. The maximum value allowed in tag 0x86 remains 0xFF.

ASTN message

The following changes have been made:

Tag	Description
0xFE	Cause Code 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 TAOS unit by this feature.

- In VoIP call-persistence mode and 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 and 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.

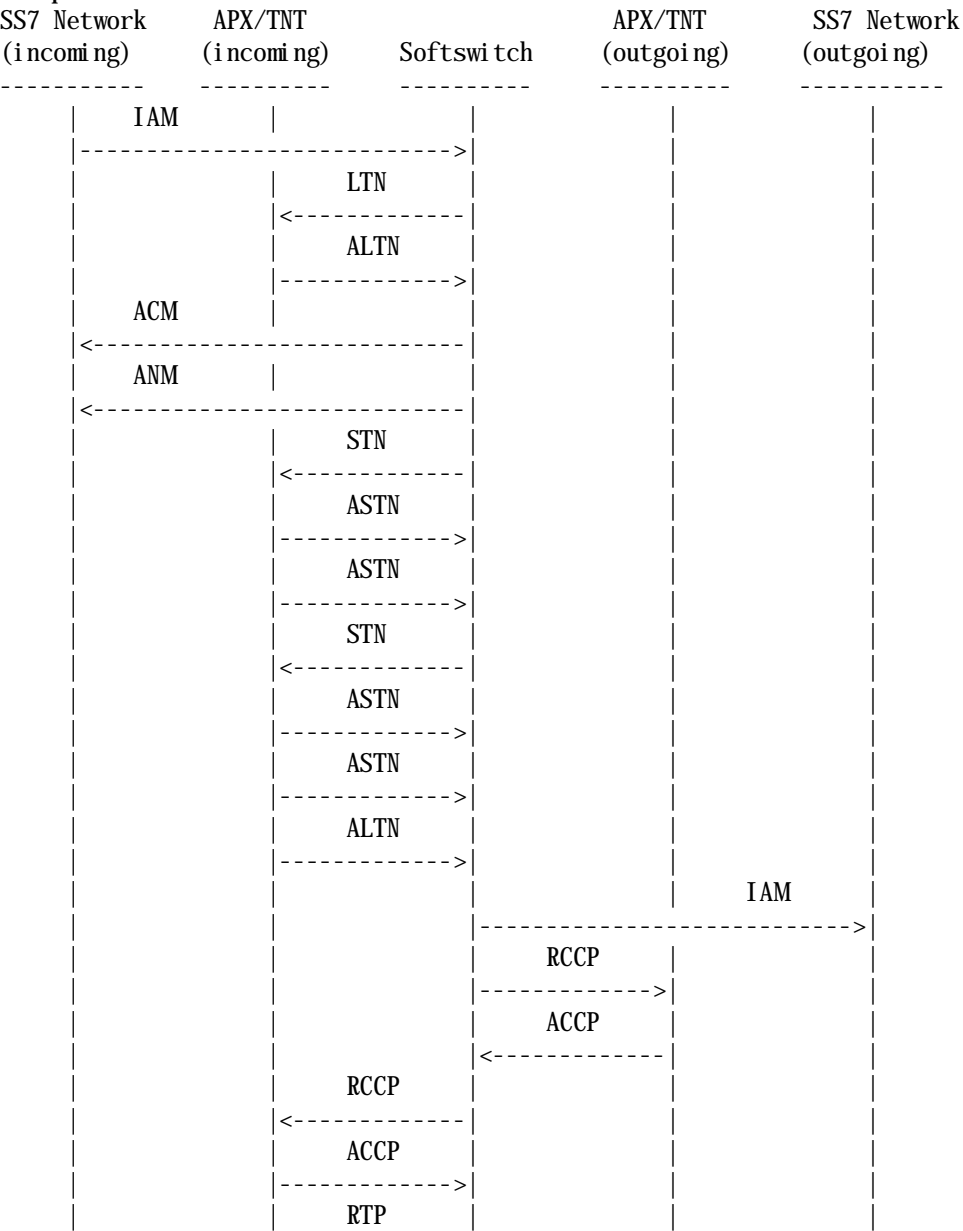
For more information, see the example call flows below.

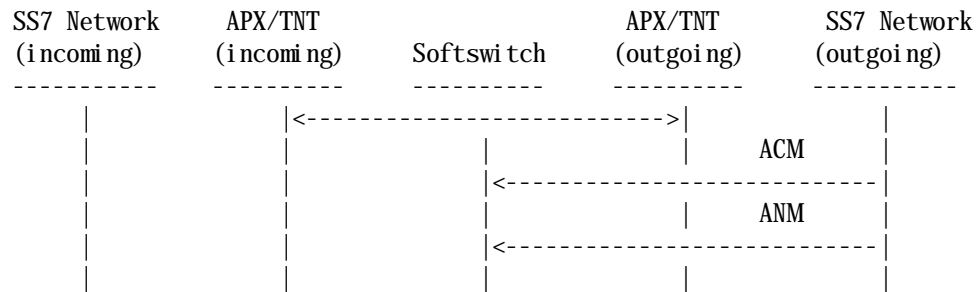
Call flows—VoIP call-persistence mode enabled

When VoIP call-persistence mode is enabled, there are many possible call flows for two-stage dialing. Only a few representative flows are described below.

Successful Two-Stage Packet Call

The following call flow shows the interaction between the TAOS unit 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 MultiVoice Gateway, and ends with the receipt of the last ALTN message by the Softswitch.

The first (and in this example only) LTN instructs the MultiVoice Gateway to enable DTMF VoIP call route setup by the MultiVoice Gateway when the LTN is received. Upon setting up the VoIP call route, the MultiVoice Gateway 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 MultiVoice Gateway sends an ASTN message (“Operation Started”) and plays the announcement. In previous releases, it was 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 your to enter the DNIS. Upon receipt of the second STN, the MultiVoice Gateway sends an ASTN message (“Operation Started”) and plays the announcement. In previous releases, this was done using the VoIP call route that was setup when the first LTN was received.

The fourth ASTN message is sent when the announcement is completed. The MultiVoice Gateway sends the ALTN message when the user has completed DTMF entry of the DNIS. You do 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.

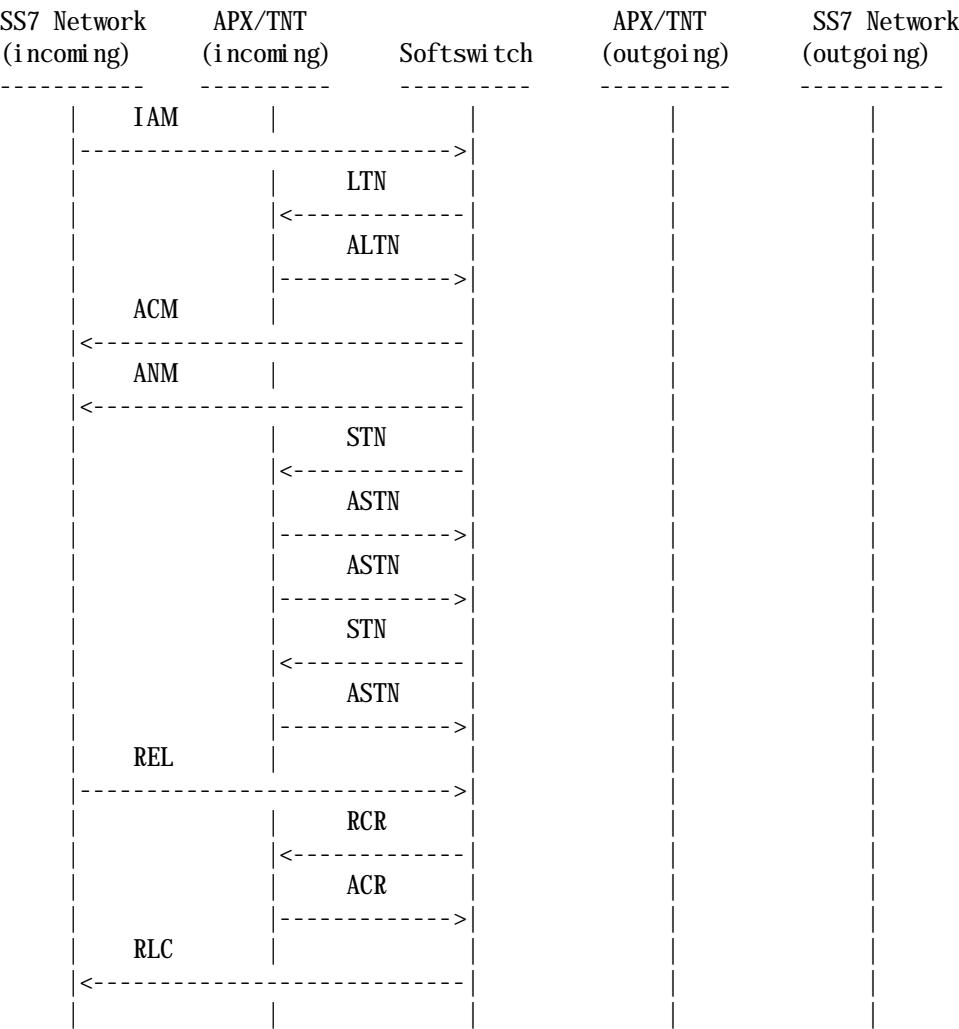
The call then continues in the usual way. When the incoming MultiVoice Gateway receives the RCCP, it sets up its side of the packet call using the VoIP call route that was setup when the first LTN message was received. When the outgoing MultiVoice Gateway receives the RCCP, it sets up a VoIP call route 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

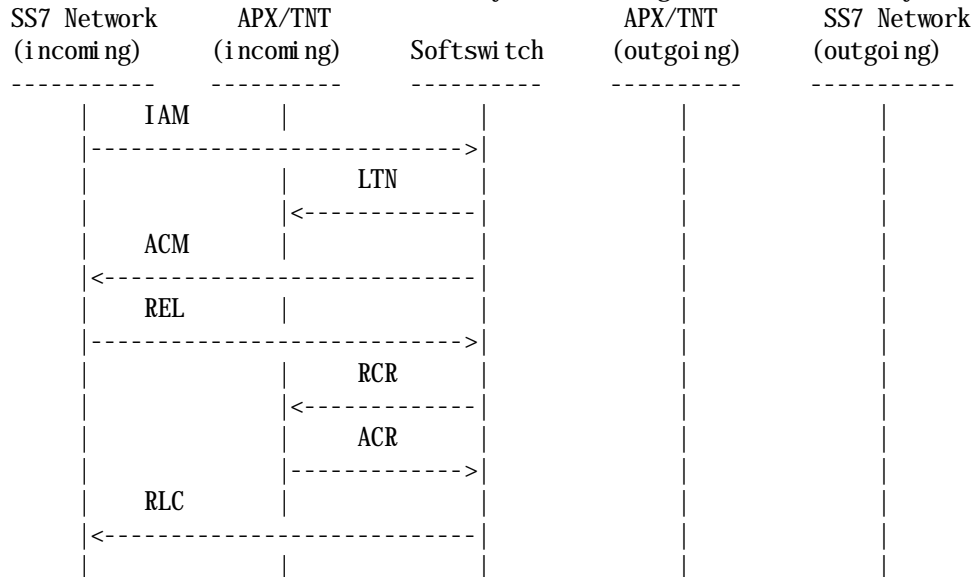
The following call flow shows a two-stage call that is aborted by an incoming call release, after an STN has been received by the incoming MultiVoice Gateway.



The RCR allows the MultiVoice Gateway 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 an incoming call release, after an LTN has been received by the incoming MultiVoice Gateway.

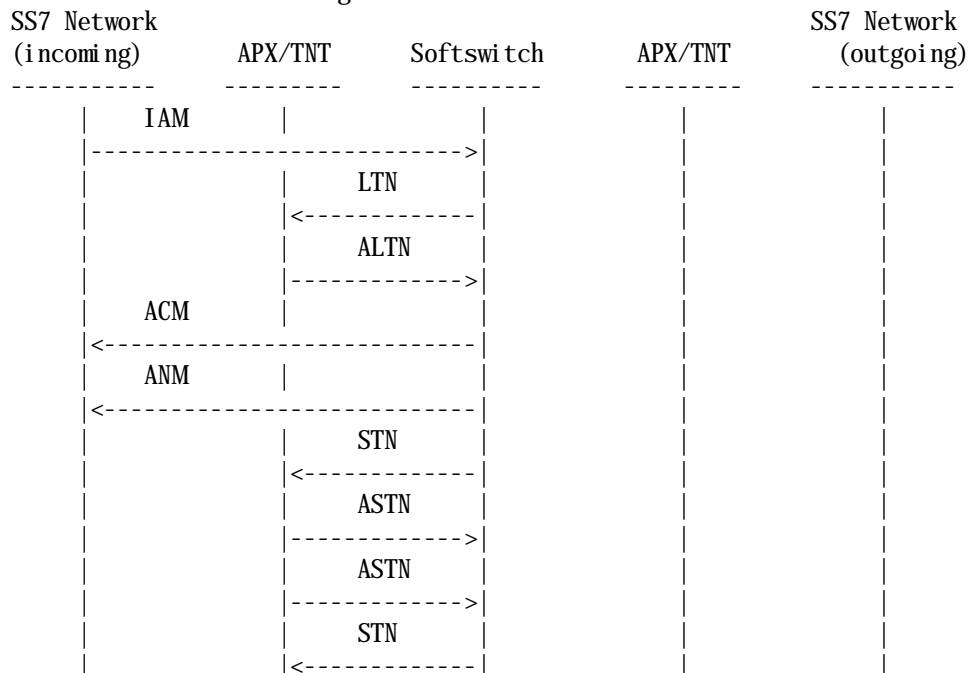


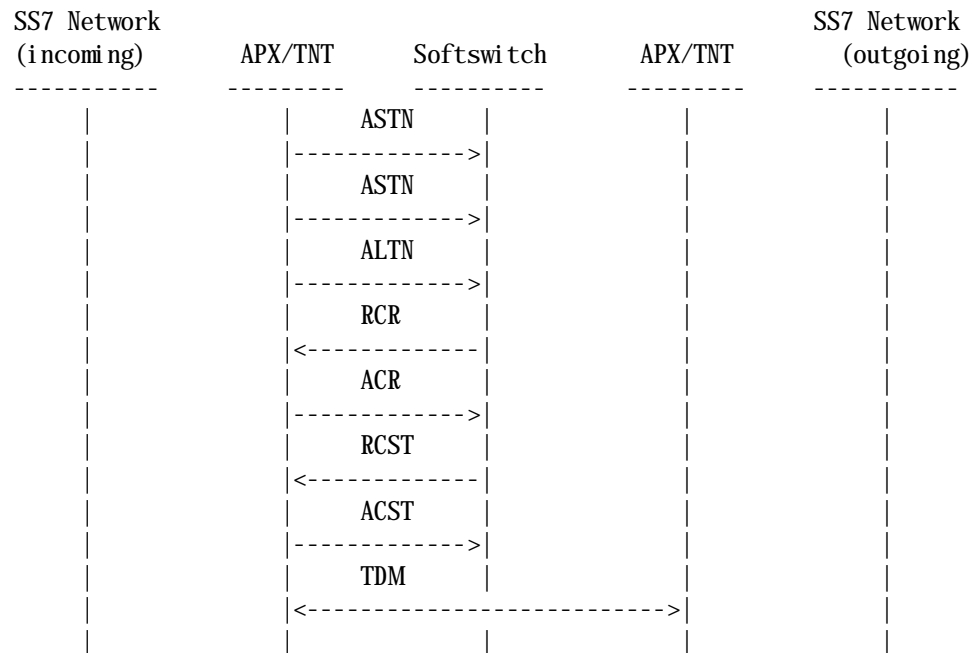
The RCR message allows the MultiVoice Gateway to free the resources (for example, a MultiDSP slot card DSP) associated with the VoIP call route that was set up for the two-stage call when the first LTN message was received.

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 MultiVoice Gateway and the Softswitch for a two-stage TDM call.





The RCR allows the MultiVoice Gateway 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.

