Cisco IOS ISDN Voice Configuration Guide

Cisco IOS Release 12.4

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco IOS ISDN Voice Configuration Guide, Release 12.3
Copyright © 2003-2005 Cisco Systems, Inc. All rights reserved.

ISDN Features Roadmap

This chapter contains a list of ISDN features (Cisco IOS Release 12.3 and earlier) and the location of feature documentation.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Release	Features in That and Later Releases	Feature Description	Feature Documentation
12.3(7)T	Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks	Enables the H.323 gateway to access B-channel information for all H.323 calls.	"Configuring H.323 Gateways" on page 39 of the *Cisco IOS H.323 Configuration Guide*
12.2(15)T	Clear Channel T3/E3 with Integrated CSU/DSU	Delivers Clear Channel service as a T3/E3 pipe.	"Implementing Clear Channel T3/E3" on page 71 of this guide
	Expanded Scope for Cause-Code-Initiated Call Establishment Retries	Enables a gateway to reattempt calls upon receipt of a disconnect message from the PSTN without maintaining extra dial peers.	"Implementing Expanded Scope for Cause-Code-Initiated Call-Establishment Retries" on page 65 of this guide
	Integrated Voice and Data WAN on T1/E1 Interfaces with the AIM-ATM-VOICE-30 Module	Provides a voice-processing termination solution at a density of 30 VoIP or VoFR voice or fax channels without consumption of a network-module slot.	"Implementing Integrated Voice and Data WAN on T1/E1 Interfaces" on page 93 of this guide
	ISDN Generic Transparency Descriptor (GTD) for Setup Message	Provides support for mapping ISDN information elements (IEs) to corresponding GTD parameters.	"Implementing ISDN GTD" on page 119 of this guide
	Support for IUA with SCTP for Cisco Access Servers	Supports ISDN user adaptation (IUA) with SCTP. Provides an alternative to existing IP-based UDP-to-Reliable Link Manager (RLM) transport between a Cisco PGW2200 and Cisco gateways.	"Implementing SCTP Features" on page 155 of this guide

Release	Features in That and Later Releases	Feature Description	Feature Documentation
12.2(11)T	Non-Facility Associated Signaling (NFAS) with D-Channel Backup feature	Allows a single D channel to control multiple ISDN PRI interfaces.	"Implementing NFAS" on page 143 of this guide
	QSIG for Toolkit Command Language Interactive Voice Response (Tcl IVR) 2.0	Provides transparent Q.SIG interworking with a Tcl IVR 2.0 voice application on a Cisco gateway.	"Implementing QSIG for Tcl IVR" on page 213 of this guide
	T1 Channel-Associated Signaling (CAS) for VoIP	Adds support for T1 CAS and E1 R2 signaling with the voice feature card.	"Implementing T1 CAS" on page 223 of this guide
12.2(8)T	Digital J1 Voice Interface Card	Provides the proper interface for directly connecting Cisco multiservice access routers to PBXs throughout Japan that use a J1 (2.048-Mbps TDM) interface.	"Implementing the Digital J1 VIC" on page 241 of this guide
12.1(1)T	PRI Backhaul Using Stream Control Transmission Protocol (SCTP) and the ISDN Q.921 User Adaptation Layer	Provides PRI/Q.921 signaling backhaul for call-agent applications using SCTP with the IDSN user adaptation (IUA) layer.	"Implementing SCTP Features" on page 155 of this guide
12.0(7)T	Fusion Call-Control Signaling (FCCS)—also known as NEC Fusion	Allows a voice network to integrate seamlessly into an IP network, enabling the addition of voice-networking capabilities to a LAN or WAN without major network restructuring.	"Implementing FCCS (NEC Fusion)" on page 233 of this guide

Overview of ISDN Voice Interfaces

This chapter provides an overview of ISDN Basic Rate Interface (BRI) and Primary Rate Interface (PRI) for support of voice traffic. With those ports so configured, you can do the following:

- Bypass PSTN tariffed services such as trunking and administration.
- Connect your PBXs directly to a Cisco router and route PBX station calls automatically to the WAN.
- Configure a voice interface on a Cisco router to emulate either a terminal-equipment (TE) or network-termination (NT) interface. All types of PBXs can send calls through a router and deliver those calls across the customer network.
- Configure Layer 2 operation as point-to-point (static terminal endpoint identifier [TEI]) or point-to-multipoint (automatic TEI).

Contents

Prerequisites for Configuring ISDN Voice Interfaces

- Obtain PRI or BRI service and T1 or E1 service from your service provider, as required. Ensure that the BRI lines are provisioned at the switch to support voice calls.
- Establish a working IP, Frame Relay, or ATM network. Ensure that at least one network module or WAN interface card is installed in the router to provide connection to the LAN or WAN.
- Complete your company's dial plan.
- Establish a working telephony network based on your company's dial plan and configure the network for real-time voice traffic. This chapter describes only a portion of the process; for further information, see the chapter "Cisco Voice Telephony."
- Cisco 2600 series and Cisco 3600 series routers—Install digital T1 or E1 packet-voice trunk network modules, BRI voice interface cards, and other voice interface cards as required on your network.
- Cisco 7200 series routers—Install a single-port 30-channel T1/E1 high-density voice port adapter.

- Cisco MC3810 multiservice concentrators—Install the required digital voice modules (DVMs), BRI voice module (BVM), and multiflex trunk modules.
- Configure, for all platforms (as required), the following:
  - Voice card and controller settings
  - Serial and LAN interfaces
  - Voice ports
  - Voice dial peers

Restrictions for Configuring ISDN Voice Interfaces

ISDN Voice Interface Limitations

- Basic-net3 and basic-qsig are the only ISDN switch types currently supported for an NT interface.
- When the ISDN BRI port on the router is configured as an NT port, you must use a "rolled" cable (one with the transmit and receive leads swapped) to connect to a TE interface.
- Layer 1 can be configured only as point-to-point (that is, with one TE connected to each NT). Automatic TEI support issues only one TEI.

QSIG Support Limitations

- Cisco 2600 series routers do not support VoATM.
- The following restrictions apply to the Cisco MC3810 multiservice concentrator:
  - QSIG data calls are not supported. All calls with bearer capability indicating a nonvoice type (such as for video telephony) are rejected.
  - Cisco MC3810 supports only one T1/E1 interface with direct connectivity to a private integrated services network exchange (PINX).
  - Cisco MC3810 supports a maximum of 24 B channels.
  - When QSIG is configured, serial port 1 does not support speeds higher than 192 kbps. This restriction assumes that the MFT is installed in slot 3 on the Cisco MC3810. If the MFT is not installed, then serial port 1 does not operate.
- The following restrictions apply to Cisco 7200 series routers:
  - VoATM is not supported.
  - BRI is not supported.

Information About ISDN Voice Interfaces

To configure ISDN voice interfaces, you should understand the following concepts:

- ISDN Media Types, page 5
- Interface Cards and Network Modules, page 5
- Typical ISDN Application, page 6
- QSIG Protocol, page 6
- Traceability of Diverted Calls, page 10

ISDN Media Types

Cisco routing devices support ISDN BRI and ISDN PRI. Both media types use bearer (B) channels and data (D) channels as follows:

- ISDN BRI (referred to as "2 B + D") uses the following:
  - Two 64-kbps B channels that carry voice or data for a maximum transmission speed of 128 kbps
  - One 16-kbps D channel that carries signaling traffic—that is, instructions about how to handle each of the B channels.
- ISDN PRI (referred to as "23 B + D" or "30 B + D") uses the following:
  - 23 B channels (in North America and Japan) or 30 B channels (in the rest of the world) that carry voice or data
  - One 64-kbps D channel that carries signaling traffic

The D channel, in its role as signal carrier for the B channels, directs the central-office switch to send incoming calls to particular timeslots on the Cisco access server or router. It also identifies the call as a circuit-switched digital call or an analog modem call. Circuit-switched digital calls are relayed directly to the ISDN processor in the router; analog modem calls are decoded and then sent to the onboard modems.

Interface Cards and Network Modules

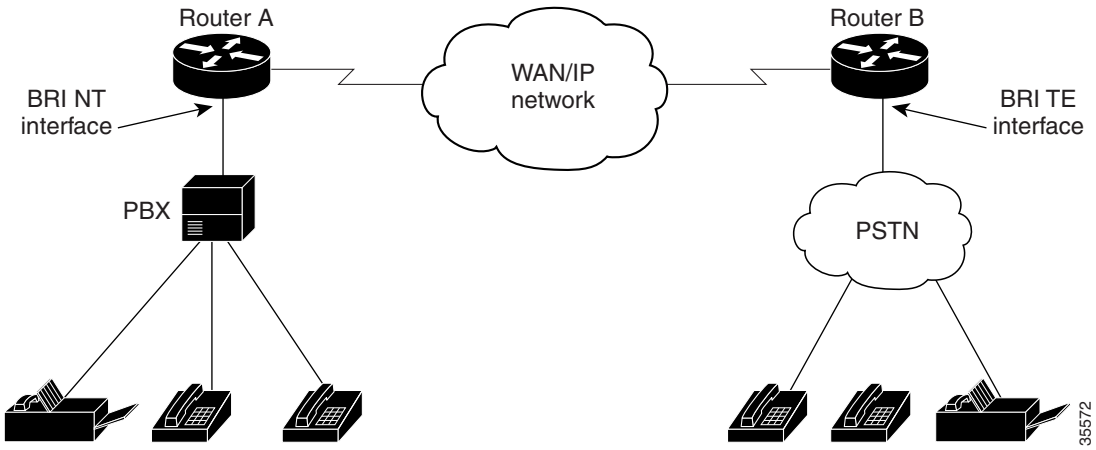
The VIC-2BRI-NT/TE voice interface card for the Cisco 2600 series and Cisco 3600 series routers and the BVM4-NT/TE voice module for the Cisco MC3810 multiservice concentrator enable Cisco IOS software to replicate the PSTN interface to a PBX that is compatible with European Telecommunications Standards Institute (ETSI) NET3 and QSIG switch types.

Before these cards and modules became available, if your PBXs implemented only a BRI TE interface, you had to make substantial hardware and software changes on the PBX to provide an NT interface to the router. provide an NT interface to the router. VIC-2BRI-NT/NE and BVN4-NT/NE allow you to connect ISDN PBXs and key systems to a multiservice network with minimal configuration changes on the PBX.

Typical ISDN Application

A typical application (see Figure 1) allows an enterprise customer with a large installed base of legacy telephony equipment to bypass the PSTN.

Figure 1 Typical Application Using BRI-NT/TE Voice Interface Cards or BVM4-NT/TE Voice Modules



QSIG Protocol

This section contains the following information:

- QSIG Basics, page 6
- ISDN Switch Types for Use with QSIG, page 9

QSIG Basics

QSIG is a variant of ISDN Q.921 and Q.931 ISDN D-channel signaling, for use in private integrated-services network-exchange (PINX) devices such as PBXs or key systems. Using QSIG signaling, a router can route incoming voice calls from a PINX across a WAN to a peer router, which can then transport the signaling and voice packets to another PINX.

The QSIG protocol was originally specified by European Computer Manufacturers Association (ECMA), and then adopted by European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO). It is becoming the standard for PBX interoperability in Europe and North America.

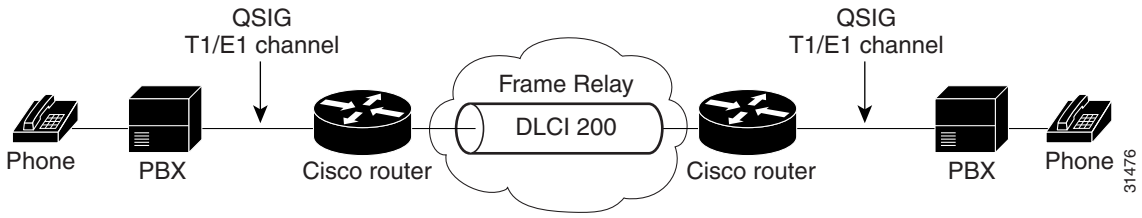
Table 1 identifies the ECMA standards and the OSI layer of the QSIG protocol stack to which they relate.

Table 1 QSIG Protocol Stack

OSI Layer	Standard	Description
7 to 4	Application mechanisms	End-to-end protocols; network transparent
3	Multiple ECMA standards	Standards for supplementary services and advanced network features
	ECMA-165	QSIG generic functional procedures
	ECMA-142/143	QSIG basic call
2	ECMA-141	Interface-dependent protocols
1	I.430 / I.431	PRI and BRI

QSIG enables Cisco networks to emulate the functionality of the PSTN. A Cisco device routes incoming voice calls from a PINX across a WAN to a peer device, which then transports the signaling and voice packets to a second PINX (see Figure 2).

Figure 2 QSIG Signaling



The Cisco voice-packet network appears to the QSIG PBXs as a distributed transit PBX that can establish calls to any PBX, non-QSIG PBX, or other telephony endpoint served by a Cisco gateway, including non-QSIG endpoints.

QSIG messages that originate and terminate on QSIG endpoints pass transparently across the network; the PBXs process and provision any supplementary services. When endpoints are a mix of QSIG and non-QSIG, only basic calls that do not require supplementary services are supported.

QSIG signaling provides the following benefits:

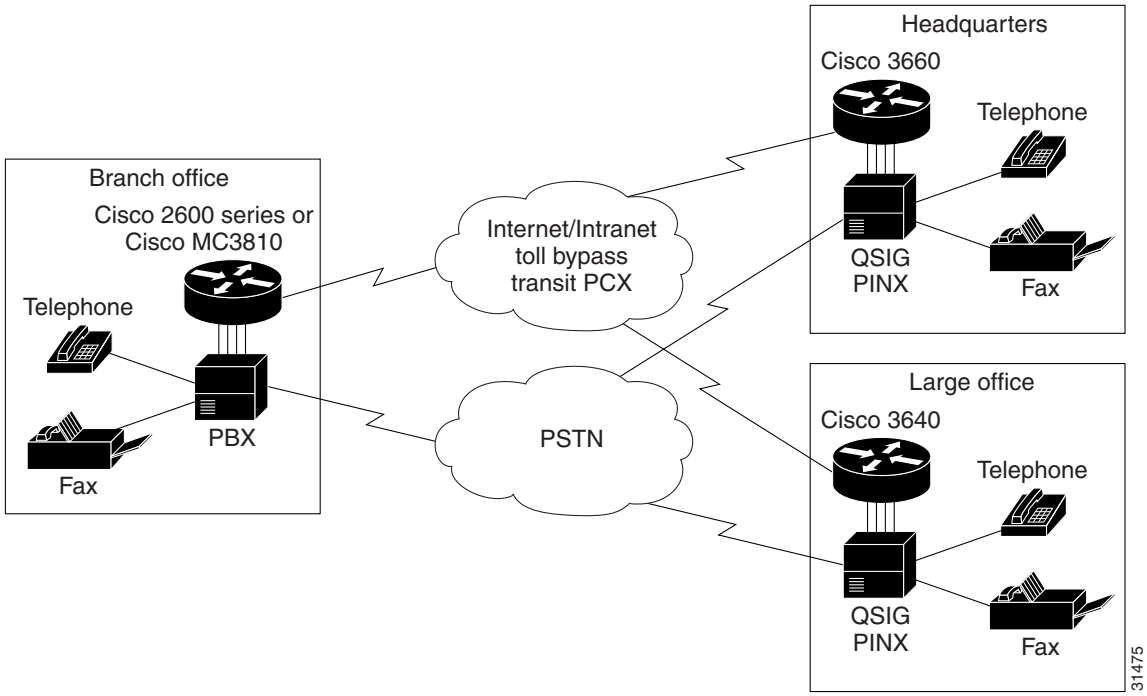
- It provides efficient and cost-effective telephony services on permanent (virtual) circuits or leased lines.
- It allows enterprise networks that include PBX networks to replace leased voice lines with a Cisco WAN.
- It eliminates the need to route connections through multiple tandem PBX hops to reach the desired destination, thereby saving bandwidth, PBX hardware, and switching power.
- It improves voice quality through the single-hop routing provided by voice switching while allowing voice to be compressed more aggressively, resulting in additional bandwidth savings.
- It supports PBX feature transparency across a WAN, permitting PBX networks to provide advanced features such as calling name and number display, camp-on/callback, network call forwarding, centralized attendant, and centralized message waiting. Usually these capabilities are available on only a single site where users are connected to the same PBX.

QSIG support enables the following:

- Digit forwarding on POTS dial peers
- On Cisco 2600 series, QSIG-switched calls over VoFR and VoIP for T1/E1 and BRI voice interface cards
- On Cisco 3600 series, QSIG-switched calls over VoFR, VoIP, and VoATM for T1/E1 and BRI voice interface cards
- On Cisco 7200 series, QSIG-switched calls over VoFR and VoIP on T1/E1 voice interface cards
- On Cisco MC3810, T1 or E1 PRI and BRI QSIG-switched calls over VoFR, VoIP, and VoATM for Cisco MC3810 digital voice modules and BRI voice module.

Figure 3 shows an example of how QSIG support can enable toll bypass.

Figure 3 QSIG Toll-Bypass Application



ISDN Switch Types for Use with QSIG

You can configure QSIG at either the global configuration level or the interface configuration level. To do so requires that you know your switch type. Available types are shown in Table 2.