Using H.323 authentication

The method of authentication is set from MVAM. The following explains how MVAM provides authentication when MultiVoice Gateways are not partitioned into Multiple Logical Gateways (see “Multiple Logical Gateways” on page 3-44).

MultiVoice supports two methods of user authentication for H.323 VoIP:

- Using a caller-entered personal identification number (PIN).
- Using the Automatic Number Identification (ANI) string of the caller’s telephone.

When PIN authentication is enabled, the call proceeds as follows:

- 1 The TAOS unit presents the caller either with a dial tone or with a prompt indicating that MVAM requires PIN authentication.
- 2 The collected PIN is sent to MVAM as part of the nonStandardData field in the admission request (ARQ) message.
- 3 MVAM validates the PIN against the caller’s user database record.
- 4 If the PIN is valid, call-setup continues.

When ANI authentication is enabled, the call proceeds as follows:

- 1 The TAOS unit collects the ANI information for the caller’s telephone from the PSTN.
- 2 The collected ANI is sent to the Access Manager as part of the nonStandardData field in the admission request (ARQ) message.

- 3 The Access manager Validates the ANI against the caller's user database record.
- 4 If the ANI is valid, call-setup continues. If the ANI is not valid, it checks for a PIN (see Step 1. above for PIN authentication).

One or both methods of authentication may be used by a MultiVoice network. PIN/ANI collection is handled by the TAOS unit.

See "Deactivating trunks used for VoIP calls" on page 3-36 for instructions on configuring PIN collection. See "Configuring trunk signaling for H.323 VoIP networks" on page 2-54 for instructions on configuring ANI collection.



Caution If you elect to use both ANI and PIN authentication, entry of an invalid PIN causes the call to be rejected. If you enter a valid PIN, but the ANI of the calling number does not match the information in the user database, the call is rejected.

Call processing using no authentication

When you do not configure PIN authentication, the TAOS unit processes calls as follows:

- 1 The caller dials the local TAOS unit.
- 2 The local TAOS unit presents a dial tone to the caller.
- 3 The caller enters the destination phone number, followed by the pound sign (#).
- 4 The local TAOS unit initiates a session with MVAM, passing the destination phone number to it.
- 5 MVAM sends the local TAOS unit the IP address of the destination TAOS unit, selected on the basis of configured coverage areas.

If the MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.

- 6 The local TAOS unit initiates a session with the destination TAOS unit.
- 7 The destination TAOS unit initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant gateway.

If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.

- 8 The destination TAOS unit dials the destination phone number, and the connection is complete.

If the caller does not press the pound sign after entering a string of digits, the TAOS unit waits for a timer to expire, then sends the string to MVAM. Initially set to 16 seconds, the timer starts running when the caller enters the first digit, but restarts after each subsequent digit. However, each restart decrements the timer by one seconds, up to a maximum of 14. If the caller enters 15 or more digits, the TAOS unit waits two seconds before sending the string.



Note Unless your T1 or E1 line supports ISDN signaling, callers might not receive some call information, such as busy signals.

Call processing using PIN authentication

If you configure PIN authentication, the MultiVoice Access Manager processes calls as follows:

- 1 The caller dials the local TAOS unit.
- 2 The local TAOS unit presents three quick tones to the caller.
- 3 The caller enters a PIN, followed by the pound sign (#).
If the pound sign is omitted, the TAOS unit sends the user's input after a few seconds.
- 4 The caller enters the destination phone number, followed by the pound sign (#).
- 5 The local TAOS unit initiates a session with the gatekeeper running MVAM and passes the PIN and destination phone number to it.
If the caller enters an incorrect PIN the TAOS unit prompts for a new PIN by sending the caller a single long tone followed by three quick tones. The TAOS unit allows three incorrect PINs before disconnecting the caller.
- 6 If the caller enters a correct PIN, MVAM selects the IP address of the destination TAOS unit, on the basis of configured coverage areas, and sends it to the local TAOS unit.
If MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.
- 7 The local TAOS unit initiates a session with the destination TAOS unit.
- 8 The destination TAOS unit initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant gateway.
If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.
- 9 The destination TAOS unit dials the destination phone number to complete the connection.



Note If you require PIN authentication, you must set the Vpn-Mode to no on all registered MultiVoice Gateways. Otherwise, callers will not be prompted for their PINs, and their calls will fail.

When callers dial into the TAOS unit, it presents them either with a dial tone or with prompts indicating that MVAM requires PIN authentication.

If the caller does not press the pound sign after entering a string of digits, the TAOS unit waits for a timer to expire, then sends the string to the gatekeeper running MVAM. Initially set to 16 seconds, the timer starts running when the caller enters the first digit, but restarts after each subsequent digit. However, each restart decrements the timer by half a second, up to 14.5 seconds. If the caller enters 30 or more digits, the TAOS unit waits two seconds before sending the string.

Call processing using ANI authentication

If you configure ANI authentication, the TAOS unit processes calls as follows:

- 1 The caller dials the local TAOS unit.
- 2 The local TAOS unit presents a dial tone to the caller.

- 3 The caller enters the destination phone number, followed by the pound sign (#).



Note The caller may experience up to 10 seconds of silence after dialing during ANI processing.

- 4 The local TAOS unit collects the ANI for the calling phone number.
- 5 The MultiVoice Gateway initiates a session with the gatekeeper running MVAM and passes the ANI and destination phone number to it.
- 6 MVAM compares the ANI to the User Alias information in the user database.
If the ANI does not match a User Alias, MVAM disconnects the caller.
- 7 If the ANI matches a User Alias, MVAM selects the IP address of the destination TAOS unit, on the basis of configured coverage areas, and sends it to the local TAOS unit.
If MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.
- 8 The local TAOS unit initiates a session with the destination TAOS unit.
- 9 The destination TAOS unit initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant gateway.
If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.
- 10 The destination TAOS unit dials the destination phone number to complete the connection.

The MultiVoice Gateway collects the caller's ANI and forwards it, in the Admissions Request (ARQ) message, along with the destination phone number, to MVAM. If the ANI matches the information in the user database on MVAM, call-setup continues.



Note Since the TAOS unit collects both ANI and DNIS as a single operation, callers may experience a delay of up to 10 seconds for processing before hearing a dial tone, fast-busy, or other call-progress tones.

For information on configuring ANI collection see "Configuring trunk signaling for H.323 VoIP networks" on page 2-54.



Caution ANI authentication does not work across WANs or behind PBXs that do not support delivery of DNIS/ANI.

Voice Announcement Administration

Using voice announcements	4-1
How voice announcements work	4-1
Enabling voice announcements	4-5
Creating voice announcements	4-10

Using voice announcements

A TAOS unit can play user-defined voice announcements rather than playing out tones to indicate call progress. This feature lets service providers use voice announcements:

- In place of traditional PSTN-progress tones
- In place of MultiVoice-specific call-progress tones (for example, PIN prompts)
- For time-out, time-remaining, and call-termination messages for time-measured billing plans.

By default, MultiVoice callers are notified of call progress using DTMF-based tones. These are either generated locally on the TAOS unit or sent across the IP network from the PSTN by way of the distant TAOS unit.

These tones included traditional PSTN call-progress tones, like ringback, busy, etc. which are easily recognized by callers, and MultiVoice-specific call-progress tones, such as PIN prompt, PIN error tone, etc., which are not as easily recognized.

How voice announcements work

When the request to play an announcement is received, by default, the TAOS unit first looks in the /current directory on pc-flash card 1. If this card is not present or the voice announcement file is not found, the TAOS unit then looks at pc-flash card 2.

Announcements are first played back across the cell bus from the shelf router to the MultiDSP slot card. However, subsequent announcement playbacks of the same announcement on the same MultiDSP slot card are done directly from a voice announcement cache on the MultiDSP slot card.

However, only a limited number of announcements can fit in this cache. When an announcement is not contained in the cache, it must be played from the shelf router to the digital signal processor (DSP) slot card across the cell bus. Cache size must be taken into consideration when generating a voice announcement plan and files.

An announcement that is cached is purged from the cache under the following conditions:

- A playback is initiated and the modification timestamp of the file stored in nonvolatile RAM (NVRAM) is newer than that of the cache entry.
- When another announcement is being played, that is not currently in the DSP slot card cache, and there is not enough room to add another announcement to the cache. A last-read use (LRU) policy is used here. In addition, multiple announcements may be paged out of the cache to fit the new announcement.

Voice announcement files originating in the flash file system are cached in the shelf controller memory before being cached on the MultiDSP slot card. TAOS units can respond for requests sent to the shelf controller for voice announcement playout, when the requested voice announcement is not cached on the MultiDSP slot card.

By default, TAOS attempts to respond to a request for voice announcement playout by checking the memory cache on the MultiDSP slot card first, then attempt to retrieve that voice announcement from the cache on the shelf controller, before attempting to retrieve that voice announcement from the external flash file system. This was implemented without changing the TAOS command line interface.

Voice announcements for time-measure billing plans

For providers offering time-measured or prepaid calling plans, MultiVoice supports playing voice announcements during the call, on request from MVAM, to warn callers when their credit is low or they have limited time left on a call, and to explain why a call has been terminated. The capability to play out messages on request allows a TAOS unit to respond to drop request messages or information request messages containing instructions to play out an announcement.

The announcement request can specify a user-defined announcement file, or use the default announcement file `h323drq.au`. In this case, announcement selection is controlled by using the MultiVoice API, to specify announcement files in messages from MVAM or a third-party billing application for H.323 call processing.

Multiple voice announcements

MultiVoice Gateways can play break-in announcements and queue messages in response to caller-entered DTMF signals. This expanded capability enhances the use of third-party billing and prepaid billing applications and support queuing call services.

A MultiVoice Gateway can play out multiple voice announcements, in response to an Information Request (IRQ) sent from the MultiVoice Access Manager, in response to either

- User-entered DTMF tones
- A time out/time delay interval

Callers can be presented with voice menus and prompts that respond to caller input using DTMF tone collection. When the message request/reporting fields in the `nonStandardData` byte of the Information Request (IRQ) messages exchanged between MultiVoice Gateways and the MVAM. Customers have a mechanism for providing automated attendant functions on their MultiVoice networks, and provide call services in response to DTMF entries.

Requests to play specific messages to callers are initiated from MVAM, or in response to caller entered digits. Message initiation is tied to call progress or user entered DTMF sent by the MultiVoice Gateway to MVAM. Message selection by MVAM is controlled through the MultiVoice API.

When processing voice announcement play out requests from MVAM, the MultiVoice Gateway does the following:

- Acknowledges receipt of the IRQ containing the play out request
- Acknowledges play out of the message
- When collecting caller entered DTMF, if appropriate, plays out messages in response to DTMF entries
- When collecting caller entered DTMF, if appropriate, plays out messages after a predefined time out/time interval expires when no DTMF entries are collected
- Reports collected DTMF strings to the MVAM for further processing by third-party billing, prepaid billing, or other applications utilizing the MultiVoice API to perform call administration

When requesting voice announcement play out from the MultiVoice Gateway, MVAM does the following:

- Acknowledges receipt of Information Request Response (IRR) containing the voice announcement play out results, including collected DTMF strings
- Reports collected DTMF strings to any third-party billing, prepaid billing or other applications utilizing the MultiVoice API to perform call administration
- Sends the next play message, when appropriate, in response to results reported in an IRR
- Sends requests to break in with new announcements, even when a previously requested announcement is still playing.

Audio file requirements

All voice announcements are stored on the flash memory card in the PCMCIA slot. By default, messages reside in the /current directory, unless the user has specified a different directory. The voice announcements must be standard .au (NeXT/Sun) format audio files with the following additional attributes:

Attribute	Value
Sampling rate	8000 bps
Data format	G.711 μ -law, G.729
Channel count	1
Info string	Less than 40 bytes long.
Maximum file size	200Kbytes. (This means the largest announcement can be 20 seconds in duration.)



Note The announcement file's format and contents are only checked at playback time, not upon card insertion or file write.

Voice announcement guidelines

The following lists some guidelines for voice announcements:

Table 4-1. Guidelines for voice announcements

Guideline	Specification
Maximum size of an announcement file	The maximum size can be no larger than 200Kbytes.
Total storage capacity allocated for voice announcements	The total space for voice announcements cannot exceed 8Mbytes. This capacity permits up to four brand or language announcement file sets with 2Mbytes of data per set.
Total talk time for voice announcements	The total talk time is dependent on the data encoding used for the announcement files. If G.711 is used, then the 8Mbytes total data limit translates into a total talk time of about fourteen minutes. Using G.729 encoding permits a total talk time of nearly two hours from 8Mbytes of data.

Voice announcement file names

If voice announcements are enabled, MultiVoice requests the following announcements, by name, for play out for the corresponding H.323 call state:

Table 4-2. File names for voice announcements (Page 1 of 2)

Call state	Announcement purpose	Announcement filename
PIN prompt	Lets callers know they must enter a PIN	h323pi n. au
PIN/DNIS error	When vpn-mode=nNo, lets callers know that the PIN/DNIS is invalid	h323per. au
DNIS entry	Lets callers know they need to enter the destination telephone number. This is supported when single-dial-enable=no	h323dns. au

Table 4-2. File names for voice announcements (Page 2 of 2)

Call state	Announcement purpose	Announcement filename
Gateway not available	Used when a destination gateway is not able to accept the call at the present time. This is currently used for: <ul style="list-style-type: none">• A gateway is not registered with the gatekeeper.• A gateway can not handle current call load/rate.	h323ngw. au
Call failure	Default call failure prompt.	h323f. au
Call drop request (gatekeeper initiated)	The gatekeeper sent a request to drop an active call (DRQ) to the gateway. This is used in conjunction with debt-account billing systems.	h323drq. au

Enabling voice announcements

The TAOS unit supports play out of voice announcements for both IPDC and H.323 VoIP calls. Announcements are enabled by

- Specifying announcement files in STN messages from the SS7 signaling gateway for IPDC
- Enabling the use of voice announcements from within the voi p { 0 0 } profile for H.323 call operations



Note By default, both IPDC and H.323 VoIP voice announcement file names are the same. The IPDC STN messages from the SS7 signaling gateway must call voice announcements using file names stored on the TAOS unit .

Enabling voice announcements for IPDC calls

For IPDC VoIP, voice announcements are requested by the SS7 signaling gateway. A request to play an announcement is passed to the TAOS unit, in IPDC format. From the IPDC specification (*Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15*), announcements are specified as Send Tones or Announcement (STN) messages with the following tags:

- Tone Type (0x49) (now supports a value of “0x03 - Voice Announcement”)
- Announcement Treatment (0x86) (number of times to play the announcement)
- Tone String (0x33) (the file name or identifier of the announcement to be played)

Call-progress tone parameters set in the voi p profiles have no affect on IPDC announcement playbacks.



Note This feature requires obtaining a pre-paid billing application.

STN Message

Voice announcement playlists allow a list of announcement files to be signaled to the MultiVoice Gateway in the STN message. The following describes how tags in the STN message support voice announcements.

Tag 0x33 (Tone String)

This tag accepts 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 a playlist format is used, this value is ignored.

An example of where Tag 0x86 is equivalent to 2 is:

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 in IPDC

You can configure 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.

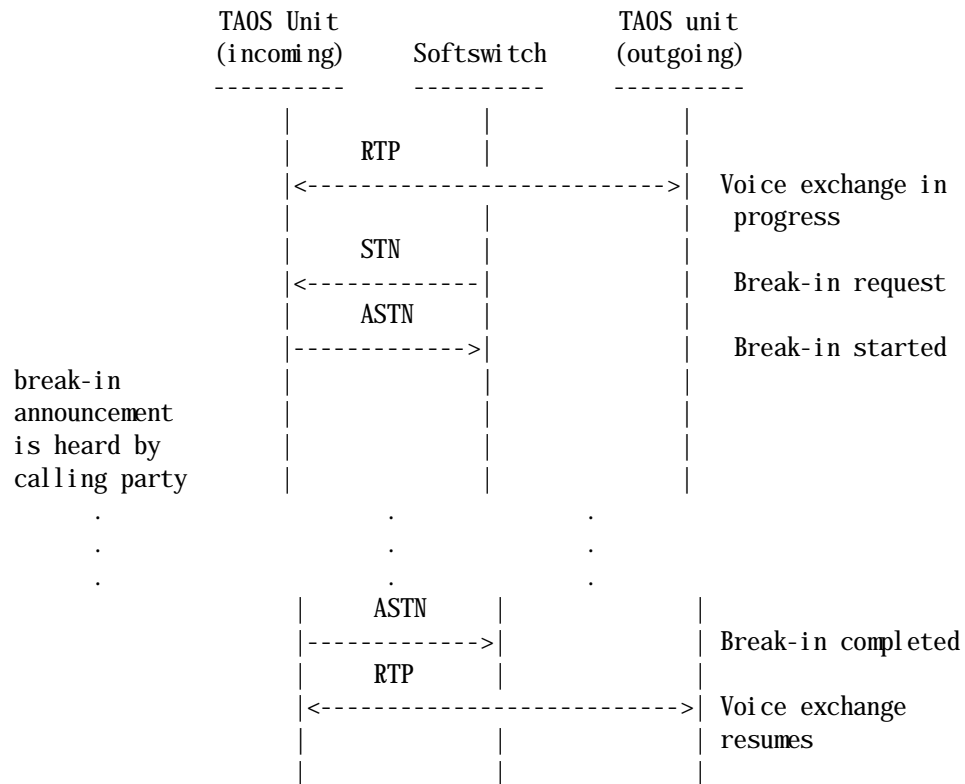
Typically, a break-in announcement is played to the calling party, however it could be played to the called party or both parties.



Note Break-in voice announcements are supported for packet calls, but not for time-division multiplexing (TDM) calls.

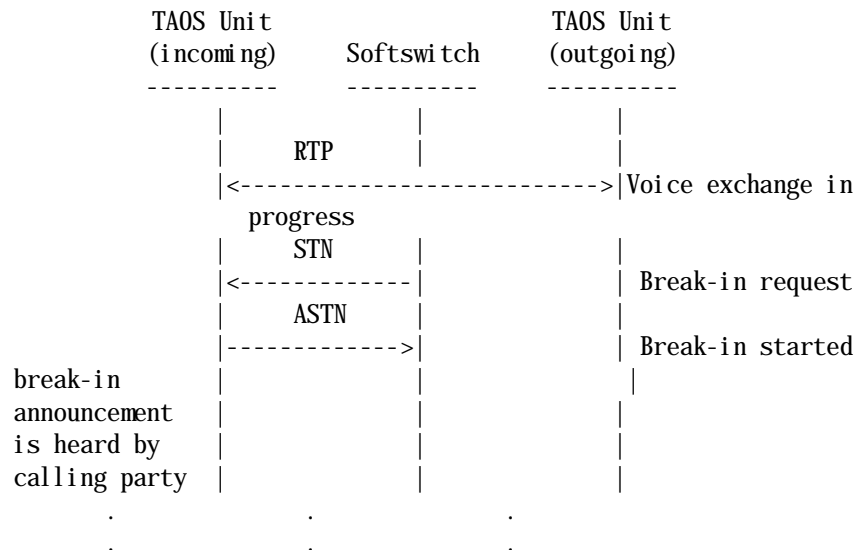
STN/ATN message call flow

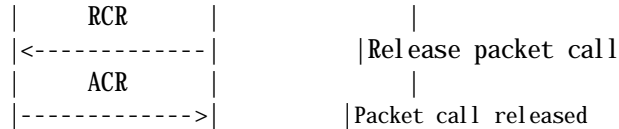
Break-in voice announcements utilize existing STN/ASTN messaging as follows, fully supporting the cancel operation. Refer to *Level 3 Communications, Internet Protocol Device Control (IPDC), Revision 0.15* for a description of messages (for example, RTP, STN, etc.).



Break-in announcement 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:





Enabling voice announcements for H.323 calls

Three parameters located in the voip { 0 0 } profile are used to enable MultiVoice voice announcements for H.323 call processing:

Parameter	Specifies
h323-voice-ann-enabled	<p>Enable voice announcement play out. Setting the parameter to yes enables voice announcement play out; No disables this feature. The default value for this parameter is no. Changes to this parameter are effective with the next VoIP call.</p> <p>Even when voice announcements are enabled, users still hear call-progress tones under the following conditions:</p> <ul style="list-style-type: none"> • A traditional call progress tone is available (ringback, busy, etc.). • The gateway cannot play any more simultaneous announcements.
voice-ann-dir	<p>The directory location where the voice announcement files are stored on the TAOS unit. This value defaults to the /current directory on pc-flash card 1. Changes to this parameter are effective with the next VoIP call.</p> <p>Enter the file path to the directory location containing the H.323 VoIP voice announcement files. This may be a string of 40 characters or less beginning with "/". This parameter defaults to N/A when h323-voice-ann-enabled = no. Changes to this parameter are effective with the next VoIP call.</p>
voice-ann-enc	<p>Either the G.711 μ-law or G.729 encoding of voice announcements that are played out by a MultiVoice Gateway. Voice announcements are used for reporting call progress to callers.</p>

These parameters have no effect on SS7-IPDC voice announcement play out.

To enable voice announcements for H.323 call operations on a TAOS unit:

- 1 Open the voip { 0 0 } profile.

```
admin> read voip { 0 0 }
VOIP/{0 0} read
```
- 2 Turn on voice announcement play out by setting the h323-voice-ann-enabled parameter to yes. For example:


```
admin> list h323-voice-ann-enabled
[in VOIP/{ 0 0 }:h323-voice-ann-enabled]
h323-voice-ann-enabled = no

admin> set h323-voice-ann-enabled = yes
```

3 Write your changes to the voip { 0 0 } profile.

```
admin> write voip { 0 0 }
VOIP/{0 0} written
```

Enabling G.711 μ -Law or G.729 encoding

Either G.729 or G.711 encoded speech for voice announcement play out can be used on MultiVoice Gateways. You configure the choice through the TAOS administration interface. Audio encoded in G.729 format is eight times smaller than the audio encoded in G.711, which allows customers to store and play a larger number of voice announcements.



Note While, G.711 encoded voice announcements files can be created with standard off-the-shelf software, a special tool is need to create G.729 encoded voice announcements that the MultiVoice Gateway will recognize and be able to play. This tool is available free to customers from the Lucent Technologies FTP download site. Customers requiring this tool should contact their account representative for details.

You configure the voice-ann-enc parameter to the voip profile on the MultiVoice Gateway as illustrated in the following example:

```
[in VOIP/{ 0 0 }]
voip-index* = { 0 0 }
gatekeeper-ip = 135. 92. 52. 138
gk-mlg-control = no
.....
voice-ann-enc = g711-ulaw
.....
```

The voice-ann-enc parameter specifies either the G.711 μ -law or G.729 encoding of voice announcements that are played out by a MultiVoice Gateway. Voice announcements report call progress to callers. Changes to the voice-ann-enc parameter are effective with the next VoIP call.

The following example illustrates how to configure a MultiVoice Gateway to use G.729 encoding for voice announcement play out.

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read

admin> set voice-ann-enc=g729

admin> write
```

The voice-ann-enc parameter has the following dependencies:

- The MultiVoice Gateway must be configured for using voice announcements to report call progress.
- Before a MultiVoice Gateway is configured to use G.729 voice-announcement encoding (voice-ann-enc=g729), voice announcement files must be converted to the G.729 compatible format. Lucent Technologies offers a tool, at no charge to MultiVoice Customers, that creates G.729 encoded voice announcement files.

- The MultiVoice Gateway must be configured to use G.729 voice-announcement encoding (voice-ann-enc=g729) when the Lucent Technologies prepaid billing message set is used for reporting call progress and for billing announcements.

Creating voice announcements

To create or edit a voice announcement, proceed as follows:

- 1 **Using your favorite midi or audio editor on your PC, open the file containing the voice announcement.**
- 2 **Create or edit the contents of the message. Then save your work.**
- 3 **Change the recorded file to an .au formatted file.**
- 4 **Move the file to a TFTP server download directory (for example, C:\Users\default).**
- 5 **From the TAOS unit, enter the CLI Load command using the load type file, as in the following example:**

```
load file network xxx.xxx.xxx.xxx filename.au
```

where xxx.xxx.xxx.xxx is the IP address of the TFTP server. By default, this command writes to the destination directory /current on flashcard 1.

Once the file is loaded on the flash card, the message is available for playback.

To make use of voice announcements, the flash card must use the FAT 12 format. Use the CLI Format command to apply the FAT format to the flash card.

The following dependencies apply when planning and creating voice announcements:

- Voice announcement files must always be in .au format. There are easily accessible tools available to convert from the standard Windows .wav format to an .au format file, including
 - CoolEdit (<http://www.syntrillium.com/cooledit/index.html>)
 - GoldWave32 (<http://www.goldwave.com>)
- The number of announcements that can be stored on a TAOS unit is limited only by the available space on the flash card, which has a capacity of 32Mb for the APX or 8Mb for the MAX TNT. However, having many different announcements might impact performance and sound quality during playback because the cache size is limited.

Formatting flash cards

Before using a PCMCIA card for loading voice announcement files, you must format it using a FAT format. The Format command creates this DOS-compatible flat file system by default on PCMCIA flash cards.

After inserting a flash card into slot 1 in the Shelf-controller, enter the Format command, as in the following example:

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

or

```
admin> format 1
```

Before loading any tar images or message files, use the fsck command to verify the format, as in the following example:

```
admin> fsck
Volume Stats:
    Block Size: 512 (typical: 512)
    Blocks Per Cluster: 3 (typical: 1, may be powers of 2 up to 16)
    Reserved Blocks: 1 (typical: 1, but may be 0 - hundreds)
    Number of FATs: 2 (must be 2)
    Number of Root Directory Entries: 96 (typically between 32 and 224)
    Total Blocks: 11264
    Media Descriptor: f0 (ignored)
Volume Info calculated from values above:
    Blocks Per Fat: 11
    Fat Start Block: 1
    Root Dir Start Block: 23
    Data Start Block: 29
    Number of Root Dir Blocks: 6
    Number of Clusters: 3745
    FAT Type: Fat12
Cluster Usage
    Usable Clusters: 3743
    Free Clusters: 1828
    Clusters lost during interrupted writes: 0
    Other reserved clusters: 1909
admin>
```

For new format cards, fsck prints a summary of the file structure on the card (parenthetical text is not part of the output of this command).

Creating the voice announcements directory

You can create up to four directories on the external flash memory card for customized voice announcements. These voice announcements can be used to report call progress or for playback on command from MVAM, Softswitch, or a third-party billing application.

After creating any directory on a flash card and moving voice announcement files into it, specify the location by entering a pathname in the voice-ann-dir setting. For example, the following commands create a directory named messages and a subdirectory named announce on the flash card in slot 1:

```
admin> mkdir 1/messages
admin> mkdir 1/messages/announce
```

The following command loads a voice-announcement file named busy.au from a TFTP server at 10.10.10.10 to the /current directory on flash card 1 (flash card 1 is the default):

```
admin> load file network 10.10.10.10 busy.au
```

The following command moves the busy.au file to the new subdirectory on flash card 1:

```
admin> mv 1/current/busy.au 1/messages/announce/busy.au
```

The following commands inform the MultiVoice subsystem of the location of the voice announcement files:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set voice-ann-dir = /messages/announce
```

```
admin> write
VOIP/{ 0 0 } written
```

You can specify a pathname up to 40 characters long. When the system receives a request to play an announcement, it looks in the specified directory on the flash card in slot 1. If the card is not present or the voice announcement file is not found, the system looks for the specified directory on flash card 2.

Displaying voice announcement files

The voice announcement files are displayed by name with all the other code images and tarballs stored on the flash card, when you enter the `dircode` command. For example:

```
admin> dircode
Flash card code directory:
Card 1, format FTL/FAT, capacity 8MB
/current:
shelf-controller1231877Tue Oct 27 17:17:22 1998 7.1.0
8t1-card209191Tue Oct 27 17:17:42 1998 7.1.0
4ether-card180385Tue Oct 27 17:17:56 1998 7.1.0
hdlc-card588610Tue Oct 27 17:18:38 1998 7.1.0
48modem-56k-card724319Tue Oct 27 17:19:58 1998 7.1.0
hold.au72723Thu Jan 21 19:54:12 1999
admin>
```

The `dircode` command output includes the type and capacity of each card inserted. For an old-format card, the output is unchanged from previous versions. For FAT-format cards, the output is slightly different, since information about each image is stored differently.

Voice announcement log messages

Several log messages are generated to alert the user of invalid voice announcement files. These include the following:

Table 4-3. Error/log messages (Page 1 of 2)

Message	Cause
LOG error, Shelf 1, Controller, Time: 19:06:23-- Announcement File /current/test.au not found	Appears when the TAOS unit cannot find the requested announcement.
LOG error, Shelf 1, Controller, Time: 20:32:07-- Invalid voice announcement format for drip.au	Appears when the voice announcement file does use a valid .au format file

Table 4-3. Error/log messages (Page 2 of 2)

Message	Cause
LOG error, Shelf 1, Controller, Time: 15:00:11-- Au File vopc4.a not supported, format 27, samplingRate 44100, channelCount 2	Appears when the voice announcement file uses a valid .au format file but does not meet the attributes for sampling rate, data format, channel count, string length, or file size.
LOG error, Shelf 1, Controller, Time: 15:00:11-- Announcement file too large. Max size = 102400	Appears when the voice announcement audio size is larger than 200K.

WARNING messages

Table 4-4. Warning messages

Message	Cause
LOG error, Shelf 1, Controller, Time: 15:00:20-- Voice Announcement info string in header is too big.	Appears when the information string of the .au file header is larger than can be handled. This is not harmful. Announcement playback still succeeds.

MultiVoice Real-time Fax

5

Real-time fax processing	5-1
Real-time fax configuration	5-2
Fax session detection	5-13

Real-time fax processing

Real-time fax calls begin when a VoIP call is placed from an originating fax machine to the answering machine. If the TAOS unit is configured to perform out-of-band dual tone multi-frequency (DTMF) signaling, a DSP automatically enables inband DTMF signaling at the start of the fax call. When the destination fax machine picks up the call and sends an answer tone, known as a CED tone, the destination Gateway detects this tone and initiates a switchover to real-time fax on both itself and the Gateway at the other end of the call. When the switchover is complete, the fax transmission proceeds normally.

The switch over from voice session to fax can occur at any point in a call. For example, the call can start as a normal VoIP call where two participants converse for any length of time before initiating a fax. Once the switch to fax is made, however, there is no switching back; i.e. once in fax mode, the fax is sent and then the call will be terminated.

You must create the appropriate coverage areas on the MultiVoice Access Manager to ensure that fax calls are routed between Gateways that are fax capable. For details, see the *MultiVoice Access Manager User's Guide*.



Note For MultiVoice to complete a fax call, both the Gateways involved in the call must have real-time fax enabled.

H.323 Annex D T.38 fax support

Support for real-time facsimile (FAX) interoperability with other vendors H.323 gateways is made possible 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.

MultiVoice gateways automatically detect other gateways of a call that are not MultiVoice gateways. Subsequently, if fax tones are detected, this system uses 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.

Real-time fax configuration

MultiVoice real-time fax is an implementation of the ITU-T T.38 standard for fax transmission across IP networks, using the VoIP framework for call establishment, fax initiation, and detection of an incoming fax call.



Note Real-time fax communications require guaranteed quality of service between the two fax-capable gateways. The packet loss on the network must be less than 1%.

To use MultiVoice real-time fax:

- The network must use TAOS units.
- The TAOS units must be licensed to provide support for the real-time fax feature.

Configure the TAOS unit to process real time fax calls by enabling fax mode through the voip {0 0} profile. By default, all calls begin as voice calls. Upon detection of a fax tone, the call type switches to fax mode.