Table 2 ISDN Central-Office Switch Types

Country	ISDN Switch Type	Description
Australia	basic-ts013	Australian TS013 switches
Europe	basic-1tr6	German 1TR6 ISDN switches
	basic-nwnet3	Norwegian NET3 ISDN switches (phase 1)
	basic-net3	NET3 ISDN switches (United Kingdom and others)
	vn2	French VN2 ISDN switches
	vn3	French VN3 ISDN switches
Japan	ntt	Japanese NTT ISDN switches
New Zealand	basic-nznet3	New Zealand NET3 switches
North America	basic-5ess	Lucent Technologies basic rate switches
	basic-dms100	NT DMS-100 basic rate switches
	basic-ni1	National ISDN-1 switches

Table 3 lists the ISDN service-provider BRI switch types.

Table 3 ISDN Service-Provider BRI Switch Types

ISDN Switch Type	Description
basic-1tr6	German 1TR6 ISDN switches
basic-5ess	Lucent Technologies basic rate switches
basic-dms100	NT DMS-100 basic rate switches
basic-net3	NET3 (TBR3) ISDN, Norway NET3, and New Zealand NET3 switches. (This switch type covers the Euro-ISDN E-DSS1 signaling system and is ETSI-compliant.)
basic-ni1	National ISDN-1 switches
basic-nwnet3	Norwegian NET3 ISDN switches (phase 1)
basic-nznet3	New Zealand NET3 switches
basic-qsig	PINX (PBX) switches with QSIG signaling in compliance with Q.931
basic-ts013	Australian TS013 switches
ntt	Japanese NTT ISDN switches
vn2	French VN2 ISDN switches
vn3	French VN3 ISDN switches

Cisco platforms that support Q.931 offer both user-side and network-side switch types for ISDN call processing, providing the following benefits:

- User-side PRI enables the Cisco device to provide a standard ISDN PRI user-side interface to the PSTN.
- Network-side PRI enables the Cisco device to provide a standard ISDN PRI network-side interface via digital T1/E1 packet voice trunk network modules on Cisco 2600 series and Cisco 3600 series routers.

Traceability of Diverted Calls

European Telecommunication Standard ETSI 300 207-1 specifies that calls must be traceable if diverted. This requires that a VoIP call, when diverted, must translate into divertingLegInformation2 instead of Redirection IE. Cisco's ISDN implementation satisfies this requirement.

Additional References

The following sections provide references related to ISDN.

Note

- In addition to the references listed below, each chapter provides additional references related to ISDN.
- Some of the products and services mentioned in this guide may have reached end of life, end of sale, or both. Details are available at http://www.cisco.com/en/US/products/prod_end_of_life.html.

Related Documents

Related Topic	Document Title
AIM, ATM, and IMA	• *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04gin.htm • *ATM Software Segmentation and Reassembly (SAR)* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_t1atm.htm • *Cisco IOS Wide-Area Networking Configuration Guide, c*hapter on configuring ATM at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfatm.htm • *Installing the High Performance ATM Advanced Integration Module in Cisco 2600 Series Routers* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/aim_inst/aim_inst.htm

Related Topic	Document Title
Basic router configuration	• Cisco 2600 series documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm • Cisco 3600 series documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm • Cisco 3700 series documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/index.htm • Cisco AS5300 documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm
Cisco IOS command references	• *Cisco IOS Debug Command Reference, Release 12.3T* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123dbr/index.htm • *Cisco IOS Voice Command Reference, Release 12.3T* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tvr/index.htm
Cisco IOS configuration fundamentals and examples	• *Cisco IOS Configuration Fundamentals Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ • *Cisco IOS Interface Command Reference* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/index.htm • *Cisco IOS Interface Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/ • Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html From the website, select a technology category and subsequent hierarchy of subcategories, then click **Technical Documentation > Configuration Examples**.
Cisco IOS Voice Configuration Library, including library preface and glossary	• Cisco IOS Voice Configuration Library at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm
Clock sources	• *Cisco IOS Voice, Video, and Fax Configuration Guide* chapter on configuring voice ports at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfport.htm#18533
ISDN basics	• Cisco IOS Release 12.2 Configuration Guides and Command References library at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ • Cisco IOS Release 12.3 Configuration Guides and Command References library at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm
ISDN cause codes	• *ISDN Switch Types, Codes, and Values* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm

Related Topic	Document Title
ISDN configuration	• *Cisco IOS Voice, Video, and Fax Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfisdn.htm • *ISDN Basic Rate Service Setup Commands* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_r/drprt1/drbri.htm
ISDN interfaces for voice	• *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines* at http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/config/ • *Cisco MC3810 Multiservice Concentrator Hardware Installation* at http://www.cisco.com/univercd/cc/td/doc/product/access/multicon/3810hwig/ • *Quick Start Guide: Cisco MC3810 Installation and Startup* at http://www.cisco.com/univercd/cc/td/doc/product/access/multicon/3810qsg.htm • *Voice over IP for the Cisco 3600 and Cisco 2600 Series* at http://cco-rtp-1.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip3600/index.htm
ISDN network modules and interface cards	• *Cisco Network Modules Hardware Installation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/ • *Cisco WAN Interface Cards Hardware Installation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/wan_mod/ • *Installing and Configuring 1-Port J1 Voice Interface Cards* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/hw_inst/hw_notes/j1vwic.htm • *Update to Cisco WAN Interface Cards Hardware Installation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wan_updt.htm • *Voice Network Module and Voice Interface Card Configuration Note* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/voice/4712voic.htm
MIX module	• *Multiservice Interchange (MIX) for Cisco 2600 and 3600 Series Multiservice Platforms* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mix.htm
RADIUS VSA configuration	• *RADIUS VSA Voice Implementation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm
SCTP	• *Stream Control Transfer Protocol (SCTP)* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sctp2.htm
Security	• *Cisco IOS Security Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm

Related Topic	Document Title
SS7 for voice gateways	• *Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/gateway/dascfg5.htm
Tcl IVR programming	• *Tcl IVR API Version 2.0 Programmer's Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/index.htm
Troubleshooting	• *Cisco IOS Debug Command Reference, Release 12.3T* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123dbr/index.htm • *Cisco IOS Voice Troubleshooting and Monitoring Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/voipt_c/index.htm • *Internetwork Troubleshooting Guide* at http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm • *Voice over IP Troubleshooting and Monitoring* at http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/voipt_c/index.htm
VoATM configuration	• *Configuring AAL2 and AAL5 for the High-Performance Advanced Integration Module on the Cisco 2600 Series* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_ataim.htm
VoIP configuration	• *Voice over IP for the Cisco 2600/3600 Series* at http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip3600/index.htm • *Voice over IP for the Cisco AS5300* at http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip5300/index.htm • *Voice over IP for the Cisco AS5800* at http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip5800/index.htm
WAN configuration	• *Cisco IOS Wide-Area Networking Command Reference* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_r/index.htm • *Cisco IOS Wide-Area Networking Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfatm.htm

Standards

Standards	Title
014-0018-04.3D-ER	*CPE Requirements for MCI ISDN Primary Rate Interface,* revision 4.3D, February 10, 1998
ETSI 300 207-1	*Integrated Services Digital Network (ISDN): Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification*, December 1994

Standards	Title
TR-41459	*AT&T Network ISDN Primary Rate Interface and Special Applications Specifications, User-Network Interface*, 1999
TTC JJ-20.10 to JJ-20.12	*PBX*

MIBs

MIBs	MIBs Link
• CISCO-CAS-IF-MIB.my • CISCO-ICSUDSU-MIB • RFC 1407 MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
SCTP	*Stream Control Transmission Protocol (SCTP), Release 2*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Basic ISDN Voice-Interface Configuration

This chapter describes how to configure ISDN BRI and PRI ports to support voice traffic.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 64.

Contents

Prerequisites for Configuring an ISDN Voice Interface

- Perform the prerequisites that are listed in the "Prerequisites for Configuring ISDN Voice Interfaces" section on page 3.
- Obtain PRI or BRI service and T1 or E1 service from your service provider, as required. Ensure that the BRI lines are provisioned at the switch to support voice calls.
- Establish a working IP, Frame Relay, or ATM network. Ensure that at least one network module or WAN interface card is installed in the router to provide connection to the LAN or WAN.
- Complete your company's dial plan.
- Establish a working telephony network based on your company's dial plan and configure the network for real-time voice traffic.

- Cisco 2600 series and Cisco 3600 series—Install digital T1 or E1 packet-voice trunk network modules, BRI voice interface cards, and other voice interface cards as required on your network.
- Cisco 7200 series—Install a single-port 30-channel T1/E1 high-density voice port adapter.
- Cisco MC3810—Install the required digital voice modules (DVMs), BRI voice module (BVM), and multiflex trunk modules.
- Configure, for all platforms (as required), the following:
  - Voice card and controller settings
  - Serial and LAN interfaces
  - Voice ports
  - Voice dial peers

Restrictions for Configuring an ISDN Voice Interface

Restrictions are described in the "Restrictions for Configuring ISDN Voice Interfaces" section on page 4.

Information About ISDN Voice Interfaces

General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

How to Configure an ISDN Voice Interface

This section contains the following procedures:

Configuring a Router for ISDN BRI Voice-Interface Support

This section contains the following procedures:

Configure BRI NT and TE Interfaces

To configure BRI NT and TE interfaces, perform the following steps.

Note Set up each channel for either user side or network side.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn switch-type**
4. **interface bri**
5. **no ip address**
6. **isdn overlap-receiving**
7. **isdn twait-disable**
8. **isdn spid1**
9. **isdn spid2**
10. **isdn incoming-voice**
11. **shutdown**
12. **isdn layer1-emulate**
13. **no shutdown**
14. **network-clock-priority**
15. **line-power**
16. **isdn protocol-emulate**
17. **isdn sending-complete**
18. **isdn static-tei**
19. **isdn point-to-point-setup**
20. **exit**
21. **clear interface bri**
22. Repeat for other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.

	Command or Action	Purpose
Step 3	**isdn switch-type** *switch-type* **Example:** `Router(config)# isdn switch-type basic-qsig`	Configures the telephone-company ISDN switch type. Table 3 on page 9 shows a list of switch types. **Note** The only switch types currently supported for an NT interface are basic-net3 and basic-qsig.
Step 4	**Cisco MC3810** **interface bri** *number* **Other Supported Routers** **interface bri** *slot/port* **Example:** `Router(config)# interface bri 1/1`	Enters interface configuration mode for the specified port, connector, or interface card number (location of voice module) or slot/port (location of voice network module and voice interface card).
Step 5	**no ip address** **Example:** `Router(config-if)# no ip address`	Specifies that there is no IP address for this interface.
Step 6	**isdn overlap-receiving** **Example:** `Router(config-if)# isdn overlap-receiving`	(Optional) Activates overlap signaling to send to the destination PBX. In this mode, the interface waits for possible additional call-control information.
Step 7	**isdn twait-disable** **Example:** `Router(config-if)# isdn twait-disable`	(Optional) Delays a national ISDN BRI switch for a random length of time before activating the Layer 2 interface at switch startup. Use this command when the ISDN switch type is basic-ni1. Twait time is enabled by default.
Step 8	**isdn spid1** *spid-number* [*ldn*] **Example:** `Router(config-if)# isdn spid1 40855501220101`	(Optional; TE only) Service-profile identifier (SPID) and optional local directory number for the B1 channel. Currently, only DMS-100 and NI-1 switch types require SPIDs. Although some switch types might support a SPID, Cisco recommends that you set up ISDN service without SPIDs.
Step 9	**isdn spid2** *spid-number* [*ldn*] **Example:** `Router(config-if)# isdn spid2 40855501220102`	(Optional; TE only) Specifies SPID and optional local directory number for the B2 channel.
Step 10	**isdn incoming-voice** {**voice** | **modem**} **Example:** `Router(config-if)# isdn incoming-voice voice`	Configures the port to treat incoming ISDN voice calls as voice calls that are handled by either a modem or a voice DSP, as directed by the call-switching module.
Step 11	**shutdown** **Example:** `Router(config-if)# shutdown`	Turns off the port (before setting port emulation).

	Command or Action	Purpose

Step 12	**isdn layer1-emulate user**
	or
	isdn layer1-emulate network
	Example:
	`Router(config-if)# isdn layer1-emulate user`
	or
	Example:
	`Router(config-if)# isdn layer1-emulate network`
		(User side only) Configures Layer 1 port mode emulation and clock status for the user—that is, the TE (clock slave).
		or
		(Network side only) Configures Layer 1 port mode emulation and clock status for the network—that is, the NT (clock master).

Step 13	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Turns on the port.
Step 14	**network-clock-priority** {**low** | **high**} **Example:** `Router(config-if)# network-clock-priority low`	(Optional; TE only) Sets priority for recovering clock signal from the network NT device for this BRI voice port. Keywords are as follows: • **high**—First priority (default for BRI voice interface cards) • **low**—Low priority (default for BRI voice modules) **Note** Do not use this command if the port is configured as NT in Step 12.
Step 15	**Cisco MC3810 Only** **line-power** **Example:** `Router(config-if)# line-power`	Turns on the power supplied from an NT-configured port to a TE device.

Step 16	**isdn protocol-emulate user**
	or
	isdn protocol-emulate network
	Example:
	`Router(config-if)# isdn protocol-emulate user`
	or
	Example:
	`Router(config-if)# isdn protocol-emulate network`
		(User side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the user—that is, the TE (clock master).
		or
		(Network side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the network—that is, the NT (clock slave).

	Command or Action	Purpose
Step 17	**isdn sending-complete** **Example:** `Router(config-if)# isdn sending-complete`	(Optional) Configures the voice port to include the "Sending Complete" information element in the outgoing call-setup message. This command is used in some geographic locations, such as Hong Kong and Taiwan, where the "Sending Complete" information element is required in the outgoing call setup message.
Step 18	**isdn static-tei** *tei-number* **Example:** `Router(config-if)# isdn static-tei 0`	(Optional) Configures a static ISDN Layer 2 terminal endpoint identifier (TEI).
Step 19	**isdn point-to-point-setup** **Example:** `Router(config-if)# isdn point-to-point-setup`	(Optional) Configures the ISDN port to send SETUP messages on the static TEI (point-to-point link). **Note** A static TEI must be configured in order for this command to be effective.
Step 20	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.
Step 21	**Cisco MC3810** **clear interface bri** *number* **Other Supported Routers** **clear interface bri** *slot/port* **Example:** `Router# clear interface bri 1/1`	(Optional) Resets the specified port, connector, or interface card number (location of voice module) or slot/port (location of voice network module and voice interface card). The interface needs to be reset if the static TEI number was configured in Step 18.
Step 22	Repeat the appropriate steps for the other BRI NT/TE interfaces.	—

Note To complete voice configuration, set up your voice ports and dial peers.

Verify BRI Interfaces

To verify BRI interfaces, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show controllers bri**
2. **show interfaces bri**
3. **show isdn** {**active** | **history**}
4. **show isdn** {**memory** | **status** | **timers**}
5. **show isdn status**

6. **show running-config**
7. **show voice port**

DETAILED STEPS

Step 1 **show controllers bri** *number* or **show controllers bri** *slot/port*

Use this command to display information about the specified BRI port, connector, or interface card number (location of voice module) or slot/port (location of voice network module and voice interface card).

Step 2 **show interfaces bri**

Use this command to display information about the physical attributes of the BRI B and D channels. In the output, look for the term *spoofing*, which indicates that the interface presents itself to the Cisco IOS software as operational.

Step 3 **show isdn** {**active** [*serial-number*] | **history** [*serial-number*]}

Use this command to display current (**active** keyword) or both historic and current (**history** keyword) call information for all ISDN interfaces or, optionally, a specific ISDN PRI interface (created and configured as a serial interface). Information displayed includes called number, remote node name, seconds of connect time, seconds of connect time remaining, seconds idle, and advice of charge (AOC) charging time units used during the call.

Step 4 **show isdn** {**memory** | **status** | **timers**}

Use this command to display information about memory, status, and Layer 2 and Layer 3 timers.

Step 5 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 6 **show running-config**

Use this command to display basic router configuration.

Step 7 **show voice port** [*slot/port* | **summary**]

Use this command to display information about BRI voice ports.

Examples

This section provides the following output examples:

- Sample Output for the show running-config Command, page 21
- Sample Output for the show interfaces bri Command, page 24

Sample Output for the show running-config Command

The following is sample output from a Cisco 2600 series system. Note that BRI1/0 and BRI1/1 are configured as ISDN user side and BRI2/0 and BRI2/1 are configured as ISDN network side. Table 4 describes significant fields shown in this output

```
Router# show running-config

Building configuration...
Current configuration:
```

```
!
version 12.2
!
no service udp-small-servers
service tcp-small-servers
!
hostname Router
!
username xxxx password x 11x5xx07
no ip domain-lookup
ip host Labhost 172.22.66.11
ip host Labhost2 172.22.66.12
ip name-server 172.22.66.21
!
.
.
.
interface BRI1/0
no ip address
no ip directed-broadcast
isdn switch-type basic-net3
isdn overlap-receiving
isdn T306 30000
isdn skipsend-idverify
isdn incoming-voice voice
!
interface BRI1/1
no ip address
no ip directed-broadcast
isdn switch-type basic-net3
isdn overlap-receiving
isdn T306 30000
isdn skipsend-idverify
isdn incoming-voice voice
!
interface BRI2/0
no ip address
isdn switch-type basic-net3
isdn overlap-receiving
isdn protocol-emulate network
isdn layer1-emulate network
isdn T306 30000
isdn sending-complete
isdn skipsend-idverify
isdn incoming-voice voice
!
interface BRI2/1
no ip address
isdn switch-type basic-net3
isdn overlap-receiving
isdn protocol-emulate network
isdn layer1-emulate network
isdn T306 30000
isdn sending-complete
isdn skipsend-idverify
isdn incoming-voice voice
!
.
.
.
```

The following is sample output from a Cisco MC3810 system. Table 4 describes significant fields shown in this output.

```
Router# show running-config

Building configuration...
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging console
!
network-clock base-rate 56k
network-clock-select 2 T1 0
network-clock-select 3 system(SCB)
network-clock-select 1 BVM
ip subnet-zero
!
isdn switch-type basic-net3
isdn voice-call-failure 0
call rsvp-sync
!
voice-card 0
!
controller T1 0
 mode atm
 framing esf
 linecode b8zs
!
interface BRI1
no ip address
isdn switch-type basic-net3
isdn protocol-emulate network
isdn layer1-emulate network
isdn incoming-voice voice
isdn T306 30000
isdn skipsend-idverify
no cdp enable
!
interface BRI2
no ip address
isdn switch-type basic-net3
isdn protocol-emulate network
isdn layer1-emulate network
isdn incoming-voice voice
isdn T306 30000
isdn skipsend-idverify
no cdp enable
!
interface BRI3
no ip address
shutdown
network-clock-priority low
isdn switch-type basic-net3
isdn T306 30000
no cdp enable
!
interface BRI4
no ip address
shutdown
network-clock-priority low
isdn switch-type basic-net3
```

```
isdn T306 30000
no cdp enable
!
.
.
.
```

Table 4 describes significant fields shown in these outputs.