Base profiles

For MultiVoice real-time fax to be available, the TAOS unit must be licensed to support both real-time fax and VoIP call processing. The base profile must include the following parameters:

Table 5-1. Base profile parameters

Parameter	Description
voip-enabled	Enables/disables VoIP call processing. When this parameter is set to yes, the TAOS unit has been hashed to process VoIP calls.
rtfax-enabled	Enables/disables real-time fax processing on a TAOS unit for H.323 call operations. When this parameter is set to yes, the TAOS unit has been licensed to process faxes for H.323 calls.

Rt-fax-options sub-profile

Following are the rt-fax-options sub-profile parameters (shown with default values) for enabling and improving the performance of real-time fax processing. Changes to these parameters take effect with the next VoIP call.

```
[in VOIP/{ 0 0 }:rt-fax-options]
```

```
rt-fax-enable = no
```



```
ecm-enable = yes
low-latency-mode = yes
command-spoof = yes
local-retransmit-lsf = yes
packet-redundancy = 0
fixed_packets = no
max-data-rate = 14400
```

Parameter	Setting
rt-fax-enable	Enable/disable real-time fax call processing. When the parameter is set to no (the default), fax tones are passed as if they were normal voice samples, and the other parameters in the sub-profile are not applicable. When the parameter value is set to yes, the TAOS unit switches over from voice session to fax upon detection of a CED tone or V.21 HDLC flag.
ecm-enable	Enable/disable error correction mode (ECM) for real-time fax calls. When the parameter is set to yes (the default), fax frames can be retransmitted in the event that a frame is not received correctly. ECM frames are relayed end to end between terminals. Setting the parameter to no disables ECM, so fax frames containing errors are not corrected.
low-latency-mode	Enable/disable low latency mode for real-time fax operations over networks with low packet loss and low latency characteristics. Low latency mode allows operation on networks with less than 2.5 seconds or less of aggregate latency between pages. When the parameter is set to no, a minimum of 10 seconds delay is added to processing fax calls to allow interpretation of T.30 frames and implement spoofing.
command-spoof	Enable/disable spoofing of certain fax commands. Command spoofing is a method of improving performance and reducing fax errors on low latency networks.
local-retransmit-lsf	Enable/disable local retransmission of a low speed fax frame if no response is detected from the destination fax. This is designed to reduce fax transmission errors on low packet loss networks.
packet-redundancy	Improves reliability of MultiVoice real-time fax transmissions. Packet redundancy is recommended when transmissions are sent over unmanaged networks (such as the public Internet) or networks experiencing measurable packet loss. Assign a value between 0 and 5 to append that number of previously sent packets onto the current packet. Values larger than 2 should be assigned for networks experiencing packet loss greater than one percent.
fixed-packets	Enable/disable the addition of <i>n</i> -length payload pairs at the end of the packet when packet-redundancy is enabled, where <i>n</i> is the value of the packet-redundancy parameter.

Parameter	Setting
max-data-rate	Assigns a maximum rate in bits per second (bps) to the real-time fax transmission. Assign either 2400, 4800, 9600, or 14400.

In an SS7 environment, values in IPDC messages override corresponding call management settings in the default Voip profile. For information about IPDC support for real-time fax, see “IPDC message support for real-time fax and transparent modem” on page 5-8.

The following example shows the commands that enable T.38 fax call processing and leave all performance parameters enabled:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set rt-fax-options rt-fax-enable = yes  
admin> write  
VOIP/{ 0 0 } written
```

Routing fax calls

Once real-time fax is enabled on a TAOS unit, the MultiVoice administrator needs to create the appropriate coverage areas on the MVAM to ensure that fax calls are routed between gateways that are fax capable.

Both the originating and connecting Gateway must be capable of detecting the CED tone or the V.21 HDLC flag, and acknowledging (respond with the proper ACK signal) for fax transmission to succeed. Only MultiVoice Gateways that have been loaded with the proper licensed software code and have the real-time fax feature enabled have this capability.

To ensure proper routing and processing of fax calls, the MultiVoice administrator can do the following:

- Enable real-time fax on all gateways. This ensures that any fax call which comes in can be connected regardless of routing. This requires that all gateways used by that network are TAOS units.
- Enable real-time fax on selected gateways, and assign them to a virtual zone managed by MVAM. This solution uses a feature available from the MultiVoice Access Manager which allows it to administer the fax gateways as if they were part of a separate H.323 zone. Access numbers for these gateways could be reserved for fax calls only. Calls initiated and completed within the virtual zone would always be between fax capable gateways. Voice calls could still be initiated and completed both within that virtual zone and across any other zones administered by MVAM. This reduces the number of TAOS units necessary to support network fax operations.

Using error correction mode (ECM)

The `ecm-enable` parameter enables/disables error correction mode (ECM) for real-time fax calls. Change the setting from its default value to no, when performing real-time fax processing on MultiVoice networks with low packet loss and low latency characteristics.

When this parameter is set to yes (the default), fax frames are retransmitted whenever a frame is not received correctly. ECM frames are relayed end to end between terminals. For certain network environments, using the default value for the `ecm-enable` parameter might result in the following:

- Fax transmission delays
- Diminishment fax call performance
- Disconnection of fax calls in progress
- Fax calls time out without ever connecting

Enabling packet redundancy

A packet redundancy scheme and jitter buffer improve the performance of MultiVoice real-time fax over unmanaged networks (such as the public Internet). Packet redundancy allows the MultiVoice Gateway to process several hundred milliseconds of packet jitter and allows the optional transmission of redundant packet data for fax calls across networks experiencing instances of packet loss and packet jitter.

To support this feature, MultiVoice requires real-time fax to be enabled on the MultiVoice Gateway. This may be verified by checking the base profile for the `rt-fax-enabled=yes` entry.

Packet redundancy parameter

Redundant packet data is defined as the last n packets transmitted appended to the current packet. The value of n is set through the CLI using the `packet-redundancy` parameter in the `rt-fax-options` sub-profile of the `voip` profile.

Assigning the `packet-redundancy` parameter a value (such as `packet-redundancy = 4`), causes the TAOS unit to append the specified number of previously sent packets onto the current packet. On networks experiencing measurable packet loss, this improves the reliability of the fax transmission.

Depending upon the amount of measurable packet loss for a network, the redundancy parameter should be set accordingly:

Network condition	Recommended value(s)
Packet loss occurs in frequent bursts.	1 through 5
Occasional packet loss (less than one percent)	0 (default)
Occasional packet loss (greater than one percent)	1 or 2

The additional bandwidth required for each fax call increases proportionally to the level of redundancy, adding 50 bytes of packet data per increment.

Packet redundancy uses a slip buffer to

- Allow MultiVoice real-time fax to tolerate packet jitter
- Keep the modem fed with data, preventing modem underrun

Fixed-size packet format

The packet redundancy scheme uses a fixed-size packet format, consisting of a 49-byte payload, a prefixed sequence number, and a length field that precedes the payload data. When packet redundancy is enabled, n -length payload pairs are added at the end of the packet; where n is the value of the packet-redundancy parameter.

Previously, the TAOS unit sent variable length packets that were guaranteed to be zero terminated; allowing Class 1 modems to underrun gracefully.

The packet-redundancy parameter causes the TAOS unit to append the designated number of previously sent fax packets onto the current packet. On networks experiencing measurable packet loss, this improves the reliability of the fax transmission.

This parameter accepts values from 0 through 5, directing MultiVoice to append the designated number of previously transmitted fax packets to the current packet, as follows:

Parameter value	Specifies
0	No change from the default packet behavior.
1	Append and send the previous fax packet with the current fax packet.
2	Append and send the two previous fax packets with the current fax packet.
3	Append and send the three previous fax packets with the current fax packet.
4	Append and send the four previous fax packets with the current fax packet.
5	Append and send the five previous fax packets with the current fax packet.

The following example illustrates how to change the default value of the packet-redundancy parameter.

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
admin> set packet-redundancy=4  
admin> write  
VOIP/{ 0 0 } written
```

The following dependencies apply to this parameter:

- Once saved, packet redundancy is enabled with the next VoIP call
- This value is set to N/A when fixed-packets=no.

Disabling Packet Redundancy

The fixed-packets parameter enables MultiVoice Gateways running TAOS 9.0 to process real-time fax calls to and from MultiVoice Gateways running earlier TAOS versions. The new packet sequence numbering introduced in TAOS 10.0 for real-time

fax required a format change, creating high speed data packets. When these packets are absent (for example, a fax call is initiated from a MultiVoice Gateway running a pre-TAOS 10.0) MultiVoice Gateway interprets image data as sequence data. Also the smaller packets forwarded by the new code rely on the slip buffer to keep the modem fed with data or it drops the carrier.

The `fixed-packets` parameter disables use of redundant packets and the slip buffer, enabling the gateway to use pre-TAO 10.0 fax packet scheme.

When enabled, fax calls are processed using variable length packets that are zero terminated; allowing Class 1 modems to underrun gracefully.

When the value of this parameter is yes, the default, the pre-TAOS 10.0 fax packet scheme is enabled. When the value of this parameter is no, jitter buffering and packet redundancy for real-time fax processing is disabled. Once saved, the selected packet scheme is enabled with the next fax call.

The following example illustrates how to disable jitter buffering and packet redundancy on a TAOS unit:

```
admin> read voip { 0 0}
VOIP/{ 0 0} read
admin> set fixed-packets=no
admin> write
VOIP/{ 0 0 } written
```

The following dependency applies to this parameter:

- When this value is set to yes, then `packet-redundancy=n/a`.

Verifying H.323 fax call operations

The `h323debug` command verifies fax call operations. This diagnostic command reports when a fax session

- Is initiated
- Is acknowledged (ACK)
- Fails

For each event, `h323debug` reports the following

Table 5-2. Events reported by the `h323debug` command (Page 1 of 2)

Event	Message	Condition
Fax session is successfully initiated on the near-end gateway	H323: <CALL#> ^a : stackH245Event: Received mode request for T38	The gateway detected a CED tone or the V.21 HDLC flag received from the PSTN/gateway.
Fax session request is successfully received on a far-end gateway	H323: <CALL#> ^a : stackH245Event: Received mode request ACK for T38	The gateway acknowledged a CED tone or the V.21 HDLC flag received from the connecting gateway.

Table 5-2. Events reported by the h323debug command (Page 2 of 2)

Event	Message	Condition
Fax session fails to initiate on the near-end gateway	H323: <CALL#> ^a : WARNING: _stackH245Event() FAX not enabled, request mode refused!	The gateway could not respond to a CED tone or the V.21 HDLC flag received from the PSTN/gateway.

a. <CALL#> is the unique identifier assigned to a call by the originating Gateway.

The h323ShowStats command provides the following summary of fax call activity, for failed fax requests:

FAX Originate Failed = 0

IPDC message support for real-time fax and transparent modem

IPDC message request packet pass-through call (RCCP), accept packet pass-through call (ACCP), request modify for packet pass-through call (RMCP), and accept modify packet pass-through call (AMCP) messages enable an Signaling Gateway (SoftSwitch) to direct the TAOS unit to enter T.38 fax mode or transparent modem mode on the basis of tone detection.

In addition, the Signaling Gateway (SoftSwitch) can control echo cancellation by disabling it or setting it to 32 milliseconds on a per-call basis.

Transparent data

Transparent data enables users to run a modem on an SS7 VoIP channel using IPDC, regardless of the vocoder in use. Transparent data is encoded as an audio-mode type, either G.711 μ -law (64K) or G.711 a-law (64K).

MultiVoice Gateways detect fax/modem tones in both the TDM connection and RTP stream. When fax/modem tones are detected, echo cancellation and suppression are automatically disabled. When codes other than the G.711 μ -law and a-law are used, IPDC messages allow the SoftSwitch to request the TAOS unit to enable G.711 transparent data mode upon fax tone detection from the MultiVoice Gateway.

T.38 fax

Real-time fax (if supported) is encoded as a data-mode type, T.38 fax. T.38 fax is used to carry facsimile traffic over an IP link. Currently, T.38 is only employed over H.323 VoIP calls. New IPDC messages allow the SoftSwitch to tell the TAOS unit to enter T.38 fax mode upon fax tone detection from the MultiVoice Gateway.



Note The real-time fax license is required to enable T.38 fax for IPDC.

Echo canceller

The Echo Cancellation Tag (0x74) is implemented on a per-call basis. Only values of 0 (off) and 32 milliseconds are currently supported.

An echo canceller, compliant with International Telecommunications Union's (ITU) G.168-2000 standard is supported for the G.711 and G.729A audio codecs.

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, Full-Rate GSM) use the ITU-G.165 standard.

Notify tone (NTN)

The notify tone (NTN) message notifies the Signaling Gateway (SoftSwitch) when an asynchronous fax or modem tone is detected. The TAOS unit sends this message to the Signaling Gateway (SoftSwitch) if either fax or modem tone detection is enabled and the Signaling Gateway (SoftSwitch) identifies the tone. The TAOS unit detects fax tone if `rt-fax-enable` is set to yes in the default voip profile or if it receives the relevant IPDC message from the Signaling Gateway (SoftSwitch).

The TAOS unit detects modem tone if `g711-transparent-data` is set to yes in the default voip profile or if it receives the relevant IPDC message from the Signaling Gateway (SoftSwitch).

Changes to existing message tags

The following existing message tag values are modified for the NTN message to support T.38 and transparent modem/fax detection.

Table 5-3. Modified NTN message tag values (Page 1 of 2)

Tag	Description	Values
0x33	Tone string	f: Fax tone (CED, no phase reversal, or V.21 flags)
		o: Modem tone (CED, phase reversal)

Table 5-3. Modified NTN message tag values (Page 2 of 2)

Tag	Description	Values
0x49	Tone type	0x06: Fax tone (CED, no phase reversal, or V.21 flags)
		0x07: Modem tone (CED, phase reversal)

The following existing message tag values are modified for the RCCP, ACCP, RMCP, and AMCP messages to support T.38 and transparent modem and fax detection.

Table 5-4. Modified RCCP, ACCP, RMCP and AMCP message tag values

Tag	Description	Values
0x70	Encoding type	0x60: Transparent Data encoding ^a
		0x61: T.38 Fax over UDP

a. Currently, Transparent Data is G.711 RTP with several features disabled.

RCCP, ACCP, RMCP, and AMCP message tags

The following new message tag values are added to the RCCP, ACCP, RMCP and AMCP messages to support T.38 and transparent modem/fax detection. These values are applied on an individual call basis.

Table 5-5. New the RCCP, ACCP, RMCP and AMCP message tag values

Tag	Description	Values
0x74	Echo Cancellation	0x00 : Echo canceller off (0 msecs.)
		0x01 : Echo canceller on (32 msecs.)
0x77	Constant Fax tone detection	Report which fax tone support is enabled (either rt-fax-enable=yes or g711-trans-data=yes) and override this setting if appropriate.
0x78	Constant Modem tone detection	Report whether modem tone support is enabled (either g711-trans-data=yes or g711-trans-data=no) and override this setting if appropriate.

New NTN message tags

The NTN message is sent by the MultiVoice Gateway to Signaling Gateway (SoftSwitch) when fax or modem tone detection is enabled and either tone is detected. The fax/modem tone detection can be enabled or disabled either by the IPDC tags in RCCP and RMCP messages or in the voi p profile.

The following new NTN message is added to support T.38 and transparent modem/fax detection. These values are applied on an individual call basis.

Table 5-6. New NTN message

Tag	Description	Values
0x00F0	Notify Tone	This NTN message from the TAOS unit notifies Signaling Gateway (SoftSwitch) of asynchronous fax/modem tone detections.

The following tags may be included in a Notify Tone message:

Table 5-7. Notify Tone message tags

Tag	Description	Values
0x65	Source Post Type	Required.
0x07	Source Module Number	Required.
0x0D	Source Line Number	Required.
0x15	Source Channeled Number	Required.
0x40	Ascend Route ID	Optional.
0x33	Tone String	Required.
0x49	Tone Type ^a	Required.

a. Currently Tone String and Tone Type convey the same information.

ss7nmi command

The `ss7nm -m` command output includes modifications for the RMCP, AMCP and NTN messages as illustrated by the following:

```
admin>ss7nmi -m
```

IPDC message processing statistics:

Message code	Received	Sent
RCR (0x0011):	1	0
ACR (0x0012):	0	1
RCCP (0x0013):	1	0
ACCP (0x0014):	0	1
RMCP (0x0015):	1	0
AMCP (0x0016):	0	1
RMS (0x0041):	1	0
NMS (0x0042):	0	17

RLS	(0x0043):	1	0
NLS	(0x0044):	0	1
NSUP	(0x0081):	0	1
ASUP	(0x0082):	1	0
NTN	(0x00f0):	0	1

Data collection was started: [04/26/2000 15:40:47]

Max Data Transmission Rate Configuration

The `max-data-rate` parameter in the `rt-fax-options` sub-profile of the `voip` profile sets the maximum data transmission rate allowed for a T.38 fax session configurable on a MultiVoice Gateway. The bandwidth used for fax sessions on your networks can be regulated.

Through the MultiVoice Gateway administration interface, you can modify the rate negotiation between the originating and destination fax terminals. This improves the reliability of the fax transmission by selecting lower fax transmission rates, resulting in fewer lost or repeated fax packets and requiring less bandwidth for fax transmissions.

Rate modification of the fax transmission rate is accomplished by modifying the content of the Digital Identification Signal (DIS) frame transmitted from the destination fax, using the `max-data-rate` parameter in the `rt-fax-options` sub-profile. Upon receipt of that DIS frame, the originating fax will use the data transmission rate specified in the Max Rate parameter (or slower), and a supported modulation type. The content of the DIS frame is defined in the ITU Telecommunication sector standard (ITU-T) T.30, *Procedures for document facsimile transmission in general switched telephone networks*.

Changing the `max-data-rate` parameter modifies the high-speed data transmission rate reported by the destination fax, and masks certain modulation types associated with higher fax transmission speeds. For example, once the data rate is set for 9600 bps, V.17 and V.33 are disallowed even though V.17 supports 9600 and 7200 bps. This is necessary since the DIS frame can specify only the supported modulation types for the highest selected transmission speeds on the destination fax, and since the calling fax terminal requires “training” to match the supported modulation. The value assigned to the Max-Rate parameter on the egress MultiVoice Gateway sets the maximum fax transmission rate for the call.

Setting the max-data-rate parameter

The `max-data-rate` parameter modifies the rate negotiation between the originating and destination fax terminals. This improves the reliability of the fax transmission by reducing the number of lost or repeated packets which occur during high rate transmissions, and reduces the required bandwidth for fax transmissions. Changes made to this parameter setting take effect with the next VoIP call.

Values assigned to this parameter cause MultiVoice to do the following:

Parameter value	Specifies
14400	(Default). Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 14,400bps.
9600	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 9,600bps.
4800	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 4,800bps.
2400	Mask the fax capabilities in the DIS frame that support fax data transmission at rates higher than 2,400bps.

The following example illustrates how to set the fax data transmission rates:

```
admin> read voip { 0 0 }  
VOIP/{ 0 0 } read  
  
admin> list rt-fax-options  
[in VOIP/{ 0 0 }:rt-fax-options]  
  
admin> set max-data-rate=9600  
  
admin> write  
VOIP/{ 0 0 } written
```

This parameter has the following dependency:

- This parameter is N/A when `rt-fax-enable=no`.

Fax session detection

In a regular fax session, the called terminal (fax machine) sends a CED tone (a continuous 2100Hz +/-15Hz, -10 dBm nominal, for not less than 2.6 seconds and not more than 4 seconds) to indicate a connection with a called nonspeech terminal. Then CCITT V.21 channel #2 (FSK) modulation at 300BPS from the called terminal begins. Each FSK frame is preceded by one second (+/- 15%) of HDLC flags 0x7E. The one and zero correspond to the tones at 1650Hz and 1850Hz (lasting a bit duration, 1/300 sec) respectively in FSK frames. Since both signals are generated by the called terminal, they should be detected on the egress gateway. Fax call processing is initiated as follows:

```
Call -> Answer -> CED -> FSK Frames ->
```

Because certain fax machines do not send CED, both the CED and the V.21 flags detection is implemented on the egress gateway to detect fax calls. Once either tone is detected, the slave DSP informs i960 through SARM. When CED is detected, the

gateway initiates the switch over to a fax call without waiting on detection of V.21 flags. Then the fax session begins. The detection ranges are as follows:

Table 5-8. Detection ranges

Detected tones	frequency tolerance	min reception level
CED	+/- 21Hz	-30dBm
V.21 Flags :	+/- 21Hz	-27dBm

Fax compatibility

While real-time fax is generally compatible with any fax machine with supports CED and V.21 signaling, the following faxes/fax software have been successfully tested with MultiVoice real-time fax:

- Ricoh Fax 7700L
- Brother Intellifax 770
- Canon Faxphone B640
- Xerox Workcenter 450c
- Sharp Ux107
- Brother Intellifax I550
- Panasonic Kx-FM220
- Winfax Pro
- Procomm Plus
- Telegra scripts



Note The Mitsubishi FA 1500W, which does not retransmit the DCS/TCF exchange during the negotiation phase of a fax call, proved to be incompatible with MultiVoice real-time fax.

Network Reporting

6

Network reporting options	6-1
Enabling SNMP traps for MultiVoice	6-1
NavisAccess™ support for VoIP call reporting	6-8
NavisAccess™ support for RTP payload information	6-11
Reporting cause codes to MVAM	6-14
Calculating and reporting packet jitter	6-19
Q.931 messaging for SS7 V.110 calls	6-19

Network reporting options

When a TAOS unit is used as a MultiVoice Gateway, the unit can be configured to report call activity using either Simple Network Management Protocol (SNMP) or by generating call record information for NavisAccess™.

Base profile parameters

A TAOS unit must be licensed to support extended network management reporting of VoIP and fax. Extended network management reporting is enabled when the `network-mgmt-voip-enabled` parameter is present and set to yes. This allows monitoring of MultiVoice using SNMP or NavisAccess™.

Enabling SNMP traps for MultiVoice

VoIP-enabled TAOS units can generate notifications for the following MultiVoice Gateway events:

- Change in the call logging server
- Change in configured Gatekeeper for VoIP
- Change in state of a WAN line

For the traps to be sent, they must be enabled in the system and the individual trap conditions must be set to yes. For details about enabling traps, see the *APX/MAX TNT Administration Guide*.

Following are the relevant parameters (shown with default values) for enabling the individual trap conditions:

```
[in TRAP/""]  
call-log-serv-change-enabled = no  
voip-gk-change-enabled = no  
wan-line-state-change-enabled = no
```

Parameter	Setting
call-log-serv-change-enabled	Enable/disable notification when the call-logging server changes. If the call-logging server index is changed or if the IP address of the active call-logging server is changed, this trap notification sends the following information to the SNMP manager: <ul style="list-style-type: none">• The new call logging server index (callLoggingServerIndex)• The IP address of new call logging server (callLoggingServerIPAddress)• The absolute that the server change occurred (sysAbsoluteCurrentTime) (Ascend Trap 38)
voip-gk-change-enabled	Enable/disable notification when the registered gatekeeper changes. If a new Gatekeeper is registered with the gateway, a register request (RRQ) message is sent from the gateway to the new gatekeeper. When the gateway receives the admission request (ARQ) message from the new gatekeeper, this notification sends the following information to the SNMP manager: <ul style="list-style-type: none">• The new gatekeeper index (voipCfgGkIndex)• The IP address of new gatekeeper (voipCfgGkIpAddress)• The absolute time that the gatekeeper change occurred (sysAbsoluteCurrentTime) (Ascend Trap 39)
wan-line-state-change-enabled	Enable/disable notification if the state of an E1 or T1 line changes. This trap sends the following information to the SNMP manager: <ul style="list-style-type: none">• The T1 or E1 line interface index (wanLineIfIndex)• The line usage (wanLineUsage). This usage is reported as trunk, quiesced, or disabled.• The absolute time that the line state changed (sysAbsoluteCurrentTime) (Ascend Trap 40)

The VoIP MIB (ascend 28)

The VoIP MIB enables network management stations to monitor MultiVoice Gateway operations using SNMP. Attributes in the MIB can be obtained by SNMP Get and Get-Next commands. The MIB uses the following object identifiers for identifying MultiVoice Gateway or MultiVoice Gatekeepers to a network manager:

- voipCfgGroup (voipGroup 1)
- voipCfgGkGroup (voipCfgGroup 1)
- voipCfgGwGroup (voipCfgGroup 2)

The MIB uses the following tables for identifying MultiVoice Gateway and MultiVoice Access Manager functions.

voipCfgGkTable OBJECT-TYPE (voipCfgGkGroup 1)

SYNTAX SEQUENCE OF VoipCfgGkEntry

ACCESS not-accessible

STATUS mandatory

DESCRIPTION A list of entries for H323 network Gatekeeper.

voipCfgGkEntry OBJECT-TYPE (voipCfgGkTable 1)

SYNTAX VoipCfgGkEntry

ACCESS not-accessible

STATUS mandatory

DESCRIPTION An entry holding information about the Gatekeeper for the system.

INDEX (voipCfgGkIndex)

VoipCfgGkEntry:

SEQUENCE :

voipCfgGkIndex-INTEGER

voipCfgGkStatus-INTEGER

voipCfgGkIpAddress-IpAddress)

voipCfgGkIndex OBJECT-TYPE (voipCfgGkEntry 1)

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION This number uniquely identifies the Gatekeeper.

voipCfgGkStatus OBJECT-TYPE (voipCfgGkEntry 2)

SYNTAX INTEGER:

registered(1)

not_registered(2)

ACCESS read-only

STATUS mandatory

DESCRIPTION This value indicates whether the gateway is registered with the Gatekeeper.

voipCfgGkIpAddress OBJECT-TYPE (voipCfgGkEntry 3)

SYNTAX IpAddress

ACCESS read-only

STATUS mandatory

DESCRIPTION The IP address of the Gatekeeper.

voipCfgGwVpnMode OBJECT-TYPE (voipCfgGwGroup 1)

SYNTAX INTEGER:

no (1)

yes(2)

ACCESS read-only

STATUS mandatory

DESCRIPTION Virtual Private Network Toggle Switch.

```
voipCfgGwPktAudioMde OBJECT-TYPE (voipCfgGwGroup 2)
    SYNTAX INTEGER:
        other(1)
        g711_ulaw(2)
        g711_alaw(3)
        g723(4)
        g729(5)
        g723_6_4kps(6)
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION Audio Coder to be used for voice packetization.
```

The voipCfgGwVpnMde and voipCfgGwPktAudioMde objects can be accessed using index 0 because they are separate leaves in the MIB tree.

The voipCfgGkIndex, voipCfgGkCurrent and voipCfgGkIpAddress objects are located in the voipCfgGkTable table. They can be obtained using voipCfgGkIndex as an index.

Sending H.323 call information to SNMP log clients

H.323 call information from MultiVoice Gateways can be collected. This includes the capability to generate start, stop, and call progress records for both VoIP and fax calls.

H.323 call information from MultiVoice Gateways performing VoIP call processing can be sent to SNMP log clients. Each MultiVoice Gateway provides the following H.323 call information:

- Billing start records
- Billing stop records
- Call disconnect records
- Fax start records

Billing start records

A billing start record reports the point in the call where speech communications is established. Start records provide the following information:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track H.225.0 call setup messages related to a particular call.
Dial time	The time a user spends dialing the destination telephone number. This is the time a MultiVoice Gateway waits to collect the dialed telephone number. This value is zero for calls originating from the LAN.

Attribute	Specifies
Setup time	The time from the moment a user finishes dialing the destination telephone number until the moment the speech is established to the called destination.
Call origin	The IP address used to identify the calling origin. This can be the ingress MultiVoice Gateway or an H.323-compliment terminal.
Remote IP	The IP address used to identify the called destination. This can be the egress MultiVoice Gateway or an H.323-compliment terminal (PC).
Telephone number	The dialed number string entered by the user.
CLID number	The E.164 address associated with the calling origin.
Audio mode	The audio codec used to connect an H.323 call.

Billing stop records

A billing stop record reports the point in the call where speech communications terminates (end points go on-hook). Stop records provide the following information:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call and is used to track H.225.0 call setup messages related to a particular call.
Connect time	The time from the moment speech is established until the callers hang up (go onhook) normally.
Drop time	The time a call connection is dropped by the WAN or LAN connection, which ever signal is reported first.
Drop reason	The H.323 call drop reason. For normal call termination, the billing stop record reports normal Drop.

Call disconnect records

A call disconnect record is generated whenever a call is not terminated normally (such as when a connection between end points is lost as a result of equipment failure or network failure). Disconnect records provide the following information;

though some information may not be present as depending upon the origin of the call failure:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track H.225.0 call setup messages related to a particular call.
Dial time	The time a user spends dialing the destination telephone number. This is the time a MultiVoice Gateway waits to collect the dialed telephone number. This value is zero for calls originating from the LAN.
Setup time	The time from the moment a user finishes dialing the destination telephone number until the moment the speech is established to the called destination.
Call origin	The IP address used to identify the calling origin. This can be the ingress MultiVoice Gateway or an H.323-compliment terminal.
Remote IP	The IP address used to identify the called destination. This can be the egress MultiVoice Gateway or an H.323-compliment terminal (PC).
Telephone number	The dialed number string entered by the user.
CLID number	The E.164 address associated with the calling origin.
Audio mode	The audio codec used to connect an H.323 call.
Drop from	The location which disconnected the call, either WAN or LAN.
Drop reason	The H.323 call drop reason. For disconnect reports, this is an incomplete and interrupted call termination reason.

Fax start records

A fax start record is generated whenever a fax answer tone is detected during a VoIP. The fax record provides the following information:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call and is used to track H.225.0 call setup messages related to a particular call.
Modulation type	The fax modulation type detected by the MultiVoice Gateway (such as V.21, V.27, V.29, V.17, etc.)
Speed	The transmission speed, modulation rate, detected for this fax transmission by the MultiVoice Gateway (such as 2400, 4800, 7200, etc.)



Note Fax records are generated for T.38 fax transmissions.

H.323 disconnect reasons

H.323 disconnect reasons have been added to disconnect-reason-type.mibdef for the Ascend disconnect type. Reported disconnect reasons for standard and nonstandard call termination are recorded in the following table.

Call drop reason	Call drop code	Specifies
DIS_H323_DROP_REASON_NULL	500	Call drop reason not available
DIS_H323_DROP_REASON_NORMAL	501	Normal disconnect (caller hung up)
DIS_H323_DROP_REASON_DEST_BUSY	502	Called destination busy
DIS_H323_DROP_REASON_DEST_UNREACHABLE	503	Called destination unreachable
DIS_H323_DROP_REASON_REJECT	504	Call rejected by TAOS
DIS_H323_DROP_REASON_WAN_FAILURE	505	WAN failure, egress MultiVoice Gateway could not connect the call

Call drop reason	Call drop code	Specifies
DIS_H323_DROP_REASON_GATEWAY_RESOURCES	506	Egress MultiVoice Gateway could not process the call
DIS_H323_DROP_REASON_NO_BANDWIDTH	507	Sufficient bandwidth not available on the WAN for this call
DIS_H323_DROP_REASON_GW_NOT_REGISTERED	508	Egress MultiVoice Gateway is currently unregistered with the MVAM
DIS_H323_DROP_REASON_INVALID_PIN	509	Caller entered an invalid PIN
DIS_H323_DROP_REASON_INVALID_DNIS	510	Caller dialed invalid number for called destination
DIS_H323_DROP_REASON_NO_LAN_ANSWER	511	A LAN connection was not available
DIS_H323_DROP_REASON_STATE_MACHINE	512	Call state machine on MultiVoice Gateway could not advance
DIS_H323_DROP_REASON_NO_LAN_DISCONNECT	513	The WAN dropped the connection
DIS_H323_DROP_REASON_FEGW_CAUSE_CODE	514	The egress MultiVoice Gateway dropped the connection
DIS_H323_DROP_REASON_MAX_PIN_ATTEMPTS	515	The caller failed to authenticate on all attempts to enter the PIN
DIS_H323_DROP_REASON_CODER_DENIED	516	The MultiVoice Gateway could not negotiate an audio codec selection with the far-end gateway

NavisAccess™ support for VoIP call reporting

Basic VoIP call reporting using NavisAccess™ includes the capability to generate start records, stop records, and call progress records for both VoIP and fax calls. These

records allow NavisAccess™ to monitor gateway resource usage and provide information to create billing records. Each VoIP call can generate two or more records.