Table 4 Significant Fields from the show running-config Command

Field	Description
isdn T306 *timer-value*	Value of the T306 timer, in ms. An ISDN timer is started when a Q.931 Disconnect message with progress indicator number 8 is sent. The timer is stopped when a ISDN Release/Disconnect message is received from the other end. The call clears on expiration of the T306 timer.
isdn T310 *timer-value*	Value of the T310 timer, in ms. An ISDN timer is started when a Q.931 Call Proceeding message is received. The timer is stopped when a Q.931 Alerting/Connect/Disconnect message is received from the other end. The call clears on expiration of the T310 timer.

Sample Output for the show interfaces bri Command

The following shows sample output for a Cisco 2610. Table 5 describes significant fields shown in this output.

```
Router# show interfaces bri 1/0

BRI3/1 is up, line protocol is up (spoofing)
  Hardware is Voice NT or TE BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation VOICE, loopback not set
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     26110 packets input, 104781 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 output buffer failures, 0 output buffers swapped out
     9 carrier transitions
```

The following shows sample output for a Cisco MC3810. Table 5 describes significant fields shown in this output.

```
Router# show interfaces bri 1

BRI1 is up, line protocol is up (spoofing)
  Hardware is BVM
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Last input 19:32:19, output 19:32:27, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
   Conversations  0/1/16 (active/max active/max total)
   Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   13282 packets input, 53486 bytes, 0 no buffer
   Received 1 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   13292 packets output, 53515 bytes, 0 underruns
   0 output errors, 0 collisions, 4 interface resets
   0 output buffer failures, 0 output buffers swapped out
   33 carrier transitions
```

Table 5 Significant Fields from the show interfaces bri Command

Field (in alpha order)	Description
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
BRI... is {up | down | administratively down}	Whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator.
broadcasts	Total number of broadcast or multicast packets received by the interface.
BW	Bandwidth of the interface in kbps.
bytes	Total number of bytes, including data and media access control (MAC) encapsulation, in the error-free packets sent or received by the system.
carrier transitions	Number of times that the carrier detect signal of a serial interface has changed state. Check for modem or line problems if the carrier detect line is changing state often.
collisions	Number of collisions. These can occur when you have several devices connected on a multiport line.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
DLY	Delay of the interface in microseconds.
encapsulation	Encapsulation method assigned to interface.
five-minute input/output rate	Average number of bits and packets transmitted per second in the last 5 minutes.
frame	Number of packets that are received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.

Table 5 Significant Fields from the show interfaces bri Command (continued)

Field (in alpha order)	Description
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
Hardware is...	Hardware type.
ignored	Number of received packets that are ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can increase the ignored count.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so this sum may not balance with the other counts.
input/output queue, drops	Number of packets in output and input queues. Each number is followed by a slash (/), the maximum size of the queue, and the number of packets dropped due to a full queue.
interface resets	Number of times that an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system recognizes that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
Internet address is...	IP address and subnet mask, followed by packet size.
keepalive	Whether keepalives are set.
last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a nonfunctioning interface failed.
line protocol is {up | down | administratively down}	Whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful).
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
loopback	Whether loopback is set.
MTU	Maximum transmission unit of the interface.
no buffer	Number of received packets that are discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.

Table 5 Significant Fields from the show interfaces bri Command (continued)

Field (in alpha order)	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
output/input queue, drops	Number of packets in output and input queues. Each number is followed by a slash (/), the maximum size of the queue, and the number of packets dropped due to a full queue.
overrun	Number of times that the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
packets input/output	Total number of error-free packets received or sent by the system.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
restarts	Number of times that the controller was restarted because of errors
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.

Troubleshooting Tips

- Use the **debug isdn q921** command to display Layer 2 access procedures that are taking place at the router on the D channel (LAPD) of its ISDN interface.
- Use the **debug isdn q931** command to display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network.
- For information on these and additional **debug** commands, see the following references:
  - *Cisco IOS Debug Command Reference, Release 12.3T* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123dbr/index.htm
  - *Cisco IOS Voice Troubleshooting and Monitoring Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/voipt_c/index.htm

Configuring ISDN PRI Voice-Interface Support

This section contains the following procedures:

Configure PRI Interfaces

To configure PRI interfaces, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn switch-type**
4. **controller**
5. **description**
6. **framing esf**
7. **linecode**
8. **pri-group timeslots**
9. **exit**
10. **interface serial**
11. **isdn incoming-voice modem**
12. **description**
13. **isdn-bchan-number-order**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.

	Command or Action	Purpose
Step 3	**isdn switch-type** *switch-type* **Example:** `Router(config)# isdn switch-type basic-qsig`	Configures the telephone company ISDN switch type. Table 3 on page 9 shows a list of switch types. **Note** The only switch types currently supported for an NT interface are basic-net3 and basic-qsig.
Step 4	**Cisco AS5300** **controller** {**t1** | **e1**} **0** **Cisco AS5800 (T1 card)** **controller t1 1/0/0** **Cisco AS5800 (T3 card)** **controller t1 1/0/0:1** **Example:** `Router(config)# controller t1 1/0/0`	Enters T1/E1 controller configuration mode for the specified (as appropriate) dial shelf, slot, port (or T3 port), and timeslot as follows: • Cisco AS5300: T1 0 or E1 0 controller • Cisco AS5800 (T1 card): T1 0 controller • Cisco AS5800 (T3 card): T1 1 controller
Step 5	**description** *string* **Example:** `Router(config-if)# description interface01`	Includes a specific description about the digital signal processor (DSP) interface.
Step 6	**framing esf** **Example:** `Router(config-controller)# framing esf`	Defines the framing characteristics.
Step 7	**linecode** {**ami** | **b8zs** | **hdb3**} **Example:** `Router(config-controller)# linecode ami`	Sets the line-encoding method to match that of your telephone-company service provider. Keywords are as follows: • **ami**—Alternate mark inversion (AMI), valid for T1 or E1 controllers. Default for T1 lines. • **b8zs**—B8ZS, valid for T1 controllers only. • **hdb3**—High-density bipolar 3 (hdb3), valid for E1 controllers only. Default for E1 lines.
Step 8	**pri-group timeslots** *range* **Example:** `Router(config-controller)# pri-group timeslots 1-23`	Specifies PRI on the specified or timeslots that make up the PRI group. Maximum T1 range: 1 to 23. Maximum E1 range: 1 to 31. Separate low and high values with a hyphen. **Note** You can configure the PRI group to include all available timeslots, or you can configure a select group of timeslots for the PRI group.
Step 9	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

	Command or Action	Purpose
Step 10	**Cisco AS5300** **interface serial 0:***channel-number* **Cisco AS5800** **interface serial 1/0:***channel-number* **Example:** `Router(config)# interface serial 0:23`	Enters interface configuration mode for the specified PRI slot/port and D-channel ISDN interface. D-channel ISDN interface is (for T1) 23 and (for E1) 15.
Step 11	**isdn incoming-voice modem** **Example:** `Router(config-if)# isdn incoming-voice modem`	Enables incoming ISDN voice calls. The **modem** keyword specifies that incoming voice calls are passed over to digital modems, where they negotiate the appropriate modem connection with the far-end modem. Its use here is required.
Step 12	**description** *string* **Example:** `Router(config-if)# description interface02`	Includes a specific description about the digital signal processor (DSP) interface.
Step 13	**isdn-bchan-number-order** {**ascending** | **descending**} **Example:** `Router(config-if)# isdn-bchan-number-order descending`	Configures an ISDN PRI interface to make outgoing call selection in ascending or descending order—that is, to select the lowest or highest available B channel starting at either channel B1 (ascending) or channel B23 for a T1 and channel B30 for an E1 (descending). Default: descending. **Note** Before configuring ISDN PRI on your router, check with your service vendor to determine if ISDN trunk call selection is configured for ascending or descending order. A mismatch between router and switch causes the switch to send an error message stating that the channel is not available.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure PRI Voice Ports

Under most circumstances, default voice-port command values are adequate to configure voice ports to transport voice data over your existing IP network. However, because of the inherent complexities of PBX networks, you might need to configure specific voice-port values, depending on the specifications of the devices in your network.

Verify PRI Interfaces

To verify PRI interfaces, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show isdn** {**active** | **history**}

2. **show isdn status**
3. **show vfc version**
4. **show voice port**

DETAILED STEPS

Step 1 **show isdn** {**active** [*serial-number*] | **history** [*serial-number*]}

Use this command to display current (**active** keyword) or both historic and current (**history** keyword) call information for all ISDN interfaces or, optionally, a specific ISDN PRI interface (created and configured as a serial interface). Information displayed includes called number, remote node name, seconds of connect time, seconds of connect time remaining, seconds idle, and advice of charge (AOC) charging time units used during the call.

Step 2 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 3 **show vfc** *slot* **version**

Use this command to display the version of software residing on the voice feature card in the specified slot.

Step 4 **show voice port** [*slot*/*port* | **summary**]

Use this command to display configuration information about a specific voice port.

Troubleshooting Tips

- Verify that you have dial tone and connectivity.
- If you have not configured your device to support Direct Inward Dialing (DID), do the following:
  1. Dial in to the router and verify that you have dial tone.
  2. Enter a dual-tone multifrequency (DTMF) digit. If dial tone stops, you have verified two-way voice connectivity with the router.
- If you have trouble connecting a call and suspect that the problem is associated with voice-port configuration, do the following:
  1. Confirm connectivity by pinging the associated IP address.

     Note For more information, see the *Cisco IOS IP Configuration Guide* chapter on configuring IP.

  2. Determine if the voice feature card (VFC) is installed correctly.

     Note For more information, see the instructions that came with your voice network module.

  3. Ensure that your (T1-line) a-law or (E1-line) mu-law setting is correct.
- If dialing cannot occur, use the **debug isdn q931** command to check the ISDN configuration.

Note For T1 troubleshooting information, see http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a5f40.shtml

Configuring QSIG Support

This section contains the following procedures:

- Configure Global QSIG Support for BRI or PRI, page 32
- Configure Controllers for QSIG over PRI, page 33 (required for PRI)
- Configure PRI Interfaces for QSIG, page 34 (required for PRI)
- Configure BRI Interfaces for QSIG, page 36 (required for BRI)
- Verify the QSIG Configuration, page 39 (required)

Configure Global QSIG Support for BRI or PRI

To configure global QSIG support for BRI or PRI, perform the following steps.

Note For additional guidance on switch-type configuration, see the "ISDN Switch Types for Use with QSIG" section on page 9.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn switch-type**
4. **dspint dspfarm**
5. **card type**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.

	Command or Action	Purpose
Step 3	**BRI on Cisco MC3810, Cisco 2600 Series, and Cisco 3600 Series** **isdn switch-type basic-qsig** **PRI on Any Supported Router** **isdn switch-type primary-qsig** **Example:** `Router(config)# isdn switch-type basic-qsig`	(Optional) Configures the global ISDN switch type to support QSIG signaling. Table 2 on page 9 shows a list of switch types. **Note** You can configure all interfaces at once by using this command in global configuration mode. Or you can configure one interface at a time by using this command in interface configuration mode.
Step 4	**BRI or PRI on Cisco 7200 Series** **dspint dspfarm** *slot/port* **Example:** `Router(config)# dspint dspfarm 1/1`	Configures the digital signal processor (DSP) farm at the specified slot/port.
Step 5	**BRI or PRI on Cisco 7200 Series** **card type** {**t1** | **e1**} *slot* **Example:** `Router(config)# card type t1 0`	Configures card type (T1 or E1) at the specified slot.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configure Controllers for QSIG over PRI

To configure controllers for QSIG over PRI, perform the following steps.

Note Steps in this section apply to PRI only, and not to BRI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **pri-group timeslots**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**Cisco MC3810** **controller** {**t1** | **e1**} *controller-number* **Other Supported Routers** **controller** {**t1** | **e1**} *slot*/*port* **Example:** `Router(config)# controller t1 1/1`	Enters T1 or E1 controller configuration mode for the specified controller number o r slot/port. **Note** Cisco MC3810 supports QSIG only on controller 1.
Step 4	**pri-group timeslots** *range* **Example:** `Router(config-controller)# pri-group timeslots 1-23`	Specifies PRI on the specified or timeslots that make up the PRI group. Maximum T1 range: 1-23. Maximum E1 range: 1-31. Separate low and high values with a hyphen. **Note** You can configure the PRI group to include all available timeslots, or you can configure a select group of timeslots for the PRI group.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure PRI Interfaces for QSIG

To configure PRI interfaces for QSIG, perform the following steps.

Note Set up each channel for either user side or network side.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial**
4. **isdn switch-type primary-qsig**
5. **isdn contiguous-bchan**
6. **isdn protocol-emulate**

7. **isdn overlap-receiving**
8. **isdn network-failure-cause**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**Cisco MC3810** **interface serial 1:***channel-number* **Other Supported Routers** **interface serial** *slot*/*port*:*channel-number* **Example:** `Router(config)# interface serial 1/1:23`	Enters interface configuration mode for the specified PRI slot/port and D-channel ISDN interface. D-channel ISDN interface is (for T1) 23 and (for E1) 15.
Step 4	**isdn switch-type primary-qsig** **Example:** `Router(config-if)# isdn switch-type primary-qsig`	If you did not configure the global PRI ISDN switch type for QSIG support in global configuration mode, configures the interface ISDN switch type to support QSIG signaling. Conditions that apply to this command in global configuration mode also apply in interface configuration mode. For more information, see the "ISDN Switch Types for Use with QSIG" section on page 9. **Note** For this interface, this interface configuration command overrides the setting of the **isdn switch-type** command entered in global configuration mode.
Step 5	**isdn contiguous-bchan** **Example:** `Router(config-if)# isdn contiguous-bchan`	(E1 only) Sets contiguous bearer-channel handling, causing B channels 1 to 30 to map to timeslots 1 to 31, skipping timeslot 16.

	Command or Action	Purpose

Step 6	**isdn protocol-emulate user**
	
	or
	
	isdn protocol-emulate network
	
	Example:
	`Router(config-if)# isdn protocol-emulate user`
	
	or
	
	Example:
	`Router(config-if)# isdn protocol-emulate network`
		(User side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the user—that is, the TE (clock slave). This is the default.
		
		or
		
		(Network side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the network—that is, the NT (clock master).
		
		Note On the Cisco MC3810, the **isdn protocol-emulate** command replaces the **isdn switch-type** command.

Step 7	**isdn overlap-receiving** **Example:** `Router(config-if)# isdn overlap-receiving`	(Optional) Activates overlap signaling to send to the destination PBX. The interface waits for possible additional call-control information from the preceding PBX. **Note** You can leave the default mode of *enbloc*, in which all call-setup information is sent in the setup message without need for additional messages from the preceding PINX.
Step 8	**isdn network-failure-cause** *value* **Example:** `Router(config-if)# isdn network-failure-cause 1`	(Optional) Specifies the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure BRI Interfaces for QSIG

To configure BRI interfaces for QSIG, perform the following steps.

Note Set up each interface for either user side or network side.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface bri**
4. **isdn static-tei 0**
5. **isdn layer1-emulate user**
6. **isdn layer1-emulate network**

7. **network-clock-priority**
8. **isdn incoming-voice voice**
9. **isdn sending-complete**
10. **isdn switch-type basic-qsig**
11. **isdn protocol-emulate**
12. **isdn overlap-receiving**
13. **isdn network-failure-cause**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**Cisco MC3810** **interface bri** *number* **Cisco 2600 Series and Cisco 3600 Series** **interface bri** *slot/port* **Example:** `Router(config)# interface bri 1/1`	Enters interface configuration mode for the specified port, connector, or interface card number (location of voice module) or slot/port (location of voice network module and voice interface card).
Step 4	**Cisco MC3810, Cisco 2600 Series, and Cisco 3600 Series Only** **isdn static-tei 0** **Example:** `Router(config-if)# isdn static-tei 0`	Enables use of the ISDN lines. **Note** This command is required. In previous releases, it was set automatically with use of the **isdn switch-type basic-qsig** command.
Step 5	**Cisco MC3810 Only** **isdn layer1-emulate user** **Example:** `Router(config-if)# isdn layer1-emulate user`	Configures Layer 1 port mode emulation and clock status for the user—that is, the TE (clock slave).