Start records

A start record reports the point in the call where a speech communications is established. Start records can provide the following information:

Attribute	Specifies
Ascend-Call-Direction	Direction of the call between the gateway and PSTN. The reported values are Ascend-Call-Direction-Incoming (0) and Ascend-Call-Direction-Outgoing (1). (Ascend Trap 48)
NAS-Port	Encoded NAS port used for this call. (RFC Trap 5)
NAS-Port-Type	Encoded NAS port used for this call. The value 7 for this attribute identifies a VoIP call. (RFC Trap 61)
NAS-IP-Address	NAS IP address associated with this call. (RFC Trap 4)
Session-Id	NAS session index recorded in the session table for this call. (RFC Trap 44)
Ascend-Modem-PortNo	DSP/modem port allocated for processing this call. This value is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 120)
Ascend-Modem-SlotNo	Slot where the DSP/modem card associated with the reported Ascend-Modem-PortNo is located. This value is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 121)
Ascend-Modem-ShelfNo	Shelf where DSP/modem card allocated for processing this call is installed. This is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 122)
Called-Station-Id (DNIS)	Dialed number string reported by the gateway for the called destination. (RFC Trap 30)
Ascend-Dialed-Number	Dialed number string used by the gateway to complete the call. (Ascend Trap 24)
Service-Type	Requested type of service, the value of the Type of Service byte, for this call. (RFC Trap 6)
Ascend-H323-Destination-NAS-ID	NAS IP address used to route the call to the connecting gateway. (Ascend Trap 22)
Ascend-H323-Gatekeeper-IP	IP address of the Gatekeeper used to route the call. The gateway is registered with this gatekeeper. (Ascend Trap 19)
Ascend-Global-Call-Id	IP address used by the gatekeeper to identify the connecting gateway for this call. (Ascend Trap 20)

Attribute	Specifies
Ascend-H323-Conference-ID	IP address used to identify the called destination. (Ascend Trap 21)
Ascend-H323-PreSession-Time	Time from the moment the caller finishes dialing the destination telephone number until the moment the speech path is established to the called destination. (Ascend Trap 198)
Ascend-H323-Dial ed-Time	Time the user spends dialing the destination telephone number. This value is zero for a call originating from the WAN. (Ascend Trap 23)
Ascend-Session-Type	Audio codec used for processing the call. (Ascend Trap 18)

Stop records

A stop record is generated at the moment when MultiVoice begins to tear down the speech path or when an incoming call to a gateway fails to connect. A stop record can contain the following information:

Attribute	Specifies
Acct-Session-Time	Time from the moment the speech path is established to the called destination until the moment MultiVoice begins to tear down the speech path. (RFC Trap 46)
Ascend-Connect-Progress	A number that represents the call connect state at the time the call was terminated. (Ascend Trap 195)
Ascend-Disconnect-Cause	A number that reports the H.323 call disconnection reason. (Ascend Trap 196)
Ascend-H323-Inter-Arrival-Jitter	Estimated interarrival jitter for voice packets received by a gateway. (Ascend Trap 25)
Ascend-Dropped-Octets	The number of voice frames (in bytes) dropped by a gateway during call processing. (Ascend Trap 26)
Ascend-Dropped-Packets	Number of voice packets dropped by a gateway during call processing. (Ascend Trap 26)
Acct-Input-Octets	Number of voice frames (in bytes) received by a gateway during this call. (RFC Trap 42)
Acct-Input-Packets	Number of voice packets received by a gateway during this call. (RFC Trap 47)
Acct-Output-Octets	Number of voice frames (in bytes) sent by a gateway during this call. (RFC Trap 43)
Acct-Output-Packets	Number of voice packets sent by a gateway during this call. (RFC Trap 48)

Call progress records

A call progress record can be generated during a VoIP call when a change in resource occurs for a fax or transparent modem call. For fax calls, this record includes the modem speed and modulation. A progress message contains all the information included in a start record.

NavisAccess™ support for RTP payload information

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 a MultiVoice Gateways. 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 `rtpqos-polling-enable` can be activated so the i960 processor requests 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 a MultiVoice Gateway configured with MultiDSP cards.

TAOS collects information periodically during the voice call—the general information content is described in Table 6-1.

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 6-1 is a description of this QoS information content.

Table 6-1. 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)			Applies to both			
* 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.

To generate RTP QoS statistics, enable the rtpqos-polling-enable parameter in the voip profile.

Parameter	Setting
rtpqos-polling-enable	Setting this to yes generates RTP QoS statistics 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). Default is no. Note This parameter is only applicable when the packet-audio-mode parameter is set to G.711 or G.729.

Call logging STOP packet

The Call Logging STOP Packet contains 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

Option	Specifies
Ascend-Rtp-Local-Jitter-Variance	Variation in jitter measured at local RTP receiver
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
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
Ascend-Rtp-Local-Silence-Sent	Total number of bytes transmitted by local RTP transmitter
Ascend-Rtp-Local-Silence-Percent	Percentage silence measured at local RTP transmitter

Remote RTP transmitter and receiver

The following are statistics regarding Remote RTP Transmitter and Receiver:

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

Option	Specifies
Ascend-Rtp-Remote-Delay-Variance	Variation in round trip delay measured at Remote RTP transmitter
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
Ascend-Rtp-Remote-Silence-Sent	Total number of bytes transmitted by Remote RTP transmitter
Ascend-Rtp-Remote-Silence-Percent	Percentage silence measured at Remote RTP transmitter

End-of-call statistics

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 contains 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 contains a value estimating the jitter measured during the call.

ACR Message

Tag 0 x 99 (Estimated Latency): This tag is now added. It contains 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 contains a value estimating the jitter measured during the call.

Reporting cause codes to MVAM

The reporting capabilities of a MultiVoice Gateway include the Q.931 cause code or H.225 Release Complete reason in the data reported to the MultiVoice Access Manager (MVAM) in a Drop Request (DRQ) message.

Release codes

There are two types of release codes that can be reported when a VoIP call is terminated, either Q.931 Cause codes or H.225 Release Complete Reason codes. MultiVoice uses the event definitions in the H.323 stack to determine which release code gets reported in the DRQ.

The MultiVoice Gateway extracts the Q.931 Cause code or H.225 Release Complete reason from H.225 Connection object (release complete message); then reports the release code as part of the nonStandardData byte sent to MVAM in the DRQ message.

When reporting call release codes, MultiVoice reports:

- The Q.931 Cause code when the event that terminates the VoIP call is related to a call progress error on active calls
- The H.225 Release Complete reason code when the event that terminates the VoIP call is related to a call admission error

For TAOS 5.0Ap23, the Q.931 Cause codes listed in Table 6-2 are reported by MultiVoice Gateways as call release codes.

Table 6-2. Reported Q.931 Cause codes

H.323 Cause code	Code
H323_Call_Rejected	256
H323_Call_No_Answer	257
H323_Call_Busy	258
H323_Call_Failed	259
H323_Call_No_Resources	260
H323_Call_No_Bandwidth	262
H323_Call_No_Destination	163
H323_Call_No_Gatekeeper	164
H323_Call_Bad_Format	165
H323_Call_Not_Registered	166
H323_Call_Network_Failed	167
H323_Call_Unassigned_Num	168
H323_Call_Dest_OutofOrder	169
H323_Call_Invalid_Pin	170
H323_Call_Invalid_Dnis	171
H323_Call_Pin_Required	172
H323_Call_2Dnis_Required	173
H323_Call_PinAnd2Dnis_Required	174

For TAOS 5.0Ap23, the H.225 Release Complete reason codes found in Table 6-3 are reported by MultiVoice Gateways as call release codes.

Table 6-3. Reported H.225 Cause codes

H.225 Reason Complete	Code
H225_Idle	100
H225_RAS_Reject	112
H225_RAS_Drop	113

Reporting Q.931 messages

Q.931+ message trace information displayed in English language format. Previously, diagnostic and status information was displayed in hexadecimal format, which provides no intuitive information as to message meanings.

The diagnostic and status information that is displayed in English language format includes the following:

- Q.931 call progress events
- Layer 2 and Layer 3 transport events
- Initialization and data transport errors

Modifications to the ss7asg command

The ss7asg debug-level command output reports TUNL message statistics when entered as follows:

```
admin> ss7asg -s
```

The -s option of the ss7asg command provides an English language summary of SS7 signaling activity for a MultiVoice Gateway. A new debug option for dumping call information elements (IE) are available and added as part of this enhancement. TAOS 9.0 modifies the ss7asg debug command to include the following options:

Options	Specifies
-i	Display the SS7 interface ID map
-m	Show all MCBs (ME control blocks)
-n	Show all NLCBs (Layer 3 call blocks)
-s	Show SS7 interface statistics
-r	Reset SS7 signaling layer statistics

To set the diagnostics level for the ss7asg command, use the following Diag command to assign the appropriate debug level:

```
diag ss7asg level
```

Debug level	Specifies
0x00	Diagnostic output is disabled. No debugging information is collected.
0x01	Report errors only. Collect only high level error information as errors occur.
0x02	Record Layer 3 events and state changes. The Layer 3 state transitions are displayed as they happen.
0x04	Record call control events. Collect in session logs.
0x08	Collect decoded information elements (IE) for each SS7 call.
0x10	Show detailed debugging traces. Collect full session logs, including low-level processing information.
0x20	Enable code trace for debugging
0x40	Record Layer 3 packet information
0x80	Collect call control primitives
0x100	Collect signaling link event information
0x200	Show memory allocation/deallocations for TAOS unit processing of SS7 calls.

Displaying extended information

Extended information elements contain processing details about ASG call processing. Setting debug level 0x08 displays the following information elements decoded (nonhexadecimal) format:

- Bearer cap
- Called Party number
- Calling Party number
- Cause value
- Call state
- Channel identification
- Call reference

The following example illustrates the output of the `ss7nmi -m` command, reporting the TUNL messaging statistics:

```
tnt-176> ss7asg -s
```

```
SS7 Signaling Gateway interface statistics:
```

```
    Initialized successfully:      No
    Interface state:              Disabled
    Diagnostic level:              0
```

```
Initialization Errors:
```

```
    Number of errors in initialization: 0
    Memory pools:                   0
    Mailboxes:                      0
```

Signaling Layer:

Number of SETUP requests from:	L2: 0	CC: 0
Number of CONNECT to ASG:	0	
Number of CONNECT_ACK from ASG:	0	
Number of SETUP rejected from:	L3: 0	CC: 0
Number of DISCONNECT requests from:	L2: 0	CC: 0
Number of REGISTRATION to ASG:	0	
Number of REGISTRATION_ACK from ASG:	0	
Number of SERVICE recv:	0	
Number of SERVICE_ACK xmit:	0	
Number of DL_REL_IND from L2:	0	
Number of DL_EST_IND from L2:	0	
Number of T303 expiry events:	0	
Number of T305 expiry events:	0	
Number of T308 expiry events:	0	
Number of BC Resp without matched NLCB:	0	
Last L3 counters reset timestamp:	[09/27/2000 08:17:54]	

Data Transport Layer:

Number of link fail-overs:	0
Number of persistent errors:	0
Last error:	No Error
Last error status change timestamp:	[01/01/1990 00:00:00]

Reporting call failures in cause codes

The MultiVoice Gateway reports the call progress cause code in the billing Disengage Request (DRQ). This 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 has been 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 cause code information is displayed using h323debug.

Calculating and reporting packet jitter

Jitter calculation on the StrongARM (SARM) processor for reporting RTP packet transmissions is available in TAOS 5.0Ap23. The packet jitter on a MultiVoice Gateway is reported to both the Media Gateway Controller (SoftSwitch) for IP Device Control (IPDC) protocol packets and to NavisAccess™ administration systems.

The jitter calculation provides an estimate of the statistical variance of the RTP data packet interarrival time, measured in timestamp units and expressed as an unsigned integer. The interarrival jitter is defined to be the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets. As the control DSP accepts packets from the i960 processor shared memory interface, jitter is calculated using the formula defined in RFC 1889, *RTP: A Transport Protocol for Real-Time Applications*, (Jan. 1996), IETF, as illustrated:

$$\text{jitter} += (1/16) * (d - (\text{jitter}))$$

The results of this equation returns the equivalent of the difference in the relative transit time for the two packets; the relative transit time is the difference between a packet's RTP timestamp and the receiver's clock at the time of arrival, measured in the same units. Since all time calculations on MultiVoice Gateways are executed using a fixed point system, the jitter calculation is implemented using the following modified version of the formula specified by RFC 1889:

$$\text{jitter} += (d - (\text{jitter} + 8) \gg 4);$$

In this case, the difference (d) is the difference between the current transit time and the previous transit time, as defined in RFC 1889. This value is maintained for each Slave DSP.

Transit time is calculated by calculating the time difference between two consecutive packets, and subtracting the difference in RTP timestamps. The values are reported to the i960 through the Query Call Stats message response, the 32 bit jitter response is added to the end of message as first word, upper 16 bits, second word, lower 16 bits. The value is the number of 125us ticks.

Q.931 messaging for SS7 V.110 calls

The feature adds Q.931 messaging support for requesting V.110 bearer capability for Signal System 7 (SS7) calls. A second octet in the call setup message information element is sent by a protocol control gateway (PCG). When a PCG, such as Lucent SoftSwitch, includes the Q.931 information element in the call setup message, the information element enables asynchronous transfer mode and disables in-band negotiation.

For calls requiring V.110 bearer capability, the PCG generates a Q.931 call setup message requesting bearer capability at one of the following unrestricted

adaptation rates, in bits-per-second (bps), supported by MAX TNT or APX 8000 units:

- 2400bps to 64Kbps
- 4800bps to 64Kbps
- 9600bps to 64Kbps
- 19200bps to 64Kbps
- 38400bps to 64Kbps

Supported Q.931 bearer capability requests

The call type is set in octet 5 of the Q.931 call setup message sent from the SoftSwitch to the TAOS unit. The adaptation rate is retrieved from the user rate in octet 5a of the Q.931 call setup message.

The following table lists the TAOS-supported bearer capability requests that can be assigned to Octet 5 of the Q.931 setup message by the PCG for SS7 call processing:

Request	Specifies
0x04 0x03 0x80 0x90 0xa0	Speech bearer capability.
0x04 0x04 0x88 0x90 0x21 0xc3	V.110 bearer capability with 2400bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xc5	V.110 bearer capability with 4800bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xc8	V.110 bearer capability with 9600bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xcb	V.110 bearer capability with 19200bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xcd	V.110 bearer capability with 38400bps to 64Kbps unrestricted adaptation.

Octet 5a information element

When the Q.931 call setup message sent by the PCG requests V.110 bearer capability, the following values must be assigned to Octet 5a to enable asynchronous transfer mode and suspend in-band call signaling on a TAOS unit for the duration of the SS7 call.

Bit #	Value	Description
Bit 7	1	Enable asynchronous data mode for this call
Bit 6	0	Disable in-band negotiation

MultiVoice Packet Processing

A

MultiVoice H.323 voice and data transmissions utilize User Datagram Protocol (UDP) packetting for processing voice and RAS channel messages. The Real-time Transfer Protocol (RTP) packets, which contain the voice data, run on top of UDP.