	Command or Action	Purpose
Step 6	**Cisco MC3810 Only** **isdn layer1-emulate network** **Example:** `Router(config-if)# isdn layer1-emulate network`	Configures Layer 1 port mode emulation and clock status for the network—that is, the NT (clock master).
Step 7	**Cisco MC3810 Only** **network-clock-priority** {**low** | **high**} **Example:** `Router(config-if)# network-clock-priority high`	(TE only) Sets priority for recovering clock signal from the network NT device for this BRI voice port. Keywords are as follows: • **high**—First priority • **low**—Low priority **Note** Do not use this command if the port is configured as NT in Step 5.
Step 8	**Cisco 2600 Series and Cisco 3600 Series Only** **isdn incoming-voice voice** **Example:** `Router(config-if)# isdn incoming-voice voice`	Routes incoming voice calls. This is set for voice-capable BRI interfaces by default. The exception is for Cisco 2600 series and Cisco 3600 series BRI S/T TE voice interface cards, where, in the absence of this command, the **isdn incoming-voice modem** configuration setting converts to **isdn incoming-voice voice** when it receives an incoming call.
Step 9	**isdn sending-complete** **Example:** `Router(config-if)# isdn sending-complete`	(Optional) Configures the voice port to include the "Sending Complete" information element in the outgoing call-setup message. This command is used in some geographic locations, such as Hong Kong and Taiwan, where the "Sending Complete" information element is required in the outgoing call-setup message.
Step 10	**Cisco MC3810, Cisco 2600, and Cisco 3600 Series Only** **isdn switch-type basic-qsig** **Example:** `Router(config-if)# isdn switch-type basic-qsig`	(Optional) If the service-provider switch type for this BRI port differs from the global ISDN switch type, set the interface ISDN switch type to match the service-provider switch type. The interface ISDN switch type overrides the global ISDN switch type on this interface. For more information, see the "ISDN Switch Types for Use with QSIG" section on page 9.

Step 11	**isdn protocol-emulate user**
	or
	isdn protocol-emulate network
	
	Example:
	`Router(config-if)# isdn protocol-emulate user`
	or
	Example:
	`Router(config-if)# isdn protocol-emulate network`
		(User side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the user—that is, the TE (clock slave).
		or
		(Network side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the network—that is, the NT (clock master).
		Note On the Cisco MC3810, the **isdn protocol-emulate** command replaces the **isdn switch-type** command.

	Command or Action	Purpose
Step 12	**isdn overlap-receiving** **Example:** `Router(config-if)# isdn overlap-receiving`	(Optional) Activates overlap signaling to send to the destination PBX and causes the interface to wait for possible additional call-control information from the preceding PINX. **Note** You can leave the default mode of *enbloc*, in which all call-setup information is sent in the setup message without need for additional messages from the preceding PINX.
Step 13	**isdn network-failure-cause** *value* **Example:** `Router(config-if)# isdn network-failure-cause 1`	(Optional) Specifies the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verify the QSIG Configuration

To verify the QSIG configuration, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show call history voice record**
2. **show cdapi**
3. **show controllers t1** or **show controllers e1**
4. **show dial-peer voice**
5. **show isdn**
6. **show isdn** {**active** | **history**}
7. **show isdn service**
8. **show isdn status**
9. **show rawmsg**
10. **show running-config**
11. **show voice port**

DETAILED STEPS

Step 1 **show call history voice record**

Use this command to display information about calls made to and from the router.

Step 2 **show cdapi**

Use this command to display Call Distributor Application Programming Interface (CDAPI) information.

Step 3 **show controllers t1** or **show controllers e1**

Use this command to display information about T1 and E1 controllers.

Step 4 **show dial-peer voice**

Use this command to display how voice dial peers are configured.

Step 5 **show isdn**

Use this command to display information about switch type, memory, status, and Layer 2 and Layer 3 timers.

Step 6 **show isdn** {**active** [*serial-number*] | **history** [*serial-number*]}

Use this command to display current (**active** keyword) or both historic and current (**history** keyword) call information for all ISDN interfaces or, optionally, a specific ISDN PRI interface (created and configured as a serial interface). Information displayed includes called number, remote node name, seconds of connect time, seconds of connect time remaining, seconds idle, and advice of charge (AOC) charging time units used during the call.

Step 7 **show isdn service**

Use this command to display the state and the service status of each ISDN channel.

Step 8 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 9 **show rawmsg**

Use this command to display information about memory leaks.

Step 10 **show running-config**

Use this command to display basic router configuration.

Step 11 **show voice port** [*slot*/*port* | **summary**]

Use this command to display summary information about voice-port configuration.

Troubleshooting Tips

- Use the **debug cdapi** {**events** | **detail**} command to display information about CDAPI application events, registration, messages, and more.
- Use the **debug isdn event** command to display events occurring on the user side (on the router) of the ISDN interface. ISDN events that can be displayed are Q.931 events (call setup and teardown of ISDN network connections).
- Use the **debug tsp** command to display information about the telephony-service provider (TSP).

Examples

This section provides the following output examples:

- Sample Output for the show cdapi Command, page 41
- Sample Output for the show controller Command, page 42

Sample Output for the show cdapi Command

The following shows sample output for a PRI voice port on a Cisco 3660 series.

```
Router# show cdapi

Registered CDAPI Applications/Stacks
====================================

Application: TSP CDAPI Application Voice
        Application Type(s) : Voice Facility Signaling
        Application Level   : Tunnel
        Application Mode    : Enbloc

Signaling Stack: ISDN
        Interface: Se5/0:15

Signaling Stack: ISDN
        Interface: Se5/1:15

Signaling Stack: ISDN
        Interface: Se6/0:15

Signaling Stack: ISDN
        Interface: Se6/1:15

CDAPI Message Buffers
=====================

Used Msg Buffers: 0, Free Msg Buffers: 9600
Used Raw Buffers: 0, Free Raw Buffers: 4800
Used Large-Raw Buffers: 0, Free Large-Raw Buffers: 480
```

The following shows sample output for a PRI voice port on a Cisco MC3810.

```
Router# show cdapi

Registered CDAPI Applications/Stacks
====================================

Application: TSP CDAPI Application Voice
        Application Type(s) : Voice Facility Signaling
        Application Level   : Tunnel
        Application Mode    : Enbloc

Signaling Stack: ISDN
        Interface: Se1:15

CDAPI Message Buffers
=====================

Used Msg Buffers: 2, Free Msg Buffers: 1198
Used Raw Buffers: 2, Free Raw Buffers: 598
Used Large-Raw Buffers: 0, Free Large-Raw Buffers: 60
```

Sample Output for the show controller Command

The following shows sample output for a T1 line (not having problems).

```
Router# show controller T1

T1 3/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20020812, FPGA: 11
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (425 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following shows sample output for a T1 line (having problems).

```
Router# show controller T1 2

T1 2 is down.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  alarm-trigger is not set
  Version info of slot 0:  HW: 4, PLD Rev: 0

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
 Board Hardware Version 1.32, Item Number 800-2540-02,
 Board Revision A0, Serial Number 15264519,
 PLD/ISP Version 0.0,  Manufacture Date 24-Sep-1999.

  Framing is SF, Line Code is AMI, Clock Source is Internal.
  Data in current interval (329 seconds elapsed):
     1 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 329 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 329 Unavail Secs
  Total Data (last 24 hours)
     543 Line Code Violations, 0 Path Code Violations,
     3 Slip Secs, 86400 Fr Loss Secs, 364 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail Secs
```

Sample Output for the show isdn service Command

The following shows sample output for a PRI on a T1 controller.

```
Router# show isdn service

PRI Channel Statistics:
ISDN Se0:15, Channel (1-31)
  Activated dsl 8
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Sample Output for the show isdn status Command

The following shows sample output for a BRI voice port on a Cisco 3600 series.

```
Router# show isdn status

Global ISDN Switchtype = primary-qsig
ISDN Serial3/1:15 interface
        dsl 0, interface ISDN Switchtype = primary-qsig
         **** Master side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        29 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 29
        CCB:callid=89BF, sapi=0, ces=0, B-chan=5, calltype=VOICE
.
.
.
CCB:callid=89C8, sapi=0, ces=0, B-chan=14, calltype=VOICE
.
.
.
        CCB:callid=89D9, sapi=0, ces=0, B-chan=1, calltype=VOICE
        CCB:callid=89DA, sapi=0, ces=0, B-chan=2, calltype=VOICE
        CCB:callid=89DB, sapi=0, ces=0, B-chan=3, calltype=VOICE
    The Free Channel Mask: 0x80000018
ISDN Serial3/0:15 interface
        dsl 1, interface ISDN Switchtype = primary-qsig
         **** Master side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 0, Ces = 9, SAPI = 16, State = TEI_ASSIGNED
    Layer 3 Status:
        28 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 28
        CCB:callid=BDF, sapi=0, ces=0, B-chan=2, calltype=VOICE
        CCB:callid=BE0, sapi=0, ces=0, B-chan=1, calltype=VOICE
        CCB:callid=BE1, sapi=0, ces=0, B-chan=3, calltype=VOICE
.
.
.
CCB:callid=BFA, sapi=0, ces=0, B-chan=31, calltype=VOICE
    The Free Channel Mask: 0xB0000000
    Total Allocated ISDN CCBs = 54

Total Allocated ISDN CCBs = 0
.
.
.
CCB:callid=89C8, sapi=0, ces=0, B-chan=14, calltype=VOICE
.
.
.
        CCB:callid=89D9, sapi=0, ces=0, B-chan=1, calltype=VOICE
        CCB:callid=89DA, sapi=0, ces=0, B-chan=2, calltype=VOICE
        CCB:callid=89DB, sapi=0, ces=0, B-chan=3, calltype=VOICE
    The Free Channel Mask: 0x80000018
ISDN Serial3/0:15 interface
        dsl 1, interface ISDN Switchtype = primary-qsig
```

```
         **** Master side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 0, Ces = 9, SAPI = 16, State = TEI_ASSIGNED
    Layer 3 Status:
        28 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 28
        CCB:callid=BDF, sapi=0, ces=0, B-chan=2, calltype=VOICE
        CCB:callid=BE0, sapi=0, ces=0, B-chan=1, calltype=VOICE
        CCB:callid=BE1, sapi=0, ces=0, B-chan=3, calltype=VOICE
.
.
.
CCB:callid=BFA, sapi=0, ces=0, B-chan=31, calltype=VOICE
    The Free Channel Mask: 0xB0000000
    Total Allocated ISDN CCBs = 54
```

The following shows sample output for a BRI voice port and a PRI voice port on a Cisco MC3810.

```
Router# show isdn status

Global ISDN Switchtype = basic-qsig
ISDN BRI1 interface
dsl 1, interface ISDN Switchtype = basic-qsig
**** Slave side configuration ****
    Layer 1 Status:
DEACTIVATED
    Layer 2 Status:
TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
0 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 0
ISDN BRI2 interface
.
.
.

Router# show isdn status

     Global ISDN Switchtype = primary-qsig
     ISDN Serial1:23 interface
             dsl 0, interface ISDN Switchtype = primary-qsig
              **** Slave side configuration ****
         Layer 1 Status:
             DEACTIVATED
         Layer 2 Status:
             TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
         Layer 3 Status:
             0 Active Layer 3 Call(s)
         Activated dsl 0 CCBs = 0
         The Free Channel Mask: 0x7FFFFF
```

The following shows sample output for a PRI voice port on a Cisco 7200 series.

```
Router# show isdn status

Global ISDN Switchtype = primary-qsig
ISDN Serial1/0:15 interface
        dsl 0, interface ISDN Switchtype = primary-qsig
         **** Slave side configuration ****
    Layer 1 Status:
```

```
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x7FFF7FFF
ISDN Serial1/1:15 interface
        dsl 1, interface ISDN Switchtype = primary-qsig
         **** Slave side configuration ****
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 0
    The Free Channel Mask:  0x7FFF7FFF
    Total Allocated ISDN CCBs = 0
```

Configuring ISDN PRI Q.931 Support

To configure ISDN PRI Q.931 support, perform the following steps.

Note

- Use these commands on Cisco 2600 series and Cisco 3600 series only.
- Set up each interface for either user side or network side.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn switch-type primary-net5**
4. **controller**
5. **pri-group timeslots**
6. **exit**
7. **interface serial**
8. **isdn protocol-emulate**
9. **line-power**

10. **isdn incoming-voice voice**
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**isdn switch-type primary-net5** **Example:** `Router(config)# isdn switch-type primary-net5`	(Optional) Selects a service-provider switch type that accommodates PRI. You can set the ISDN switch type in either global configuration mode or interface configuration mode. • Global configuration mode (this step): specify the switch type for all PRI ports. • Interface configuration mode: specify the switch type for a single interface. The type specified in this mode for any individual interface overrides the type specified in global configuration mode.
Step 4	**controller** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# controller t1 1/1`	Enters T1 or E1 controller configuration mode for the specified slot/port.
Step 5	**pri-group timeslots** *range* **Example:** `Router(config-controller)# pri-group timeslots 1-23`	Specifies PRI on the specified or timeslots that make up the PRI group. Maximum T1 range: 1-23. Maximum E1 range: 1-31. Separate low and high values with a hyphen. **Note** You can configure the PRI group to include all available timeslots, or you can configure a select group of timeslots for the PRI group.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 7	**interface serial 0/0:***channel-number* **Example:** `Router(config)# interface serial 0/0:23`	Enters interface configuration mode for the specified PRI slot/port and D-channel ISDN interface. D-channel ISDN interface is (for T1) 23 and (for E1) 15.

	Command or Action	Purpose

Step 8	**isdn protocol-emulate user**
	or
	isdn protocol-emulate network
	Example:
	`Router(config-if)# isdn protocol-emulate user`
	or
	Example:
	`Router(config-if)# isdn protocol-emulate network`
		(User side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the user—that is, the TE (clock slave).
		or
		(Network side only) Configures Layer 2 and Layer 3 port mode emulation and clock status for the network—that is, the NT (clock master).

Step 9	**line-power** **Example:** `Router(config-if)# line-power`	Turns on the power supplied from an NT-configured port to a TE device.
Step 10	**isdn incoming-voice voice** **Example:** `Router(config-if)# isdn incoming-voice voice`	Routes incoming ISDN voice calls to the voice module.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configuration Examples for ISDN Voice Interfaces

This section provides the following configuration examples:

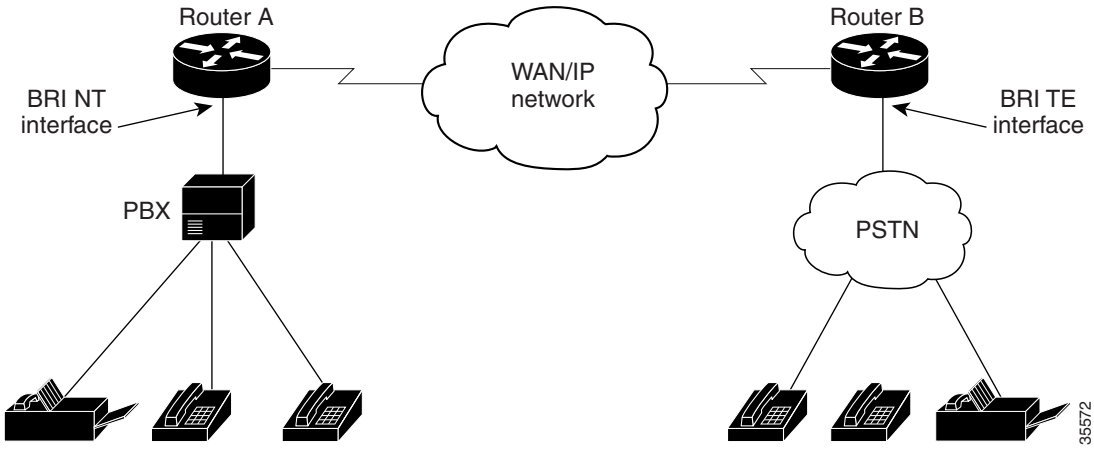
ISDN-to-PBX and ISDN-to-PSTN: Examples

This section contains the following configuration examples:

Configuration examples included in this section correspond to the topology shown in Figure 4. The routers each include a BRI voice interface card and a two-slot voice network module, along with other voice interface cards and modules that are included for completeness. Router A is connected to a PBX through the BRI voice interface card and to Router B by a serial interface. Router B includes a BRI voice

interface card for connection to the PSTN in order to process voice calls from off-premises terminal equipment. Router A is configured for ISDN BRI network-side emulation and Router B is configured for ISDN BRI user-side emulation.

Figure 4 Configuration Example Topology



ISDN Connection to a PBX Configuration (Network-Side Emulation)

The following illustrates the configuration of the BRI interfaces on a Cisco 3640 (Router A in Figure 4) connected to a PBX:

```
interface BRI1/0
no ip address
isdn switch-type basic-net3
isdn overlap-receiving
isdn protocol-emulate network
isdn layer1-emulate network
isdn T306 30000
isdn sending-complete
isdn skipsend-idverify
isdn incoming-voice voice
!
interface BRI1/1
    no ip address
isdn switch-type basic-net3
isdn overlap-receiving
isdn protocol-emulate network
isdn layer1-emulate network
isdn T306 30000
isdn sending-complete
isdn skipsend-idverify
isdn incoming-voice voice
!
ip default-gateway 1.14.0.1
ip classless
ip route 2.0.0.0 255.0.0.0 Ethernet0/1
ip route 2.0.0.0 255.0.0.0 Serial0/1
ip route 172.22.66.33 255.255.255.255 Ethernet0/0
!
```

```
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
```

ISDN Connection to the PSTN Configuration (User-Side Emulation)

The following illustrates the configuration of the BRI interfaces on a Cisco 2600 series (Router B in Figure 4) connected to the public ISDN telephone network:

```
interface BRI1/0
no ip address
 no ip directed-broadcast
 isdn switch-type basic-ni1
 isdn twait-disable
 isdn spid1 14085552111 5552111
 isdn spid2 14085552112 5552112
 isdn incoming-voice voice

interface BRI1/1
 no ip address
 no ip directed-broadcast
 isdn switch-type basic-ni1
 isdn twait-disable
 isdn spid1 14085552111 5552111
 isdn spid2 14085552112 5552112
 isdn incoming-voice voice
!
ip classless
ip route 3.0.0.0 255.0.0.0 Ethernet0/1
ip route 3.0.0.0 255.0.0.0 Serial0/1
ip route 172.21.66.0 255.255.255.0 Ethernet0/0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
```

QSIG Support: Examples

The following show QSIG configurations on a variety of supported routers:

- QSIG Support on Cisco 3600 Series Routers, page 49
- QSIG Support on Cisco 7200 Series Routers, page 54
- QSIG Support on Cisco MC3810 Multiservice Concentrators, page 59

QSIG Support on Cisco 3600 Series Routers

The following shows how a Cisco 3660 series can be configured for E1 and PRI with QSIG signaling support using VoIP and VoATM. Note that Serial5/0, Serial5/1, Serial6/0, and Serial6/1 are configured as ISDN E1 PRI (user side).

```
.
.
.
hostname router3660
```

```
!
memory-size iomem 20
voice-card 5
!
voice-card 6
!
ip subnet-zero
!
isdn switch-type primary-qsig
isdn voice-call-failure 0
!
controller E1 5/0
 pri-group timeslots 1-5,16
!
controller E1 5/1
 pri-group timeslots 1-31
!
controller E1 6/0
 pri-group timeslots 1-31
!
controller E1 6/1
 pri-group timeslots 1-31
!
interface FastEthernet0/0
 ip address 10.7.72.9 255.255.255.0
 speed auto
 half-duplex
!
interface FastEthernet0/1
 ip address 10.100.100.7 255.255.255.0
 no keepalive
 duplex auto
 speed auto
 hold-queue 1000 in
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
interface ATM3/0
 no ip address
 atm clock INTERNAL
 no atm ilmi-keepalive
 pvc 10/40
  vbr-rt 155000 50000 64000
  encapsulation aal5mux voice
 !
interface Serial5/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
```

```
 isdn overlap-receiving
 isdn incoming-voice voice
 no cdp enable
!
interface Serial5/1:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
interface Serial6/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
interface Serial6/1:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
ip classless
ip route 192.168.17.125 255.255.255.255 FastEthernet0/0
no ip http server
!
map-class frame-relay frs0
 frame-relay voice bandwidth 1260000
 frame-relay fragment 200
 no frame-relay adaptive-shaping
 frame-relay cir 1260000
 frame-relay fair-queue
!
voice-port 1/0/0
 modem passthrough system
 timing hookflash-in 0
!
voice-port 1/0/1
 modem passthrough system
 timing hookflash-in 0
!
voice-port 5/0:15
 compand-type a-law
!
voice-port 5/1:15
 compand-type a-law
 cptone DE
!
voice-port 6/0:15
 compand-type a-law
 cptone DE
!
voice-port 6/1:15
 no echo-cancel enable
 compand-type a-law
```

```
 cptone DE
!
dial-peer voice 1 pots
 shutdown
 destination-pattern 21...
 modem passthrough system
 direct-inward-dial
!
dial-peer voice 51 voip
 shutdown
 destination-pattern 6504007
 modem passthrough system
 session target ipv4:100.100.100.3
!
dial-peer voice 2 pots
 shutdown
 destination-pattern 21...
 modem passthrough system
 direct-inward-dial
 port 5/1:15
!
dial-peer voice 3 voip
 shutdown
 destination-pattern 22...
 modem passthrough system
 session target ipv4:100.100.100.6
!
dial-peer voice 5 pots
 shutdown
 destination-pattern 22...
 modem passthrough system
 direct-inward-dial
 prefix 4006
!
dial-peer voice 13 pots
 shutdown
 destination-pattern 21...
 modem passthrough system
 direct-inward-dial
 port 6/0:15
!
dial-peer voice 6 pots
 destination-pattern 21...
 modem passthrough system
 direct-inward-dial
 port 6/1:15
!
dial-peer voice 44 voatm
 destination-pattern 22...
 modem passthrough system
 session target ATM3/0 pvc 10/40
!
dial-peer voice 20 pots
 incoming called-number 4...
 destination-pattern 4007
 modem passthrough system
 direct-inward-dial
 port 5/0:15
 prefix 4007
!
dial-peer voice 21 pots
 destination-pattern 4006
 modem passthrough system
 direct-inward-dial
```

```
 port 5/0:15
 prefix 4006
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

QSIG Support on Cisco 7200 Series Routers

The following shows how QSIG protocol support is configured with VoFR on Router A (where calls originate) and Router B (where calls terminate). Note that Serial3/0:15, Serial3/1:15, Serial4/0:15, and Serial4/1:15 are configured as ISDN E1 PRI (user side).

Router A: Originating Configuration

```
.
.
.
hostname 7200_RouterA
!
card type e1 3
card type e1 4
!
dspint DSPfarm3/0
!
dspint DSPfarm4/0
!
ip subnet-zero
no ip domain-lookup
ip host routerC 192.168.17.125
ip host routerD 10.1.1.2
!
multilink virtual-template 1
frame-relay switching
isdn switch-type primary-qsig
isdn voice-call-failure 0
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 3 g729br8
!
controller E1 3/0
 pri-group timeslots 1-31
 description qsig connected to PCG 1
!
controller E1 3/1
 pri-group timeslots 1-31
 description cas connected to PCG 2
!
controller E1 4/0
 pri-group timeslots 1-31
 description qsig group connected PCG slot3
!
controller E1 4/1
 pri-group timeslots 1-31
 description qsig group connected PCG slot4
!
!
!
!
!
```

Router B: Terminating Configuration

```
.
.
.
hostname 7200_RouterB
!
card type e1 3
card type e1 4
!
dspint DSPfarm3/0
!
dspint DSPfarm4/0
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host routerC 192.168.17.125
!
multilink virtual-template 1
isdn switch-type primary-qsig
isdn voice-call-failure 0
!
!
!
!
!
!
controller E1 3/0
 pri-group timeslots 1-31
 description qsig connected to PCG 5
!
controller E1 3/1
 pri-group timeslots 1-31
 description cas connected to PCG 6
!
controller E1 4/0
 pri-group timeslots 1-31
 description cas connected to PCG slot7
!
controller E1 4/1
 pri-group timeslots 1-31
 description cas connected to PCG slot8
!
interface Loopback0
 no ip address
 no ip directed-broadcast
!
```

Router A: Originating Configuration	Router B: Terminating Configuration

interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 shutdown
 half-duplex
!
!
!
!
!
interface Serial1/0
 bandwidth 512
 ip address 10.1.1.104 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no keepalive
 shutdown
 no fair-queue
 clockrate 2015232
 ppp multilink
!
interface Serial1/1
 description vofr connection to
7200_RouterB_s1/1
 ip address 10.0.0.2 255.0.0.0
 ip broadcast-address 10.0.0.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip route-cache
 no ip mroute-cache
 no keepalive
 frame-relay traffic-shaping
 frame-relay map ip 10.0.0.1 100 broadcast
 frame-relay interface-dlci 100
  class vofr_class
  vofr data 4 call-control 5
!
interface Serial1/2
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Serial1/3
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
 clockrate 2015232
!
	interface FastEthernet0/0
	 description VOIP_10.0.0.1_maxstress to
	7200_RouterAgate
	 ip address 10.0.0.1 255.0.0.0
	 no ip directed-broadcast
	 no ip mroute-cache
	 shutdown
	 media-type MII
	 full-duplex
	!
	interface Serial1/0
	 no ip address
	 no ip directed-broadcast
	 no ip mroute-cache
	 shutdown
	!
	!
	!
	!
	!
	!
	!
	!
	!
	interface Serial1/1
	 description vofr connection to
	7200_RouterA
	 ip address 10.0.0.1 255.0.0.0
	 ip broadcast-address 10.0.0.0
	 no ip directed-broadcast
	 encapsulation frame-relay
	 no keepalive
	 clockrate 8060928
	 frame-relay traffic-shaping
	 frame-relay map ip 10.0.0.2 100 broadcast
	 frame-relay interface-dlci 100
	  class vofr_class
	  vofr data 4 call-control 5
	!
	!
	interface Serial1/2
	 no ip address
	 no ip directed-broadcast
	 shutdown
	 clockrate 2015232
	!
	!
	interface Serial1/3
	 no ip address
	 no ip directed-broadcast
	 shutdown
	!
	!
	!
	!

Router A: Originating Configuration	Router B: Terminating Configuration
interface Ethernet2/0 ip address 10.1.50.77 255.255.0.0 ip broadcast-address 10.1.0.0 no ip directed-broadcast no ip route-cache no ip mroute-cache ! interface Ethernet2/1 ip address 10.0.0.2 255.255.0.0 ip broadcast-address 10.0.0.0 no ip directed-broadcast no ip route-cache no ip mroute-cache shutdown ! interface Ethernet2/2 no ip address no ip directed-broadcast no ip route-cache no ip mroute-cache shutdown ! interface Ethernet2/3 no ip address no ip directed-broadcast no ip route-cache no ip mroute-cache shutdown ! interface Serial3/0:15 no ip address no ip directed-broadcast no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! ! ! interface Serial3/1:15 no ip address no ip directed-broadcast no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! ! !	interface Ethernet2/0 ip address 10.5.192.123 255.255.0.0 ip helper-address 192.168.17.125 no ip directed-broadcast no ip mroute-cache ! ! interface Ethernet2/1 ip address 10.0.0.1 255.255.0.0 no ip directed-broadcast no ip mroute-cache shutdown ! ! ! interface Ethernet2/2 no ip address no ip directed-broadcast shutdown ! ! ! interface Ethernet2/3 no ip address no ip directed-broadcast shutdown ! ! ! interface Serial3/0:15 no ip address no ip directed-broadcast no ip route-cache cef ip mroute-cache no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! interface Serial3/1:15 no ip address no ip directed-broadcast no ip route-cache cef ip mroute-cache no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable !

Router A: Originating Configuration	Router B: Terminating Configuration
interface Serial4/0:15 no ip address no ip directed-broadcast no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! ! ! interface Serial4/1:15 no ip address no ip directed-broadcast no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! ! ! interface ATM5/0 no ip address no ip directed-broadcast no ip route-cache no ip mroute-cache shutdown no atm ilmi-keepalive ! ! ! ! ! interface Virtual-Template1 ip address 10.0.0.2 255.255.255.0 no ip directed-broadcast load-interval 30 fair-queue 64 256 1 ppp multilink ppp multilink fragment-delay 20 ppp multilink interleave ip rtp priority 16384 16383 92 ! router igrp 144 network 10.0.0.0 ! ip default-gateway 10.21.75.10 ip classless no ip http server !	interface Serial4/0:15 no ip address no ip directed-broadcast no ip route-cache cef ip mroute-cache no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! interface Serial4/1:15 no ip address no ip directed-broadcast no ip route-cache cef ip mroute-cache no logging event link-status isdn switch-type primary-qsig isdn overlap-receiving isdn incoming-voice voice isdn bchan-number-order ascending no cdp enable ! interface ATM5/0 no ip address no ip directed-broadcast shutdown no atm ilmi-keepalive ! interface FastEthernet6/0 no ip address no ip directed-broadcast shutdown half-duplex ! interface Virtual-Template1 ip unnumbered Loopback0 no ip directed-broadcast no ip route-cache cef ip mroute-cache ppp multilink ppp multilink fragment-delay 20 ppp multilink interleave ! ! router igrp 144 network 10.0.0.0 ! ! ip classless no ip http server !

Router A: Originating Configuration	Router B: Terminating Configuration
map-class frame-relay vofr_class no frame-relay adaptive-shaping frame-relay cir 4400000 frame-relay bc 1000 frame-relay fair-queue frame-relay voice bandwidth 4000000 frame-relay fragment 256 ! voice-port 3/0:15 compand-type a-law cptone DE ! voice-port 3/1:15 compand-type a-law cptone DE ! voice-port 4/0:15 compand-type a-law cptone DE ! voice-port 4/1:15 compand-type a-law cptone DE ! dial-peer voice 5552222 pots destination-pattern +5552... direct-inward-dial port 3/1:15 prefix 5552 ! dial-peer voice 5551111 vofr destination-pattern +6...... sequence-numbers session target Serial1/1 100 codec g729br8 ! dial-peer voice 5554 pots destination-pattern 5554... direct-inward-dial port 4/1:15 prefix 5554 ! dial-peer voice 5553 pots destination-pattern 5553... direct-inward-dial port 4/0:15 prefix 5553 ! dial-peer voice 5551 pots destination-pattern +5551... direct-inward-dial port 3/0:15 prefix 5551 . . .	map-class frame-relay vofr_class no frame-relay adaptive-shaping frame-relay cir 4400000 frame-relay bc 1000 frame-relay fair-queue frame-relay voice bandwidth 4000000 frame-relay fragment 256 ! voice-port 3/0:15 compand-type a-law ! ! voice-port 3/1:15 compand-type a-law ! ! voice-port 4/0:15 compand-type a-law ! ! voice-port 4/1:15 compand-type a-law ! ! dial-peer voice 5552222 pots destination-pattern +6662... direct-inward-dial port 3/1:15 prefix 6662 ! dial-peer voice 5551111 vofr destination-pattern +5...... sequence-numbers session target Serial1/1 100 codec g729br8 ! dial-peer voice 6661 pots destination-pattern +6661... direct-inward-dial port 3/0:15 prefix 6661 ! dial-peer voice 6663 pots destination-pattern +6663... direct-inward-dial port 4/0:15 prefix 6663 ! dial-peer voice 6664 pots destination-pattern +6664... direct-inward-dial port 4/1:15 prefix 6664 . . .

QSIG Support on Cisco MC3810 Multiservice Concentrators

The following shows how a Cisco MC3810 can be configured for E1 and PRI with QSIG signaling support and VoIP and VoFR. Note that Serial1:15 is configured as ISDN E1 PRI (user side).

```
.
.
.
hostname Router3810
!
network-clock base-rate 56k
ip subnet-zero
!
isdn switch-type primary-qsig
isdn voice-call-failure 0
!
controller T1 0
 mode atm
 framing esf
 clock source internal
 linecode b8zs
!
controller E1 1
 pri-group timeslots 1-7,16
!
interface Ethernet0
 ip address 100.100.100.6 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 bandwidth 2000
 ip address 10.168.14.1 255.255.255.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no keepalive
 clockrate 2000000
 cdp enable
 frame-relay traffic-shaping
 frame-relay interface-dlci 100
  class frs0
  vofr cisco
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1:15
 no ip address
 no ip directed-broadcast
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
interface ATM0
 no ip address
 no ip directed-broadcast
 ip mroute-cache
 no atm ilmi-keepalive
```

```
 pvc 10/42
  encapsulation aal5mux voice
 !
!
interface FR-ATM20
 no ip address
 no ip directed-broadcast
 shutdown
!
no ip http server
ip classless
ip route 223.255.254.0 255.255.255.0 Ethernet0
!
map-class frame-relay frs0
 frame-relay voice bandwidth 1260000
 frame-relay fragment 200
 no frame-relay adaptive-shaping
 frame-relay cir 1260000
 frame-relay fair-queue
!
map-class frame-relay frsisco
!
voice-port 1:15
 compand-type a-law
!
dial-peer voice 100 voatm
 shutdown
 destination-pattern 4...
 session target ATM0 pvc 10/42
 codec g729ar8
 no vad
!
dial-peer voice 1 pots
 shutdown
 destination-pattern 3001
!
dial-peer voice 42 vofr
 destination-pattern 4006
 session target Serial0 100
 signal-type ext-signal
!
dial-peer voice 21 pots
 destination-pattern 4007
 direct-inward-dial
 port 1:15
 prefix 4007
!
dial-peer voice 12 voip
 shutdown
 destination-pattern 4006
 session target ipv4:100.100.100.7
.
.
.
```

Q.931-Support: Example

The following shows how a Cisco 3660 can be configured for E1 and PRI with network-side support using VoIP. Note that Serial5/0:15 and Serial6/0:15 are configured as ISDN E1 PRI (network side) and that Serial5/1:15 and Serial6/1:15 are configured as ISDN E1 PRI (user side).