MultiVoice packet format

The size of each MultiVoice packet is determined by the number of audio frames contained in each RTP packet plus the size of the respective headers required to construct the Ethernet frame. Each component of the Ethernet frame include the following elements:

Figure A-1. MultiVoice packet format

<i>Ethernet Header</i>	<i>IP Header</i>	<i>UDP Header</i>	<i>RTP Header</i>	<i>DATA (message)</i>	<i>CRC</i>
------------------------	------------------	-------------------	-------------------	-----------------------	------------

where:

Table A-1. Multivoice packet descriptions (Page 1 of 2)

Element	Size	Description
Ethernet Header	18 bytes	This header contains the source and destination MAC addresses (station addresses) used for the data link between two gateways.
IP Header	20 bytes	This header contains source and destination IP addresses. If MultiVoice packets become fragmented at the IP transport layer, multiple datagrams are generated and assigned sequence numbers so they can be reassembled at the destination gateway.
UDP Header	8 bytes	This header contains the source and destination ports as well as the sequence number of the packet.

Table A-1. Multivoice packet descriptions (Page 2 of 2)

Element	Size	Description
RTP Header	12 bytes	This header contains timestamping and synchronization information for proper reassembly of data at the destination gateway.

Packet sizes by audio codec

The RTP packet header contains a time stamp and sequence number used to reconstruct the voice message. The header size is fixed at 12 bytes. The size of the packet data will vary, depending upon the type of audio codec defined for packet-audio-mode parameter.

Table A-2 provides information on the RTP packet sizes and processing times by audio codec.

Table A-2. RTP packet sizes (Page 1 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.711	1 @ 5ms ea.	52 Bytes	98 Bytes	156800	200
	2 @ 5ms ea.	92 Bytes	138 Bytes	110400	100
	3 @ 5ms ea.	132 Bytes	178 Bytes	94933.33	66.667
	4 @ 5ms ea.	172 Bytes	218 Bytes	87200	50
	5 @ 5ms ea.	212 Bytes	258 Bytes	82560	40
	6 @ 5ms ea.	252 Bytes	298 Bytes	79466.67	33.333
	7 @ 5ms ea.	292 Bytes	338 Bytes	77257.143	28.571
	8 @ 5ms ea.	332 Bytes	378 Bytes	75600	25
	9 @ 5ms ea.	372 Bytes	418 Bytes	74311.11	22.222
	10 @ 5ms ea.	412 Bytes	458 Bytes	73280	20

Table A-2. RTP packet sizes (Page 2 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.723.1 @ 5.3 Kbps	1 @ 30 ms ea.	32 Bytes	78 Bytes	20800.000	33.333
	2 @ 30 ms ea.	52 Bytes	98 Bytes	13066.667	16.667
	3 @ 30 ms ea.	72 Bytes	118 Bytes	10488.889	11.111
	4 @ 30 ms ea.	92 Bytes	138 Bytes	9200.000	8.333
	5 @ 30 ms ea.	112 Bytes	158 Bytes	8426.667	6.667
	6 @ 30 ms ea.	132 Bytes	178 Bytes	7911.111	5.556
	7 @ 30 ms ea.	152 Bytes	198 Bytes	7542.857	4.762
	8 @ 30 ms ea.	172 Bytes	218 Bytes	7266.667	4.167
	9 @ 30 ms ea.	192 Bytes	238 Bytes	7051.852	3.704
	10 @ 30 ms ea.	212 Bytes	258 Bytes	6880.000	3.333

Table A-2. RTP packet sizes (Page 3 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.723.1 @ 6.4 Kbps	1 @ 30 ms ea.	36 Bytes	82 Bytes	21866.667	33.333
	2 @ 30 ms ea.	60 Bytes	106 Bytes	14133.333	16.667
	3 @ 30 ms ea.	84 Bytes	130 Bytes	11555.556	11.111
	4 @ 30 ms ea.	108 Bytes	154 Bytes	10266.667	8.333
	5 @ 30 ms ea.	132 Bytes	178 Bytes	9493.333	6.667
	6 @ 30 ms ea.	156 Bytes	202 Bytes	8977.778	5.556
	7 @ 30 ms ea.	180 Bytes	226 Bytes	8609.524	4.762
	8 @ 30 ms ea.	204 Bytes	250 Bytes	8333.333	4.167
	9 @ 30 ms ea.	228 Bytes	274 Bytes	8118.519	3.704
	10 @ 30 ms ea.	252 Bytes	298 Bytes	7946.667	3.333

Table A-2. RTP packet sizes (Page 4 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.728	1 @ 5ms ea.	22 bytes	68 bytes	108800.00	200
	2 @ 5ms ea.	32 bytes	78 bytes	62400.000	100
	3 @ 5ms ea.	42 bytes	88 bytes	46933.333	66.667
	4 @ 5ms ea.	52 bytes	98 bytes	39200.000	50.000
	5 @ 5ms ea.	62 bytes	108 bytes	34560.000	40.000
	6 @ 5ms ea.	72 bytes	118 bytes	31466.667	33.333
	7 @ 5ms ea.	82 bytes	128 bytes	29257.143	28.571
	8 @ 5ms ea.	92 bytes	138 bytes	27600.000	25.000
	9 @ 5ms ea.	102 bytes	148 bytes	26311.111	22.222
	10 @ 5ms ea.	112 bytes	158 bytes	25280.000	20.000
G.729A	1 @ 10ms ea.	22 bytes	68 bytes	54400	100
	2 @ 10ms ea.	32 bytes	78 bytes	31200	50
	3 @ 10ms ea.	42 bytes	88 bytes	23466.67	33.333
	4 @ 10ms ea.	52 bytes	98 bytes	19600	25
	5 @ 10ms ea.	62 bytes	108 bytes	17280	20
	6 @ 10ms ea.	72 bytes	118 bytes	15733.33	16.667
	7 @ 10ms ea.	82 bytes	128 bytes	14628.571	14.286
	8 @ 10ms ea.	92 bytes	138 bytes	13800	12.5
	9 @ 10ms ea.	102 bytes	148 bytes	13155.56	11.111
	10 @ 10ms ea.	112 bytes	158 bytes	12640	10

Table A-2. RTP packet sizes (Page 5 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
Full-rate GSM	1 @ 20ms ea.	45 bytes	91 bytes	22750	50
	2 @ 20ms ea.	78 bytes	124 bytes	24800	25
	3 @ 20ms ea.	111 bytes	157 bytes	20924.96	16.66
	4 @ 20ms ea.	144 bytes	190 bytes	19000	12.5
	5 @ 20ms ea.	177 bytes	223 bytes	17840	10
	6 @ 20ms ea.	210 bytes	256 bytes	17066.66	8.33
	7 @ 20ms ea.	243 bytes	289 bytes	16514.28	7.14
	8 @ 20ms ea.	274 bytes	320 bytes	16000	6.25
	9 @ 20ms ea.	299 bytes	345 bytes	15333.33	5.55
	10 @ 20ms ea.	342 bytes	388 bytes	15520	5

Determining Jitter Buffer Size

B

The dynamic jitter buffer size is a function of:

- RTP packet duration (in milliseconds) for the selected audio codec
- Total RTP packets as defined by the Initial-Jitter-Buffer-Size and Max-Jitter-Buffer-size parameters

Dynamic jitter buffer size is derived by multiplying the values assigned to the `initial-jitter-buffer-size` and `max-jitter-buffer-size` parameters, respectively, by *packet duration*. Packet duration is the total playout time, in milliseconds, for the speech frames contained in a single RTP packet:

initial-jitter-buffer-size x *Packet Duration (ms)*

max-jitter-buffer-size x *Packet Duration (ms)*

For example, in fixed mode, if `initial-jitter-buffer-size` = 5, and an in-coming call used the G.711 codec with one audio frame per packet, which has a packet duration of 5ms, then:

5 (Packets) x 5ms/packet = 25ms (jitter buffer length)

The instantaneous jitter buffer size for the VoIP call is 25ms. If a second in-coming call used the G.729(A) codec, and had five audio frames per packet, with a packet duration of 50ms, then the instantaneous jitter buffer size for this subsequent call is 250ms.

Dynamic jitter buffers

The following tables contain the calculated dynamic jitter buffers for a single call, by supported audio codec.

Table B-1. *Jitter buffer length (in milliseconds) for the G.711 audio codec (Page 1 of 2)*

Jitter ^a buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.711 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
1	5	10	15	20	25	30	35	40	45	50
2	10	20	30	40	50	60	70	80	90	100

Table B-1. Jitter buffer length (in milliseconds) for the G.711 audio codec (Page 2 of 2)

Jitter^a buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.711 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
3	15	30	45	60	75	90	105	120	135	150
4	20	40	60	80	100	120	140	160	180	200
5	25	50	75	100	125	150	175	200	225	250
6	30	60	90	120	150	180	210	240	270	300
7	35	70	105	140	175	210	245	280	315	350
8	40	80	120	160	200	240	280	320	360	400
9	45	90	135	180	225	270	315	360	405	450
10	50	100	150	200	250	300	350	400	450	500
11	55	110	165	220	275	330	385	440	495	550
12	60	120	180	240	300	360	420	480	540	600
13	65	130	195	260	325	390	455	520	585	650
14	70	140	210	280	350	420	490	560	630	700
15	75	150	225	300	375	450	525	600	675	750
16	80	160	240	320	400	480	560	640	720	800
17	85	170	255	340	425	510	595	680	765	850
18	90	180	270	360	450	540	630	720	810	900
19	95	190	285	380	475	570	665	760	855	950

a. This is the value entered for either initial-jitter-buffer-size and/or max-jitter-buffer-size.

Table B-2. Jitter buffer length (in milliseconds) for the G.729(A) audio codec

Jitter ^a buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.729(A) codec									
	1 frame @10ms	2 frames @20ms	3 frames @30ms	4 frames @40ms	5 frames @50ms	6 frames @60ms	7 frames @70ms	8 frames @80ms	9 frames @90ms	10 frames @100ms
1	10	20	30	40	50	60	70	80	90	100
2	20	40	60	80	100	120	140	160	180	200
3	30	60	90	120	150	180	210	240	270	300
4	40	80	120	160	200	240	280	320	360	400
5	50	100	150	200	250	300	350	400	450	500
6	60	120	180	240	300	360	420	480	540	600
7	70	140	210	280	350	420	490	560	630	700
8	80	160	240	320	400	480	560	640	720	800
9	90	180	270	360	450	540	630	720	810	900
10	100	200	300	400	500	600	700	800	900	1000
11	110	220	330	440	550	660	770	880	990	1100
12	120	240	360	480	600	720	840	960	1080	1200
13	130	260	390	520	650	780	910	1040	1170	1300
14	140	280	420	560	700	840	980	1120	1260	1400
15	150	300	450	600	750	900	1050	1200	1350	1500
16	160	320	480	640	800	960	1120	1280	1440	1600
17	170	340	510	680	850	1020	1190	1360	1530	1700
18	180	360	540	720	900	1080	1260	1440	1620	1800
19	190	380	570	760	950	1140	1330	1520	1710	1900

a. This is the value entered for either initial-jitter-buffer-size and/or max-jitter-buffer-size.

Determining Jitter Buffer Size
Dynamic jitter buffers

Table B-3. Jitter buffer length (in milliseconds) for the G.723.1 audio codec

Jitter^a buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.723.1 codec									
	1 frame @30ms	2 frames @60ms	3 frames @90ms	4 frames @120ms	5 frames @150ms	6 frames @180ms	7 frames @210ms	8 frames @240ms	9 frames @270ms	10 frames @300ms
1	30	60	90	120	150	180	210	240	270	300
2	60	120	180	240	300	360	420	480	540	600
3	90	180	270	360	450	540	630	720	810	900
4	120	240	360	480	600	720	840	960	1080	1200
5	150	300	450	600	750	900	1050	1200	1350	1500
6	180	360	540	720	900	1080	1260	1440	1620	1800
7	210	420	630	840	1050	1260	1470	1680	1890	2100
8	240	480	720	960	1200	1440	1680	1920	2160	2400
9	270	540	810	1080	1350	1620	1890	2160	2430	2700
10	300	600	900	1200	1500	1800	2100	2400	2700	3000
11	330	660	990	1320	1650	1980	2310	2640	2970	3300
12	360	720	1080	1440	1800	2160	2520	2880	3240	3600
13	390	780	1170	1560	1950	2340	2730	3120	3510	3900
14	420	840	1260	1680	2100	2520	2940	3360	3780	4200
15	450	900	1350	1800	2250	2700	3150	3600	4050	4500
16	480	960	1440	1920	2400	2880	3360	3840	4320	4800
17	510	1020	1530	2040	2550	3060	3570	4080	4590	5100
18	540	1080	1620	2160	2700	3240	3780	4320	4860	5400
19	570	1140	1710	2280	2850	3420	3990	4540	5130	5700

a. This is the value entered for initial-jitter-buffer-size.

Table B-4. Jitter buffer length (in milliseconds) for the G.728 audio codec

Jitter ^a buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.728 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
1	5	10	15	20	25	30	35	40	45	50
2	10	20	30	40	50	60	70	80	90	100
3	15	30	45	60	75	90	105	120	135	150
4	20	40	60	80	100	120	140	160	180	200
5	25	50	75	100	125	150	175	200	225	250
6	30	60	90	120	150	180	210	240	270	300
7	35	70	105	140	175	210	245	280	315	350
8	40	80	120	160	200	240	280	320	360	400
9	45	90	135	180	225	270	315	360	405	450
10	50	100	150	200	250	300	350	400	450	500
11	55	110	165	220	275	330	385	440	495	550
12	60	120	180	240	300	360	420	480	540	600
13	65	130	195	260	325	390	455	520	585	650
14	70	140	210	280	350	420	490	560	630	700
15	75	150	225	300	375	450	525	600	675	750
16	80	160	240	320	400	480	560	640	720	800
17	85	170	255	340	425	510	595	680	765	850
18	90	180	270	360	450	540	630	720	810	900
19	95	190	285	380	475	570	665	760	855	950

a. This is the value entered for initial-jitter-buffer-size.