```
.
.
.
hostname router3660
!
memory-size iomem 20
voice-card 5
!
voice-card 6
!
ip subnet-zero
!
isdn switch-type primary-net5
isdn voice-call-failure 0
!
controller E1 3/0
 pri-group timeslots 1-5,16
!
controller E1 3/1
 pri-group timeslots 1-31
!
controller E1 4/0
 pri-group timeslots 1-31
!
controller E1 4/1
 pri-group timeslots 1-31
!
interface FastEthernet0/0
 ip address 10.7.72.9 255.255.255.0
 speed auto
 half-duplex
!
interface FastEthernet0/1
 ip address 10.100.100.7 255.255.255.0
 no keepalive
 duplex auto
 speed auto
 hold-queue 1000 in
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
interface Serial5/0:15
 no ip address
```

```
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn protocol-emulate network
 no cdp enable
!
interface Serial5/1:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
interface Serial6/0:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 isdn protocol-emulate network
 no cdp enable
!
interface Serial6/1:15
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 fair-queue 64 256 0
 no cdp enable
!
ip classless
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0
no ip http server
!
voice-port 1/0/0
timing hookflash-in 0
!
voice-port 1/0/1
    timing hookflash-in 0
!
voice-port 5/0:15
 compand-type a-law
!
voice-port 5/1:15
 compand-type a-law
 cptone DE
!
voice-port 6/0:15
 compand-type a-law
 cptone DE
!
voice-port 6/1:15
 no echo-cancel enable
 compand-type a-law
 cptone DE
!
dial-peer voice 1 pots
 shutdown
```

```
 destination-pattern 21...
direct-inward-dial
!
dial-peer voice 51 voip
 shutdown
 destination-pattern 6504007
session target ipv4:100.100.100.3
!
dial-peer voice 2 pots
 shutdown
 destination-pattern 21...
direct-inward-dial
 port 5/1:15
!
dial-peer voice 3 voip
 shutdown
 destination-pattern 22...
session target ipv4:100.100.100.6
!
dial-peer voice 5 pots
 shutdown
 destination-pattern 22...
 modem passthrough system
 direct-inward-dial
 prefix 4006
!
dial-peer voice 13 pots
 shutdown
 destination-pattern 21...
direct-inward-dial
 port 6/0:15
!
dial-peer voice 6 pots
 destination-pattern 21...
direct-inward-dial
 port 6/1:15
!
dial-peer voice 20 pots
 incoming called-number 4...
 destination-pattern 4007
direct-inward-dial
 port 5/0:15
 prefix 4007
!
dial-peer voice 21 pots
 destination-pattern 4006
direct-inward-dial
 port 5/0:15
 prefix 4006
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- *Cisco IOS Debug Command Reference, Release 12.3T* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123dbr/index.htm
- *Cisco IOS IP Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/
- *Cisco IOS Voice Troubleshooting and Monitoring Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/voipt_c/index.htm
- *Cisco IOS Voice, Video, and Fax Command Reference* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/
- *E1 PRI Troubleshooting* at http://www.cisco.com/warp/public/116/E1_pri.html
- *Installing VoIP Cards* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/hw_inst/6271voip.htm
- *T1 PRI Troubleshooting* at http://www.cisco.com/warp/public/116/T1_pri.html
- T1 troubleshooting information at http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a5f40.shtml
- *Using the show isdn status Command for BRI Troubleshooting* at http://www.cisco.com/warp/public/129/bri_sh_isdn_stat.html
- *Troubleshooting ISDN* at http://cco-rtp-1.cisco.com/warp/public/779/smbiz/service/troubleshooting/ts_isdn.htm

Implementing Expanded Scope for Cause-Code-Initiated Call-Establishment Retries

This chapter describes how to implement the Expanded Scope for Cause-Code-Initiated Call Establishment Retries feature. This feature enables a gateway to reattempt calls when a disconnect message is received from the PSTN without maintaining extra dial peers.

Feature History for Expanded Scope for Cause-Code-Initiated Call Establishment Retries

Release	Modification
12.2(15)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 69.

Contents

Prerequisites for Expanded Scope for Cause-Code-Initiated Call Establishment Retries

- Perform the prerequisites that are listed in the "Prerequisites for Configuring ISDN Voice Interfaces" section on page 3.
- Configure ISDN (trunks) or the Cisco Signaling System 7 (SS7) on the gateway.

Restrictions for Expanded Scope for Cause-Code-Initiated Call Establishment Retries

Restrictions are described in the "Restrictions for Configuring ISDN Voice Interfaces" section on page 4. In addition, the following applies:

- This feature must be used with ISDN Net5 PRI or NI2 PRI switch types.

Information About Expanded Scope for Cause-Code-Initiated Call-Establishment Retries

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

Before this feature was available, there was no easy way to reattempt most calls when a disconnect was received from the PSTN. Only cause code 44 reattempted a call—and only if multiple dial peers to the same destination were configured.

This feature enables you to configure a gateway to reattempt a call when a disconnect message is received from the PSTN. You can configure up to 16 arguments (specifying values from 1 to 127 in each argument) for cause codes.

Note For a list of cause codes, see *ISDN Switch Types, Codes, and Values*.

How to Configure Expanded Scope for Cause-Code-Initiated Call-Establishment Retries

This section contains the following procedures:

Configuring Expanded Scope for Cause-Code-Initiated Call-Establishment Retries

To configure expanded scope for cause-code-initiated call-establishment retries, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface**
4. **isdn negotiate-bchan**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Router(config)# interface serial 0/4`	Configures an interface type and enters interface configuration mode for the specified slot/port.
Step 4	**isdn negotiate-bchan** [**resend-setup**] [**cause-codes** {*cause-code1* [*cause-code2...cause-code16*]}] **Example:** `Router(interface)# isdn negotiate-bchan resend-setup cause-codes 34 44 63`	Enables the router to accept a B channel that is different from the B channel requested in the outgoing call-setup message and specifies the cause codes for which the call is reattempted. **Note** You must have ISDN trunks configured on your router before you can configure the cause codes.
Step 5	**exit** **Example:** `Router(interface)# exit`	Exits the current mode.

Verifying Expanded Scope for Cause-Code-Initiated Call-Establishment Retries

To verify expanded scope for cause-code-initiated call-establishment retries, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show isdn status**
2. **show running-config**

DETAILED STEPS

Step 1 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 2 **show running-config**

Use this command to display basic router configuration, including cause codes and values entered to verify that the gateway can reattempt disconnect calls received form the PSTN.

Troubleshooting Tips

- Use the **debug isdn q931** command to display calls that the router has attempted or reattempted.

Configuration Examples for Expanded Scope for Cause-Code-Initiated Call Establishment Retries

This section provides the following configuration examples:

- ISDN Interface: Example, page 68
- Cause Codes: Example, page 69

ISDN Interface: Example

The following output shows that the ISDN interface is configured on the gateway and that the gateway is configured to reattempt disconnect calls received from the PSTN when the disconnect cause code is 18.

```
Router# show running-config
!
interface Serial7/0:0
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 isdn T306 30000
 isdn rlm-group 0
 no isdn send-status-inquiry
```

```
 isdn negotiate-bchan resend-setup cause-code 18 ==> Cause-code 18 is configured.
 no cdp enable
!
end
```

Cause Codes: Example

The following sample configuration shows that cause codes 34, 44, and 63 are set on serial slot 0 and port 23:

```
Router# show running-config
!
interface serial0:23
 isdn negotiate-bchan resend-setup cause-codes 34 44 63
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- *ISDN Switch Types, Codes, and Values* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123sup/123debug/dbg_ap2g.htm

Implementing Clear Channel T3/E3

This chapter describes how to implement the Clear Channel T3/E3 with Integrated CSU/DSU feature. The feature delivers Clear Channel service as a T3/E3 pipe a bandwidth of 28x24x64k for T3 or 16x32x64 for E3. The software-configurable T3/E3 network module allows you to switch between T3 and E3 applications with a single Cisco IOS command.

The T3/E3 NM-1 network module supports a single-port T3 or E3 with an integrated channel service unit (CSU) and a data service unit (DSU). It supports High-Level Data Link Control (HDLC), PPP, and frame relay. It includes the following features:

- Single port—universal T3/E3 version
- Clear and subrate support on both T3 and E3 modes
- Online insertion and removal (OIR) support on Cisco 3660 series and Cisco 3745 routers
- Onboard processing of Cisco Message Definition Language (MDL) and performance monitoring
- Support for scrambling and subrate can be independently or simultaneously enabled in each DSU mode
- Support for full T3 and E3 line rates

The T3/E3 NM-1 network module provides high-speed performance for advanced, fully converged networks supporting a wide array of applications and services such as security and advanced QoS for voice and video. T3/E3 and subrate T3/E3 connectivity optimizes WAN bandwidth for deploying the new applications and service delivery.

Feature History for Clear Channel T3/E3 with Integrated CSU/DSU

Release	Modification
12.2(11)YT	This feature was introduced.
12.2(15)T	This feature was integrated into this release.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 91.

Contents

Prerequisites for Clear Channel T3/E3 with Integrated CSU/DSU

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.
- Ensure that you have sufficient system memory (Table 6).

Table 6 Minimum Memory Requirements

Platform	Flash Memory	DRAM Memory
Cisco 2650	8 MB	32 MB
Cisco 2651XM		
Cisco 2691	32 MB	64 MB
Cisco 3660 series	8 MB	64 MB
Cisco 3725	32 MB	128 MB
Cisco 3745	32 MB	128 MB

Restrictions for Clear Channel T3/E3 with Integrated CSU/DSU

Restrictions are described in the "Restrictions for Configuring ISDN Voice Interfaces" section on page 4.

Information About Clear Channel T3/E3 with Integrated CSU/DSU

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

All supported platforms are capable of supporting line-rate performance, but impose varying levels of CPU overhead and therefore affect overall platform performance. Table 7 shows recommended branch-office positioning.

Table 7 T3/E3 NM-1 Branch Office Positioning and Support Comparison

Platform	Recommended Positioning		Supported T3/E3 Modes
	Type of Service	Branch Office Size	
Cisco 2650	Subrate T3/E3	Small to medium offices	1
Cisco 2651XM			
Cisco 2691	Subrate T3/E3	Small to medium offices	1
Cisco 3660 series	Subrate and full-rate T3/E3	Large and regional offices	1
Cisco 3725	Subrate and full-rate T3/E3	Medium and large offices	1
Cisco 3745	Subrate and full-rate T3/E3	Medium, large, and regional offices	2

How to Configure Clear Channel T3/E3 with Integrated CSU/DSU

This section contains the following procedures:

Configuring Clear-Channel T3

This section contains the following procedures:

Configure the Card Type and Controller for T3

To configure the card type and controller for T3, perform the following steps.

Note

- When the clear-channel T3/E3 network module is used for the first time, the running configuration does not show the T3/E3 controller and its associated serial interface. Use the **show version** command to learn if the router recognized the T3/E3 card and was able to initialize the card properly. After the card type is configured for the slot, the respective controller and serial interfaces appear in the running configuration. See the "Additional References" section on page 91.
- The autoconfig/setup utility does not support configuring the card type for the T3/E3 network module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type t3**
4. **controller t3**
5. **framing**
6. **linecode**
7. **cablelength**
8. **clock source**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**card type t3** *slot* **Example:** `Router(config)# card type t3 1`	Configures the card type on the T3 controller for the designated slot. **Note** By default, the T3 controller does not show up in the **show running-config** output.
Step 4	**controller t3** *slot/port* **Example:** `Router(config)# controller t3 1`	Specifies the T3 controller and enters controller configuration mode for the specified slot/port.

	Command or Action	Purpose
Step 5	**framing** {**c-bit** | **m23**} **Example:** `Router(config-controller)# framing c-bit`	Specifies the T3 framing type. Keywords are as follows: • **c-bit**—C-bit framing • **m23**—M23 framing
Step 6	**linecode** {**ami** | **b8zs** | **hdb3**} **Example:** `Router(config-controller)# linecode ami`	Sets the line-encoding method to match that of your telephone-company service provider. Keywords are as follows: • **ami**—Alternate mark inversion (AMI), valid for T1 or E1 controllers. Default for T1 lines. • **b8zs**—B8ZS, valid for T1 controllers only. • **hdb3**—High-density bipolar 3 (hdb3), valid for E1 controllers only. Default for E1 lines.
Step 7	**cablelength** *feet* **Example:** `Router(config-controller)# cablelength 250`	Specifies the distance from the routers to the network equipment.
Step 8	**clock source** {**internal** | **line**} **Example:** `Router(config-controller)# clock source line`	Selects the clock source. Keywords are as follows: • **internal**—Internal clock source (T3 default) • **line**—Network clock source (E3 default)
Step 9	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure DSU Mode and Bandwidth for T3

To configure DSU mode and bandwidth for T3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial**
4. **dsu mode**
5. **dsu bandwidth**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *slot/port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode for the specified slot/port.
Step 4	**dsu mode** {**0** | **1** | **2** | **3** | **4**} **Example:** `Router(config-if)# dsu mode 0`	Specifies the interoperability mode used by a T3 controller—that is, to what the T3 controller connects. Keywords are as follows: • **0**—Another T3 controller or a Digital Link DSU (DL3100) (default) • **1**—Kentrox DSU • **2**—Larscom DSU • **3**—Adtran T3SU 300 • **4**—Verilink HDM 2182
Step 5	**dsu bandwidth** *kbps* **Example:** `Router(config-if)# dsu bandwidth 44210`	Specifies the maximum allowable bandwidth, in kbps. Range: 1 to 44210. **Note** The real (actual) vendor-supported bandwidth range is 75 to 44210 kbps. See Table 6 on page 72.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure Encryption Scrambling for T3

To configure encryption scrambling for T3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial**
4. **scramble**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *slot/port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode for the specified slot/port.
Step 4	**scramble** **Example:** `Router(config-if)# scramble`	Enables the scrambling of the payload. Default: off.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure a Bit-Error-Rate Test Pattern for T3

To configure a bit-error-rate test pattern for T3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3**
4. **bert pattern**
5. **no bert**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t3** *slot*/*port* **Example:** `Router(config)# controller t3 1/1`	Enters controller configuration mode for the specified slot/port.
Step 4	**bert pattern** {**2^23** | **2^20** | **2^15** | **1s** | **0s** | **alt-0-1**} **interval** *time* **Example:** `Router(config-controller)# bert pattern 2^20 interval 10000`	Configures a bit-error-rate test pattern. Keywords and arguments are as follows: • **2^23**—Pseudorandom 0.151 test pattern, 8,388,607 bits long • **2^20**—Pseudorandom 0.153 test pattern, 1,048,575 bits long • **2^15**—Pseudorandom 0.151 test pattern, 32,768 bits long • **1s**—Repeating pattern of ones (...111...) • **0s**—Repeating pattern of zeros (...000...) • **alt-0-1**—Repeating pattern of alternating zeros and ones (...01010...) • **interval** *time*—Duration of the BER test, in minutes.
Step 5	**no bert** **Example:** `Router(config-controller)# no bert`	Disables the BERT test pattern.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure Loopback for T3

To configure loopback for T3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **controller t3**
4. **loopback**
5. **no loopback**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t3** *slot*/*port* **Example:** `Router(config)# controller t3 1/1`	Enters controller configuration mode for the specified slot/port.
Step 4	**loopback** {**local** | **network** {**line** | **payload**} | **remote**} **Example:** `Router(config-controller)# loopback local`	Loops the T3 line toward the line and back toward the router. Keywords are as follows: • **local**—Loops the data back toward the router and sends an alarm-indication signal (AIS) out toward the network. On a dual port card, it is possible to run channelized on one port and primary rate on the other port. • **network** {**line** | **payload**}—Sets loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**). • **remote**—Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. M23 format does not support remote loopbacks.
Step 5	**no loopback** **Example:** `Router(config-controller)# no loopback`	Removes the loop.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure the Maintenance Data Link for T3

To configure the maintenance date link for T3, perform the following steps.

Note This configuration information is applicable only to C-bit parity T3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3**
4. **mdl**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t3** *slot*/*port* **Example:** `Router(config)# controller t3 1/1`	Enters controller configuration mode for the specified slot/port.

	Command or Action	Purpose
Step 4	**mdl** {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*} **Example:** `Router(config-controller)# mdl transmit path`	Configures the MDL message. Keywords and arguments are as follows: • **transmit path**—Enables transmission of the MDL path message. • **transmit idle-signal**—Enables transmission of the MDL idle signal message. • **transmit test-signal**—Enables transmission of the MDL test signal message. • **string eic** *string*—Equipment identification code (EIC); can be up to 10 characters. • **string lic** *string*—Location identification code (LIC); can be up to 11 characters. • **string fic** *string*—Frame identification code (FIC); can be up to 10 characters. • **string unit** *string*—Unit identification code (UIC); can be up to 6 characters. • **string pfi** *string*—Facility identification code (PFI) sent in the MDL path message; can be up to 38 characters. • **string port** *string*—Port number string sent in the MDL idle signal message; can be up to 38 characters. • **string generator** *string*—Generator number string sent in the MDL test signal message; can be up to 38 characters.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configuring Clear-Channel E3

This section contains the following procedures:

Configure the Card Type and Controller for E3

To configure the card type and controller for E3, perform the following steps.

Note The autoconfig/setup utility does not support configuring the card type for the T3/E3 network module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type e3**
4. **controller e3**
5. **framing**
6. **linecode**
7. **clock source**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**card type e3** *slot* **Example:** `Router(config)# card type e3 1`	Configures the card type on the E3 controller for the designated slot. **Note** By default, the E3 controller does not show up in the **show running-config** output.
Step 4	**controller e3** *slot/port* **Example:** `Router(config)# controller e3 1`	Enters controller configuration mode for the specified slot/port.
Step 5	**framing** {**bypass** | **g751**} **Example:** `Router(config-controller)# framing bypass`	Specifies the framing type. Keywords are as follows: • **bypass**—G.751 framing is bypassed • **g751**—G.751 is the E3 framing type (default)

	Command or Action	Purpose
Step 6	**linecode** {**ami** | **b8zs** | **hdb3**} **Example:** `Router(config-controller)# linecode hdb3`	Sets the line-encoding method to match that of your telephone-company service provider. Keywords are as follows: • **ami**—Alternate mark inversion (AMI), valid for T1 or E1 controllers. Default for T1 lines. • **b8zs**—B8ZS, valid for T1 controllers only. • **hdb3**—High-density bipolar 3 (hdb3), valid for E1 controllers only. Default for E1 lines.
Step 7	**clock source** {**internal** | **line**} **Example:** `Router(config-controller)# clock source line`	Selects the clock source. Keywords are as follows: • **internal**—Internal clock source (T3 default) • **line**—Network clock source (E3 default)
Step 8	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure DSU Mode and Bandwidth for E3

To configure DSU mode and bandwidth for E3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial**
4. **dsu mode**
5. **dsu bandwidth**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface serial** *slot/port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode for the specified slot/port.
Step 4	**dsu mode** {**0** | **1**} **Example:** `Router(config-if)# dsu mode 0`	Specifies the interoperability mode used by an E3 controller—that is, to what the E3 controller connects. Keywords are as follows: • **0**—(default) Another E3 controller or a digital link DSU (DL3100) • **1**—Kentrox DSU
Step 5	**dsu bandwidth** *kbps* **Example:** `Router(config-if)# dsu bandwidth 34010`	Specifies the maximum allowable bandwidth, in kbps. Range: 22 to 34010. **Note** The real (actual) vendor-supported bandwidth range is 358 to 34010 kbps. See Table 6 on page 72.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure Encryption Scrambling for E3

To configure encryption scrambling for E3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial**
4. **scramble**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface serial** *slot/port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode for the specified slot/port.
Step 4	**scramble** **Example:** `Router(config-if)# scramble`	Enables the scrambling of the payload. Default: off.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configure a Bit-Error-Rate Test Pattern for E3

To configure a bit-error-rate test pattern for E3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3**
4. **bert pattern**
5. **no bert**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller e3** *slot/port* **Example:** `Router(config)# controller e3 1/0`	Enters controller configuration mode for the specified slot/port.

	Command or Action	Purpose
Step 4	**bert pattern** {**2^23** | **2^20** | **2^15** | **1s** | **0s** | **alt-0-1**} **interval** *time* **Example:** `Router(config-controller)# bert pattern 2^20 interval 1440`	Enables a bit-error-rate (BER) test pattern on a T1 or E1 line, and sets the length of the test pattern and duration of the test. Keywords and arguments are as follows: • **2^23**—Pseudorandom 0.151 test pattern, 8,388,607 bits long • **2^20**—Pseudorandom 0.153 test pattern, 1,048,575 bits long • **2^15**—Pseudorandom 0.151 test pattern, 32,768 bits long • **1s**—Repeating pattern of ones (...111...) • **0s**—Repeating pattern of zeros (...000...) • **alt-0-1**—Repeating pattern of alternating zeros and ones (...01010...) • **interval** *time*—Duration of the BER test, in minutes
Step 5	**no bert** **Example:** `Router(config-controller)# no bert`	Disables the BER test pattern.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configure Loopback for E3

To configure loopback for E3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller e3**
4. **loopback**
5. **no loopback**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller e3** *slot*/*port* **Example:** `Router(config)# controller e3 1/1`	Enters controller configuration mode for the specified slot/port.
Step 4	**loopback** {**local** | **network** {**line** | **payload**}} **Example:** `Router(config-controller)# loopback local`	Loops the E3 line toward the line and back toward the router. Keywords are as follows: • **local**—Loops the data back toward the router and sends an AIS signal out toward the network. • **network** {**line** | **payload**}—Sets loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).
Step 5	**no loopback** **Example:** `Router(config-controller)# no loopback`	Removes the loop.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configure the National Bit in the G.751 Frame for E3

To configure the national bit in the G.751 frame for E3, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller e3**
4. **national bit**

5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller e3** *slot*/*port* **Example:** `Router(config)# controller e3 1/1`	Enters controller configuration mode for the specified slot/port.
Step 4	**national bit** {**1** | **0**} **Example:** `Router(config-controller)# national bit 1`	Sets the E3 national bit in the G.751 frame used by the E3 controller. Valid values: 0 and 1. Default: 1.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Verifying Clear-Channel T3/E3

To verify clear-channel T3/E3, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show controllers**
2. **show interfaces serial**
3. **show isdn status**
4. **show running-config**
5. **show version**

DETAILED STEPS

Step 1 **show controllers**

Use this command to display information about the specified port, connector, or interface card number (location of voice module) or slot/port (location of voice network module and VIC).

Step 2 **show interfaces serial**

Use this command to display information about a serial interface.

Step 3 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 4 **show running-config**

Use this command to display basic router configuration.

Step 5 **show version**

Use this command to display whether the router recognized the T3/E3 card and was able to initialize the card properly. Lists the hardware interfaces and controllers present in the router. You should find "1 Subrate T3/E3 port(s)".

```
Router# show version

.
.
.
Router uptime is 2 hours, 6 minutes
System returned to ROM by power-on
System image file is "flash:c3725-i-mz"

cisco 3725 (R7000) processor (revision 0.4) with 111616K/19456K bytes of memory.
Processor board ID 12345678901
R7000 CPU at 240Mhz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0
Primary Rate ISDN software, Version 1.1
2 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
2 Channelized T1/PRI port(s)
1 Subrate T3/E3 port(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
15680K bytes of ATA System CompactFlas (Read/Write)

Configuration register is 0x0
```

Troubleshooting Tips

Set Loopbacks

- Use T3/E3 local loopback to ensure that the router and the T3/E3 network module are working properly. The controller clock source should be configured to "internal."
- Use T3/E3 network loopback and remote loopback to diagnose problems with cables between the T3/E3 controller and the central switching office at the link level. For this diagnostic setup to work, if the network module is looped toward the network, the network module must be configured with the clock source as "line."

Run Bit Error Rate Test

- The network module contains onboard BERT circuitry. With this circuitry present, the software can send and detect a programmable pattern that is compliant with CCITT/ITU pseudorandom and repetitive test patterns. BERT allows you to test cables and signal problems in the field.

- When a BERT is running, your system expects to receive the same pattern that it is sending. To help ensure this, two common options are available.
  - Use a loopback somewhere in the link or network.
  - Configure remote testing equipment to send the same BERT pattern at the same time.

Configuration Example for Clear Channel T3/E3 with Integrated CSU/DSU

This example shows the running configuration of a router whose E3 (slot1/0) interface is configured to use G.751 framing and a network (line, or network, is the E3 default) clock source. Note that the bandwidth of the interface is configured to 34010 kbps.

```
Router# show running-config

Building configuration...
%AIM slot 0 doesn't exist

Current configuration :1509 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
card type e3 1
no logging console
!
ip subnet-zero
no ip routing
!
voice call carrier capacity active
!
mta receive maximum-recipients 0
!
controller E3 1/0
 clock source line
 framing g751
 linecode <line code>
 dsu bandwidth 34010
!
interface Loopback0
 no ip address
 no ip route-cache
 shutdown
 no keepalive
!
interface FastEthernet0/0
 ip address 10.0.145.34 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0
 no ip address
```

```
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 shutdown
 clockrate 2000000
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no keepalive
 no cdp enable
!
interface Serial0/1
 no ip address
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 shutdown
 clockrate 2000000
!
interface Serial0/2:0
 ip address 172.27.27.2 255.255.255.0
 no ip route-cache
 no keepalive
!
interface Serial1/0
 no ip address
 no ip route-cache
 no keepalive
 dsu bandwidth 34010
!
ip classless
no ip http server
!
ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release

- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

Implementing Integrated Voice and Data WAN on T1/E1 Interfaces

This chapter describes how to implement the Integrated Voice and Data WAN on T1/E1 Interfaces with the AIM-ATM-VOICE-30 Module feature. This card provides a voice-processing termination solution at a density of 30 VoIP or VoFR voice or fax channels, while not consuming a network-module slot. It provides the following benefits:

- Integrated voice and serial data WAN functionality on the same T1/E1 interface or on the second port of the voice/WAN interface cards (VWIC)
- Support for high-complexity codecs

The serial interface supports the following features:

- Point-to-Point Protocol (PPP), Frame Relay (FR), and high-level data link control (HDLC) encapsulations—Up to 120 channels
- FR, HDLC, and PPP encapsulation and voice on the same T1/E1 voice interface available in the following two options:
  - Channel associated signaling (CAS) or Primary Rate Interface (PRI) group, plus the channel group are defined on the same T1/E1 interface in the Cisco 2600 WIC slot.
  - The DS0 or PRI, plus the channel groups are configured across two ports of the same T1/E1 VWIC. For example, you can configure a DS0 group or a PRI group on port 0, and a channel group on the same port or another port.
- HDLC data inversion—Meets the density requirement for T1 links
- Compression support—Software and hardware compression is supported on the Cisco 3660, Cisco 3725, and Cisco 3745

Note There is only one advanced integration module (AIM) slot on Cisco 2600 platforms, so hardware compression is not applicable to the Cisco 2600 series.

- Multilink PPP
- G.703 (E1 unframed mode)

Feature History for Integrated Voice and Data WAN on T1/E1 Interfaces with the AIM-ATM-VOICE-30 Module

Release	Modification
12.2(15)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 117.

Contents

Prerequisites for Configuring Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.

Cisco 2600 series and Cisco 2600XM

- Ensure that you have the following:
  - 64-MB RAM and 32-MB flash memory
  - Appropriate voice-interface hardware, as listed in *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660*

Cisco 3660, Cisco 3725, and Cisco 3745

- Ensure that you have the following:
  - Cisco IOS Release 12.2(15)T IP Plus or a later release
  - 128-MB RAM and 32-MB flash memory
  - Multiservice interchange (MIX) module (MIX-3660-64) installed in the time-division multiplexing (TDM) slot on the motherboard on the Cisco 3660 only
  - Appropriate voice-interface hardware, as listed in *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660*

Restrictions for Configuring Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4. In addition, the following apply.

Cisco 2600 Series Restrictions

- This feature does not support Drop and Insert.
- Voice channels can appear only on a single port of the two T1/E1 interfaces on the VWIC. Data channels can appear on both.

Other Platform Restrictions

- This feature is not supported on the following platforms: Cisco 1700 series, Cisco MC3810, and Cisco AS5x00.

Hardware Restrictions

- This feature is not supported on the AIM-VOICE-30 card or the AIM-ATM card.
- Modem relay is not supported on AIM-ATM-VOICE-30 DSPs.
- Codec GSM-EFR is not supported.
- With a high-complexity image set, an AIM-ATM-VOICE-30 DSP card can process up to only 16 voice channels. The 16 associated time slots must be within a contiguous range. Applications and voice interfaces that can be used with the three types of AIM are listed in *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660*.

Information About Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

To implement this feature, you should understand the following concepts:

AIM-ATM-VOICE-30 Module

The AIM-ATM-VOICE-30 module is an advanced integration module capable of supporting up to 30 voice or fax channels when used in a supported platform with one of the T1/E1 voice/WAN interface cards (such as VWIC-1T1). The module includes DSPs that are used for a number of voice-processing tasks such as voice compression and decompression, voice-activity detection or silence suppression, and PBX or PSTN signaling protocols.

The module supports VoIP, VoFR, and VoIP over ATM (VoATM) while leaving the router network-module slot open for other functions such as asynchronous or synchronous serial concentration. For additional information, see *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660*.

Integrated Voice and Data WAN

This feature adds integrated voice and serial-data WAN service on the same T1 or E1 interface or VWIC on AIM-ATM-VOICE-30 DSP cards. This enhancement enables you to use some DS0 channels for serial-data Frame Relay, high-level data link control (HDLC), and Point-to-Point Protocol (PPP), for example, while the remaining T1 or E1channels can be used for voice channel-associated signaling (CAS) or PRI.

Figure 5 shows a typical application scenario in which 16 channels of a T1 line are used for voice and 4 channels are used for Frame relay data. Integrating voice and serial data on the same T1 or E1 line minimizes the recurring cost of providing PSTN and data WAN access. In particular, integrated access provides a number of voice DS0s (for PSTN access) and a Frame Relay link on the same T1.

Figure 5 Typical Application Scenario

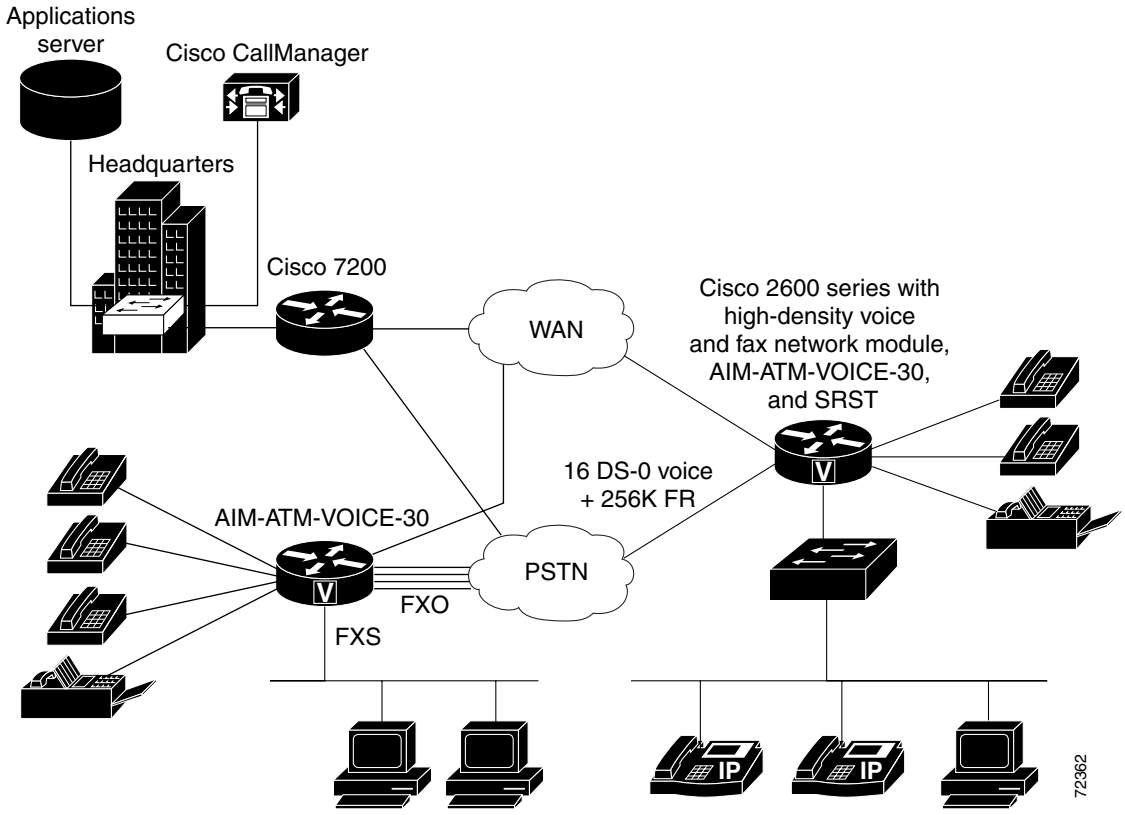
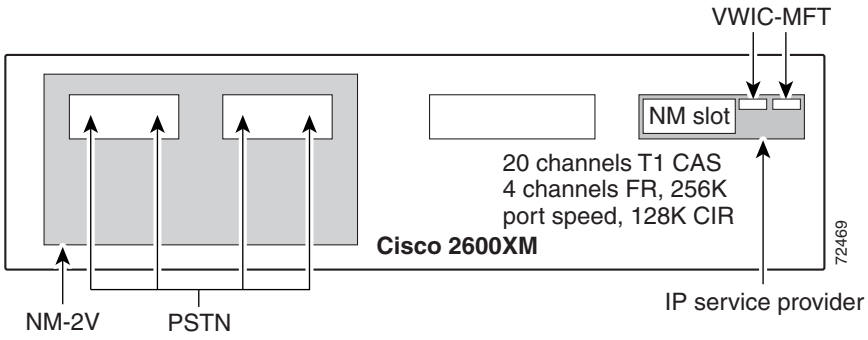


Figure 6 shows a typical deployment scenario in which port 0 of the VWIC-MFT module is connected to an integrated voice and data service provider with 20 channels. These 20 channels are used for voice (running CAS or PRI); the remaining four channels are used for serial data (running Frame Relay). Using this type of configuration, you can take advantage of the integrated service offered by a service provider and minimize the cost of leasing and supporting T1 or E1 lines.

Figure 6 Typical Feature Deployment



High-Complexity Voice Compression

This feature adds high-complexity G.723, G.728, and GSM-FR codec support to the AIM-ATM-VOICE-30 module so that the DSP can support both medium- and high-complexity codecs running separately. Each DSP core can process up to two voice channels, so each module can support up to 16 voice channels when running a high-complexity DSP firmware image.

The following high-complexity codecs are supported:

- G.723.1 5.3K
- G.723.1 6.3K
- G.723 1A 5.3K
- G.723 1A 6.3K
- G.728
- G.729
- G.729B
- GSM-FR

The following medium-complexity codecs are supported in high-complexity mode:

- G.711 mu-law
- G.711 a-law
- G.726
- G.729A
- G.729 AB
- Clear-channel codec
- Fax relay

Note Neither modem-relay nor GSM-EFR is supported.

Network Clock Source and Participation

Note You must configure network clock source and participation to use the Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module feature.

Packet voice and video are sensitive to time delays. To prevent mismatches and data slips, you must synchronize data flows to a single clock source, known as the *network clock*. When a network clock is configured on a gateway, the router is externally clocked by one T1 or E1 port and passes that clock signal across the backplane to another T1 or E1 port on another WIC or network module slot. Use of a network clock on a gateway is configured by naming the network modules and interface cards that are participating in network clocking, and then selecting a port to act as the source of timing for the network clock.