Index



Numerics

800 service, example 1-20

A

Accept-Confirm-Call-Parameters 2-39

Access Manager

definition 1-5

ACCP 1-17, 2-39

ACD 1-20

ack-threshold parameter 2-48

active parameter 3-17, 3-19

adaptive jitter buffers 3-14

Alert-Progress-Indicator parameter 3-40

allow-coder-fallback parameter 3-12

allow-g711-fallback parameter 3-12

AMCP 1-17, 2-40

ANI 2-64

authentication

behind PBXs 3-73

behind WANs 3-73

configure 3-72

with PIN 3-71

ANSWER-DEFAULTS profile

idle-timer 2-11

apply-to parameter 3-17, 3-19

architecture

packet-switched 1-1

ASTN 1-17

audio codecs

configuring negotiation 3-12

descriptions 1-4

Automatic Call Distributor (ACD) 1-20

Automatic Number Identification ANI

B

BASE profiles

real-time fax parameter 5-2

rtfax-enabled parameter 5-2

voip-enabled parameter 2-2, 5-2

Voip-Max-Capacity-Allowed parameter 2-2

xcom-ss7 parameter 2-2

bay-id parameter 2-47

billing start record 6-4

billing stop record 6-5

blocked calls 3-25

definition 3-25

busy signals, and non-ISDN signaling 3-71

C

call disconnect record 6-5

call process

MultiVoice network 1-6

using a secondary Gatekeeper 1-8

call process MultiVoice network

using overlapping coverage areas 1-7

call routing

priority-based 2-25

call signaling

PSTN 3-37

call statistics

IPDC tags supported

IPDC tags not supported 2-43

call volume control 3-20

caller-id parameter 2-56

call-hairpin parameter 3-53

Calling line identification

see CLID 3-59

call-inter-digit-timeout parameter 3-50

call-keep-alive-timeout parameter 3-33

call-progress controlling transmission of tones
3-29

Call-Route profiles 2-17

- cause codes 6-14
- circuit-switched technology 1-1
- CLID
 - gatekeeper substitution 3-59
- clid-suppress parameter 3-33
- codec descriptions 1-4
- cohabitation 2-4
- collect-incoming-digits parameter 2-56
- comfort noise generation 3-13
- configuration
 - 480 ports of G.711 voip-only calls 2-65
 - DNIS/ANI/CLID collection 2-64, 2-65
 - E1 data trunk 2-50
 - Gateway keep alive 3-33
 - H.323 trunk signalling 2-54
 - real-time fax 5-2
 - SS7 data trunks 2-49
 - T1 data trunk 2-49
 - T3 profile 2-49
- control-protocol parameter 2-47
- conventions used in this manual xvii
- country parameter 2-7
- coverage 1-6
- coverage areas, definition 1-6

D

- default-call-type parameter 2-14, 2-15, 2-56
- dest-address parameter 2-36
- Device-State profile 2-12
- Dialed Number Identification Service DNIS
- Digital Signal Processors (DSPs) 3-4, 3-20
- Dircode command 4-12
- DNIS 2-65
- documentation set xviii
- DSP allocation 2-5
- DTMF R2 signaling 2-57
- dtmf-tone-passing parameter 3-32
- dynamic call jitter buffers 3-14

E

- e1-inter-digit-timeout parameter 2-56
- early-ringback-enable parameter 3-54
- ena-adap-jitter-buffer parameter 3-14, 3-15
- enabling sequential calls 3-56
- enabling voice announcements 4-5
 - H.323 VoIP 4-8
 - IPDC VoIP 4-5

- encoded speech
 - voice announcement playout 4-9
- Ethernet header A-1

F

- far-end-number parameter 2-16, 3-8
- fastStart 3-21
- fax start record 6-7
- fax/modem transmission
 - transparent 3-34
- Feature Group D (FGD) signaling 2-55, 2-58
- Fgd-Signaling-Enabled parameter 2-59
- file format conversion for announcements 4-10
- flash cards, formatting 4-10
- FrameRelay networks 1-18
- Full Rate GSM codec 1-5
 - support for 3-11

G

- G.711 codec 1-4
- G.723.1 codec 1-4
 - support for 3-10
- G.728 codec 1-5
 - support for 3-10
- G.729(A) codec 1-5
- Gatekeeper 1-5
- gatekeeper 1-5
 - primary, identification of 3-24
 - redundancy 1-9
 - secondary, identification of 3-25
- Gatekeeper registration parameters
 - gatekeeper-ip-sec 1-11
 - gatekeeper-keepalive 1-11
 - primary-retries 1-11
 - registration-retries 1-11
 - registration-retry-timer 1-11
- gatekeeper-ip parameter 3-7, 3-24
- gatekeeper-ip-sec parameter 1-11, 3-25
- gatekeeper-keepalive parameter 1-11, 3-26
- gateway-access-number parameter 2-16, 3-8
- gateway-address parameter 2-36
- gateways 1-5
 - FrameRelay 1-18
 - registration policy 3-25
- Gateway-to-Gateway keep alive 3-33
- Gk-Mlg-Control parameter 3-2

H

H.323 1-2
 call signaling 3-29
 gatekeeper 1-5
 gateways 1-5
 Host routing
 definition 2-28
 implementation 1-5
 International Telecommunications Union
 Telephone Recommendation 1-22
 IP addressing 2-29
 IP routing 2-28
 Network routing
 definition 2-28
 packet routing 2-29
 multipath routes 2-36
 static routes 2-35
 terminal
 compliant terminals 1-22
 H.323 (v2) fast connect 3-21
 H.323 Annex D T.38 fax 5-1
 H.323 call information
 collecting 6-4
 H.323 compliant terminal 1-22
 H.323 disconnect reasons 6-7
 H.323 gatekeeper zone 1-9
 H.323 trunk signalling 2-54
 H.323 zone
 definition 1-9
 h323-voice-ann-enabled parameter 4-8
 Host routing
 configuration 2-29

I

idle-timer parameter 2-11
 in-call DTMF detection 2-67
 inclusion area
 definition 1-7
 initial-jitter-buffer-size parameter 3-15
 inter-digit timer 3-50
 default setting and behavior 3-50
 International Telecommunications Union 1-2
 IP
 soft interface address 2-9
 IP Device Control IPDC
 IP header A-1
 IPDC
 call statistics 2-43
 definition
 in-call DTMF detection 2-67

 packet routing 2-37
 PRI tunneling 2-50

IPDC messages 1-17

ACCP 1-17
 AMCP 1-17
 ASTN 1-17
 RCCP 1-17
 RMCP 1-17
 STN 1-17

IP-GLOBAL profile

 send-icmp-dest-unreachable 2-10
 throttle-no-port-match-udp-traffic-on-slot
 2-10

IP-ROUTE profile

 dest-address 2-36
 gateway-address 2-36

ITU-T. *See* International Telecommunications Union

J

jitter buffers
 configuring maximum size 3-15
 jitter calculation
 reporting 6-19

K

keepalive registration 3-26

L

Line-Interface profile

 caller-id 2-56
 collect-incoming-digits 2-56
 default-call-type 2-14, 2-15, 2-56
 e1-inter-digit-timeout 2-56
 robbed-bit-mode 2-55
 signaling-mode 2-49, 2-55
 t1-inter-digit-timeout 2-56

logical gateways 3-44, 3-50

M

madd-slot-config profile

 subtype parameter 2-66

Maxcalls parameter 3-20

Max-Dialout-Time parameter 2-7

maximum data transmission rate

- for T.38 fax 5-12
- Max-Jitter-Buffer-Size parameter 3-15
- Media Gateway Control Protocol (MGCP)
 - see MGCP 1-14
- MGCP 1-14
- MultiDSP 288-port slot card 2-65
- multiple logical gateways 3-2, 3-44
- multiple voice announcements 4-2
- multishelf TAOS units
 - use with MultiVoice 2-1
- MultiVoice Access Manager (MVAM)
 - definition 1-5
- MultiVoice Gateway
 - overlapping coverage areas 1-7
- MultiVoice Gateway registration
 - keep-alive registration 1-10
 - registration policy 1-11
 - re-registration policy 1-11
- MultiVoice network
 - coverage areas 1-6
 - H.323 implementation 1-5
 - inclusion areas 1-7
 - overlapping coverage areas 1-7
 - step-by-step call process 1-6
 - step-by-step call processing
 - overlapping coverage areas 1-7
 - secondary gatekeeper 1-8
 - using a secondary MVAM 1-8
- MVAM
 - initialization file
 - parameters
 - registrationDuration 3-26
 - keep-alive registration 1-10
 - registration policy 1-11
 - re-registration policy 1-11

N

- NavisAccess™ support for RTP payload
 - information 6-11
- Network routing
 - configuration 2-31
- next-call parameter 3-57
- non-ISDN signaling, and busy signals 3-71
- num-digits-trunk-groups parameter 2-7

O

- operator assistance 3-53
- Operator-Assist parameter 3-6, 3-54
- overlapping coverage area 1-7

- overlapping coverage areas
 - call processing 1-7

P

- Packet format A-1
- packet redundancy 5-3, 5-5
- packet-redundancy parameter 5-5
- packet-switched architecture 1-1
- parallel-dial parameter 2-7
- Parameters
 - ack-threshold 2-48
 - active 3-17, 3-19
 - alert-progress-indicator 3-40
 - allow-coder-fallback 3-12
 - allow-g711-fallback 3-12
 - apply-to 3-17, 3-19
 - bay-id 2-47
 - caller-id 2-56
 - call-hairpin 3-53
 - call-inter-digit-timeout 3-50
 - call-keep-alive-timeout 3-33
 - clid-suppress 3-33
 - collect-incoming-digits 2-56
 - control-protocol 2-47
 - country 2-7
 - default-call-type 2-14, 2-15, 2-56
 - dest-address 2-36
 - dtmf-tone-passing 3-32
 - e1-inter-digit-timeout 2-56
 - early-ringback-enable 3-54
 - ena-adap-jitter-buffer 3-14, 3-15
 - far-end-number 2-16, 3-8
 - fgd-signaling-enabled 2-59
 - gatekeeper-ip 3-7, 3-24
 - gatekeeper-ip-sec 3-25
 - gatekeeper-keepalive 3-26
 - gateway-access-number 2-16, 3-8
 - gateway-address 2-36
 - gk-mlg-control 3-2
 - h323-voice-ann-enabled 4-8
 - idle-timer 2-11
 - initial-jitter-buffer-size 3-15
 - maxcalls 3-20
 - max-dialout-time 2-7
 - max-jitter-buffer-size 3-15
 - next-call 3-57
 - num-digits-trunk-groups 2-7
 - operator-assist 3-6, 3-54
 - packet-redundancy 5-5
 - parallel dial 2-7
 - precedence 3-17
 - primary-ip-address 2-47, 2-50
 - primary-retries 3-27
 - primary-tcp-port 2-47

- pstn-attribute 3-7
- registration-retries 3-26, 3-27
- registration-retries-timer 3-27
- robbed-bit-mode 2-55
- rt-fax-options 5-2
- secondary-ip-address 2-47
- secondary-tcp-port 2-47
- send-icmp-dest-unreachable 2-10
- sequential-call-enable 3-6, 3-56
- signaling-mode 2-49, 2-55
- silence-det-cng 3-13, 3-15
- silence-threshold 3-14
- single-dial-enable 3-52, 4-4
- ss7voip-call-persistence 3-60
- subtype 2-66
- system-ip-addr 2-8
- system-type 2-47
- t1-duration 2-48
- t1-inter-digit-timeout 2-56
- t2-duration 2-48
- t3-duration 2-48
- throttle-no-port-match-udp-traffic-on-slot 2-10
- tos-options 3-16
- trunk-prefix-enable 3-55
- trunk-quiesce-enable 3-36
- type-of-service 3-18
- use-system-ip-address-as-source 2-47
- voice-ann-dir 4-8
- voice-ann-enc 4-9
- voip-max-capacity-allowed 2-2
- vpn-mode 3-56
- window-size 2-48
- PBX 1-20
- PIN 3-72
 - authentication 3-56, 3-71, 3-72
- Pipeline 85
 - router 1-18
- pound sign 3-71, 3-72
- precedence parameter 3-17
- PRI tunneling
 - configuring 2-50
- primary gatekeeper 3-24
- primary-ip-address parameter 2-47, 2-50
- primary-retries parameter 1-11, 3-27
- primary-tcp-port parameter 2-47
- priority-based call routing 2-25
- Private Branch Exchange 1-20
- PSTN
 - example of 1-1
- PSTN call signaling 3-37
- Pstn-Attribute parameter 3-7
- Public Switched Telephone Network
 - See PSTN 1-1

Q

- Q.931 messaging support 6-19
- Quality of Service (QoS) 1-18

R

- RAS 1-22
- RCCP 1-17
- Real-Time Fax
 - fax session detection 5-13
- real-time fax
 - call routing 5-4
 - H.323 Annex D T.38 standard 5-1
- registration policy
 - configuration attempts 3-26
 - primary Gatekeeper failure 3-26
 - reregistration attempts 3-27
- Registration Request (RRQ) 3-25
- Registration, Admission and Status signaling. *See* RAS
- registrationDuration parameter 1-11, 3-26
- registration-retries parameter 1-11, 3-26, 3-27
- registration-retries-timer parameter 3-27
- registration-retry-timer parameter 1-11
- related www sites xx
- relative silence threshold 3-14
- reporting
 - cause codes 6-14
 - jitter calculation 6-19
 - Q.931+ message trace information 6-16
 - trunk availability 3-28
- requesting
 - operator assistance 3-53
- Request-Modify-Call-Parameters
 - See RMCP 2-39
- reregistration policy 3-26
 - definition 3-26
- RMCP 1-17, 2-39
- Robbed-Bit-Mode parameter 2-55
- routing
 - VoIP call processing 2-5
- rt-fax-options subprofile parameters 5-2
- RTP header A-2

S

- secondary gatekeeper 3-3
- secondary MVAM 1-8

- secondary-ip-address parameter 2-47
- secondary--tcp-port parameter 2-47
- send-icmp-dest-unreachable parameter 2-10
- sequential dialing 3-57
- sequential-call-enable parameter 3-56
- signaling-mode parameter 2-49, 2-55
- silence detection 3-13
- silence-det-cng parameter 3-13, 3-15
- silence-threshold parameter 3-14
- single-dial-enable parameter 3-52, 4-4
- slow poll mode
 - definition 3-25
- SNMP
 - H.323 call information 6-4
- sparing
 - definition 1-9
- SS7 data trunk configuration 2-49
- SS7-GATEWAY profile 2-46
 - bay-id 2-47
 - control-protocol 2-47
 - primary-ip-address 2-47, 2-50
 - primary-tcp-port 2-47
 - secondary-ip-address 2-47
 - secondary-tcp-port 2-47
 - system-type 2-47
 - use-system-ip-address-as-source 2-47
- ss7nmi command 2-52, 3-61
- ss7voip command 3-61
- ss7voip-call-persistence parameter 3-60
- STN 1-17
- StrongARM processor 2-4, 6-19
- subtype parameter 2-66
- SYSTEM profile
 - country 2-7
 - max-dialout-time 2-7
 - num-digits-trunk-groups 2-7
 - parallel-dial 2-7
 - system-ip-addr 2-8
- systems-ip-addr parameter 2-8
- system-type parameter 2-47

T

- t1-duration parameter 2-48
- t1-inter-digit-timeout parameter 2-56
- t2-duration parameter 2-48
- t3-duration parameter 2-48
- throttle-no-port-match-udp-traffic-on-slot parameter 2-10
- tos-options subprofile 3-16

- transparent
 - fax/modem transmission 3-34
- Transport-Options subprofile 2-48
 - ack-threshold 2-48
 - t1-duration 2-48
 - t2-duration 2-48
 - t3-duration 2-48
 - window-size 2-48
- trunk availability
 - reporting 3-28
- trunk configuration 2-46
- trunk-prefix-enable parameter 3-55
- trunk-quiesce-enable parameter 3-36
- type-of-service parameter 3-18

U

- UDP header A-1
- user-defined Voip profiles 3-7
- use-system-ip-address-as-source parameter 2-47

V

- voice announcement playout
 - encoded speech 4-9
- voice announcements
 - converting file formats 4-10
 - creating 4-10
 - creating directories 4-11
 - displaying files of 4-12
 - multiple 4-2
- Voice over IP networks 1-5
- voice-ann-dir parameter 4-8
- voice-ann-enc parameter 4-9
- VoIP networks. *See* Voice over IP networks and MultiVoice network
- VOIP options
 - allow-coder-fallback 3-12
 - allow-g711-fallback 3-12
 - call-hairpin 3-53
 - call-inter-digit-timeout 3-50
 - call-keep-alive-timeout 3-33
 - clid-suppress 3-33
 - dtmf-tone-passing 3-32
 - early-ringback-enable 3-54
 - ena-adap-jitter-buffer 3-14, 3-15
 - gatekeeper-ip 3-7, 3-24
 - gatekeeper-ip-sec 3-25
 - gatekeeper-keepalive 3-26
 - h323-voice-ann-enabled 4-8
 - initial-jitter-buffer-size 3-15

- maxcalls 3-20
- max-jitter-buffer-size 3-15
- next-call parameter 3-57
- primary-retries 3-27
- registration-retries 3-26, 3-27
- registration-retries-timer 3-27
- rt-fax-options 5-2
- silence-det-cng 3-13, 3-15
- silence-threshold 3-14
- single-dial-enable 3-52, 4-4
- ss7voip-call-persistence parameter 3-60
- tos-options 3-16
- tos-options submenu
 - active 3-17, 3-19
 - apply-to 3-17, 3-19
 - precedence 3-17
 - type-of-service 3-18
- trunk-prefix-enable 3-55
- trunk-quiesce-enable 3-36
- voice-ann-dir 4-8
- vpn-mode 3-56
- Voip-Index subprofile
 - definition 2-15, 3-7
 - far-end-number 2-16, 3-8
 - gateway-access-number 2-16, 3-8
- vpn-mode parameter 3-56, 4-4

W

- window-size parameter 2-48
- World Wide Web sites
 - related xx
- www sites
 - related xx

X

- Xedia Access Point 45
 - router 1-18