The network clock provides timing from the source, through the port to the AIM, and then out to all participating router slots. The number of supported AIM slots is as follows:

- The Cisco 2600 series and Cisco 2600XM support one internal AIM slot.
- The Cisco 3660, Cisco 3725, and Cisco 3745 support two internal AIM slots.

The network clock source must be derived from an external source—for example, PSTN, PBX, or ATM network. For digital voice ports, the **clock source** command in configures the type of timing (internal or from the line) for each port that you designate as a primary source or backup for the network clock.

This command allows maximum flexibility. For example, on a router with a multiflex trunk VWIC connected to an ATM network and a digital T1/E1 packet voice trunk network module connected to a PBX, you can set up network clocking in any of three ways:

- The multiflex trunk VWIC provides clocking to the AIM, which provides it to the digital T1/E1 packet voice trunk network module (that is, to the PBX).
- The digital T1/E1 packet voice trunk network module provides clocking to the AIM, which provides it to the multiflex trunk VWIC.
- The ATM network and the PBX run their own clocks, which are not necessarily synchronized. However, this scenario could result in poor voice quality.

Note For a detailed discussion of clock sources on individual ports, see the information about clock sources on digital T1/E1 voice ports in the chapter on configuring voice ports in the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

How to Configure Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

This section contains the following procedures:

- Configuring Network Clock Source and Participation, page 99
- Configuring the AIM-ATM-VOICE-30 Card for High-Complexity Codecs and Time Slots, page 106 (optional)
- Configuring Integrated Voice and Serial Data WAN, page 108 (optional)
- Verifying Integrated Voice and Serial Data WAN, page 110 (optional)

Note For detailed configuration tasks for the AIM-ATM, AIM-VOICE-30, see *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660*.

Configuring Network Clock Source and Participation

Note You must configure network clock source and participation to use the Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module feature.

Configuring Clock Source Internal

To configure a clock with an internal source, perform the following steps.

Prerequisites

- Configure the controller for PRI or DS0 groups and for ATM AIM or CAS before configuring network-clock participation parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **clock source**
5. **mode atm**
6. **exit**
7. **network-clock-participate**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**controller** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# controller t1 1/0`	Enters controller configuration mode on the T1 or E1 controller on the selected slot/port.

	Command or Action	Purpose
Step 4	**clock source** {**line** [**primary**] | **internal**} **Example:** `Router(config-controller)# clock source internal`	Specifies the source from which the phase-locked loop (PLL) on this port derives its clocking and, if the source is **line**, whether this port is the primary source. Arguments and keywords are as follows: • **line**—Clock recovered from the line's receive data stream. This is the default. • **primary**—External source to which the port is connected. This option also puts a second port, which is generally connected to the PBX, into looped-time mode. Both ports are configured with **line**, but only the port connected to the external source is configured with **primary**. • **internal**—T1 or E1 controller internal PLL. **Note** With the default, the clock source does not appear in the **show running-config** command output. Use the **show controllers** command to display the current source for a port.
Step 5	**mode atm** [**aim** *aim-slot-number*] **Example:** `Router(config-controller)# mode atm aim 0`	Specifies that the configuration on this controller is for ATM, using the AIM in the specified slot for ATM processing, and creates ATM interface 0. Use when you connect the T1 line to an ATM network. The argument is as follows: • *aim-slot-number*—AIM slot number on the router chassis: – Cisco 2600 series: 0 – Cisco 3660 and Cisco 3700 series: 0 or 1 **Note** This command without the **aim** keyword uses software rather than the AIM to perform ATM SAR. This is supported on Cisco 2600 series WIC slots only and not on network module slots.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

	Command or Action	Purpose

Step 7	**network-clock-participate** [**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*]
	
	Example:
	`Router(config)# network-clock-participate slot 5`
	
	Example:
	`Router(config)# network-clock-participate wic 0`
	
	Example:
	`Router(config)# network-clock-participate aim 0`
		Allows the network module or VWIC in the specified slot to use the network clock for its timing. Keywords depend on platform.

Step 8	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring the Clock-Source Line

To configure the clock-source line, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **clock source**
5. **mode atm**

   or

   mode cas

   or

   ds0-group timeslots

   or

   pri-group timeslots
6. **exit**
7. **network-clock-participate**
8. **network-clock-select priority**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller** {**t1** | **e1**} *slot*/*port* **Example:** `Router(config)# controller t1 1/0`	Enters controller configuration mode on the T1 or E1 controller on the specified slot/port.
Step 4	**clock source** {**line** [**primary**] | **internal**} **Example:** `Router(config-controller)# clock source line`	Specifies the source from which the phase-locked loop (PLL) on this port derives its clocking and, if the source is **line**, whether this port is the primary source. Keywords are as follows: • **line**—Clock recovered from the line's receive data stream. This is the default. • **primary**—External source to which the port is connected. This option also puts a second port, which is generally connected to the PBX, into looped-time mode. Both ports are configured with **line**, but only the port connected to the external source is configured with **primary**. • **internal**—T1 or E1 controller internal PLL. **Note** With the default, the clock source does not appear in the **show running-config** command output. Use the **show controllers** command to display the current source for a port.

	Command or Action	Purpose

Step 5	**mode atm** [**aim** *aim-slot*]
	
	or
	
	mode cas
	
	or
	
	ds0-group *group-number* **timeslots** *timeslot-range* **type** *type*
	
	or
	
	pri-group timeslots *timeslot-range*
	
	Example:
	`Router(config-controller)# mode atm aim 0`
	
	or
	
	Example:
	`Router(config-controller)# mode cas`
	
	or
	
	Example:
	`Router(config-controller)# ds0-group 0 timeslots 1-4,8-23 type fxs-loop-start`
	
	or
	
	Example:
	`Router(config-controller)# pri-group timeslots 1-4,8-23`
		(**mode atm** command) Sets the controller to ATM mode and creates ATM interface ATM 0. Use for Cisco 2600 series, Cisco 3660, and Cisco 3700 series that use an AIM for ATM processing. Do not use on routers that use an AIM only for DSP resources.
		
		Note This command without the **aim** keyword uses software (rather than AIM) to perform ATM segmentation and reassembly. This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
		
		or
		
		(**mode cas** command) Sets the controller to CAS mode (for software images earlier than Cisco IOS Release 12.2(15)T). Use for Cisco 2600 series with WIC slots.
		
		or
		
		(**ds0-group timeslots** command) Creates a DS0 group that makes up a logical voice port on a T1/E1 controller and specifies the signaling type by which the router connects to the PBX or CO.
		
		or
		
		(**pri-group timeslots** command) Creates a PRI group that makes up a logical voice port on a channelized T1 or E1 controller.

Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Step 7	**network-clock-participate** [**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*]
	
	Example:
	`Router(config)# network-clock-participate wic 0`
	
	Example:
	`Router(config)# network-clock-participate slot 5`
		Allows the network module or VWIC in the specified slot to use the network clock for its timing. Keywords depend on platform.

	Command or Action	Purpose
Step 8	**network-clock-select** *priority* {**t1** | **e1**} *slot/port* **Example:** `Router(config)# network-clock-select 1 e1 0/1`	Specifies a slot/port to be used as a timing source for the network clock and the priority level for that port. The source that is given the highest priority is designated the primary source and is used first; if it becomes unavailable, the source with the second-highest priority is used, and so forth. This command is required if the clock source is from the line. The clocking is provided to the AIM, which then provides it to participating slots in the router. Keywords and arguments are as follows: • *priority*—Priority for the clock source (1 is highest priority) • **t1** or **e1**—T1 or E1 ports • *slot/port*—Slot and port for the controller clock source. Slots are as follows: – Cisco 2600 series and Cisco 2600XM—0 (built-in WIC slot) or 1 (network module slot) – Cisco 3660—1 to 6 – Cisco 3725 and Cisco 3745—1 to 4
Step 9	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring the AIM-ATM-VOICE-30 Card for High-Complexity Codecs and Time Slots

To configure the AIM-ATM-VOICE-30 card for high-complexity codecs and time slots, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card**
4. **codec complexity**
5. **dspfarm**
6. **exit**
7. **controller**
8. **ds0-group timeslot**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice-card** *slot* **Example:** `Router(config)# voice-card 0`	Enters voice-card configuration mode to configure DSP resources on the specified card. The argument is as follows: • *slot*—AIM slot number on the router chassis: – Cisco 2600 series and Cisco 2600XM—0 – Cisco 3660—7 is AIM slot 0; 8 is AIM slot 1 – Cisco 3725—3 is AIM slot 0; 4 is AIM slot 1 – Cisco 3745—5 is AIM slot 0; 6 is AIM slot 1

	Command or Action	Purpose
Step 4	**codec complexity** {**high** | **medium**} **Example:** `Router(config-voice-card)# codec complexity high`	Changes the codec complexity to high or medium and matches the DSP complexity packaging to the supported codecs. When codec complexity changes, the system prompts you to remove all existing DS0 or PRI groups. Then all DSPs are reset, loaded with the specified firmware image, and released. For switched calls, you can configure a high-complexity codec even when the DSPs are loaded with medium-complexity firmware. However, an error message displays during call setup when a high-complexity codec is detected. This command affects all DSPs on this voice card. You cannot specify the DSP firmware type based on the DSP chip type.
Step 5	**dspfarm** **Example:** `Router(config-voicecard)# dspfarm`	(Optional) Enters the DSP resources on the AIM specified in the **voice-card** command into the DSP resource pool.
Step 6	**exit** **Example:** `Router(config-voicecard)# exit`	Exits the current mode.
Step 7	**controller** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode on the T1 or E1 controller on the selected slot/port.
Step 8	**ds0-group** *group-number* **timeslots** *timeslot-range* **type** *type* **Example:** `Router(config-controller)# ds0-group 0 timeslots 1-16`	Creates a DS0 group that makes up a logical voice port on a T1/E1 controller. The keyword and argument are as follows: • **timeslots** *timeslot-range*—Number, range of numbers, or multiple ranges of numbers separated by commas. T1 range: 1 to 24. E1 range: 1 to 31. • **type** *type*—Signaling type by which the router communicates with the PBX or PSTN. **Note** High-complexity codecs with the AIM-ATM-VOICE-30 module can process up to 16 voice channels.
Step 9	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configuring Integrated Voice and Serial Data WAN

To configure integrated voice and serial data WAN, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **clock source**
5. **channel-group timeslots**
6. **ds0-group timeslots type**

   or

   pri-group timeslots
7. **no shutdown**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# controller e1 0/1`	Enters controller configuration mode on the T1 or E1 controller on the specified slot/port. The example shows a VWIC E1 card installed in WIC slot 0.

	Command or Action	Purpose
Step 4	**clock source** {**line** [**primary**] | **internal**} **Example:** `Router(config-controller)# clock source internal`	Specifies the source from which the phase-locked loop (PLL) on this port derives its clocking and, if the source is **line**, whether this port is the primary source. Arguments and keywords are as follows: • **line**—Clock recovered from the line's receive data stream. This is the default. • **primary**—External source to which the port is connected. This option also puts a second port, which is generally connected to the PBX, into looped-time mode. Both ports are configured with **line**, but only the port connected to the external source is configured with **primary**. • **internal**—T1 or E1 controller internal PLL. **Note** With the default, the clock source does not appear in the **show running-config** command output. To display the current source for a port, use the **show controllers** command.
Step 5	**channel-group** *channel-group-number* **timeslots** *timeslot-range* [**speed** *bit-rate*] **aim** *aim-slot-number* **Example:** `Router(config-controller)# channel-group 1 timeslots 1-5 aim 0`	Directs HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 digital signaling processor (DSP) card. Use to specify T1/E1 timeslots to be used for HDLC/PPP/Frame-relay encapsulated data.

Step 6	**ds0-group** *ds0-group-number* **timeslots** *timeslot-range* **type** *type*
	
	or
	
	pri-group timeslots *timeslot-range* | **d-channel** *timeslot* | **rlm-timeslot** *timeslot number*]
	
	Example:
	`Router(config-controller)# ds0-group 2 timeslots 6-12 type e&m-immediate-start`
	
	or
	
	Example:
	`Router(config-controller)# pri-group timeslots 6-23`
		(DS0 groups) Creates a DS0 group that makes up a logical voice port on a T1/E1 controller. Keywords and arguments are as follows:
		• **timeslot** *timeslot-range*—Number, range of numbers, or multiple ranges of numbers separated by commas. T1 range: 1 to 24. E1 range: 1 to 31.
		• **type** *type***—**Signaling type by which the router communicates with the PBX or PSTN.
		Note High-complexity codecs with the AIM-ATM-VOICE-30 module can process up to 16 voice channels.
		
		or
		
		(PRI groups) Creates a PRI group that makes up a logical voice port on a channelized T1 or E1 controller. The keyword and argument are as follows:
		• **timeslot** *timeslot-range*—Range of numbers. T1 range: 1 to 23. E1 range: 1 to 15.
		Note Only one PRI group can be configured on a controller.

	Command or Action	Purpose
Step 7	**no shutdown** **Example:** `Router(config-controller)# no shutdown`	Reinstates the controller.
Step 8	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Verifying Integrated Voice and Serial Data WAN

To verify integrated voice and serial data WAN, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show controllers serial**
2. **show interface serial**
3. **show isdn status**
4. **show network-clocks**
5. **show running-config**
6. **show voice dsp**

DETAILED STEPS

Step 1 show controllers serial

Use this command to display the configuration on the serial interface

```
Router# show controllers serial 0/0:3

Interface Serial0/0:3 is up
  Hardware is ATM AIM SERIAL
  hwidb=0x82C1B768, sardb=0x826404A4
  slot 0, unit 0, subunit 0
  Current (mxt5100_t)sardb:
      Ind_Q(0x3D53580), Ind_Q_idx(695), Ind_Q_size(30000)
      Cmd_Q(0x3D4E720), Cmd_Q_idx(359), Cmd_Q_size(20000)
      Inpool(0x3B9E1A0), Inpool_size(4096)
      Outpool(0x3D1B080), Outpool_size(4096)
      Localpool(0x3D20000), Localpool_size(256)
      StorBlk(0x3BA7000), host_blk(0x3BA4840), em_blk(0x3BA4900)
      tx_buf_desc(0x3D476A0), tx_free_desc_idx (1023)
      num_fallback(0)
  MXT5100 Port Info:
      Port Number (4), Port ID (0xE05)
      Interface Number (0), Interface ID (0xF5E0)
      Port Type 2, Port Open Status SUCCESS
 HDLC channels opened(1)
      Port counters:Tx Packets:50686, Rx Packets:42864
      Tx Bytes:0, Rx Bytes:0
      Discards:No Resource:0, Protocol Errors 4
```

```
  MXT5100 Channel Info:
    HDLC Channel Info (0):
      Chan_ID (0xF25), Open Status SUCCESS
  tx_limited=0(8)
```

Step 2 show interface serial

Use this command to display the configuration on the serial interface.

```
Router# show interface serial 0/0:3

Serial0/0:3 is up, line protocol is up
  Hardware is ATM AIM SERIAL
  Internet address is 20.0.0.1/16
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  LCP Open
  Open:IPCP, CDPCP
  Last input 00:00:09, output 00:00:09, output hang never
  Last clearing of "show interface" counters 18:36:25
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6696 packets input, 446400 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     6697 packets output, 460924 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
 Timeslot(s) Used:4, Transmitter delay is 0 flags
```

Step 3 show isdn status

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 4 show network-clocks

Use this command to display the current chosen clock and the list of all sources of network clocks according to their priority.

```
Router# show network-clocks

  Network Clock Configuration
  ---------------------------
  Priority      Clock Source    Clock State     Clock Type

    3             E1 6/2             GOOD               E1
    5             T1 2/0             GOOD               T1
    9          Backplane             Good               PLL

  Current Primary Clock Source
  ---------------------------
  Priority      Clock Source    Clock State     Clock Type

    3             E1 6/2             GOOD                E1
```

Step 5 show running-config

Use this command to display the basic router configuration.

Step 6 **show voice dsp**

Use this command to display the voice DSP configuration.

```
Router# show voice dsp

DSP  DSP             DSPWARE CURR  BOOT                          PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============
C5421000 00 {high}    3.6.14 IDLE  idle      0  0 0/0:0     01     0    5313/1516
```

Configuration Examples for Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

This section contains the following configuration examples:

Single-Serial-Data WAN: Example

This example shows the configuration of a router whose E1 (0/0) controller is used for integrated voice and serial data. Note that E1 timeslots 1 to 11 are configured for serial data and E1 timeslots 12 to 31 are configured for PRI voice. Also note that interface Serial0/0:1 is the logical interface for E1 timeslots 1 to 11 and interface Serial0/0:15 is the logical interface for E1 timeslots 12 to 31.

```
Router# show running-config

Building configuration...

Current configuration : 1356 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "buick-hc"
!
network-clock-participate wic 0
network-clock-participate aim 0
network-clock-select 1 E1 0/0
voice-card 5
 dspfarm
!
ip subnet-zero
!!
isdn switch-type primary-qsig
no voice hpi capture buffer
no voice hpi capture destination
!
```

```
mta receive maximum-recipients 0
!
controller E1 0/0
 channel-group 1 timeslots 1-11 aim 0
 pri-group timeslots 12-31
!
controller E1 0/1
!
controller E1 0/3
controller E1 0/2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0:1
 ip address 175.0.0.1 255.0.0.0
 encapsulation ppp
!
interface Serial0/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 no cdp enable
!
interface FastEthernet0/1
 ip address 1.10.10.1 255.0.0.0
 speed 100
 full-duplex
!
ip http server

ip classless
!
call rsvp-sync
!
voice-port 0/0:15
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 40 pots
 destination-pattern 427....
 direct-inward-dial
 port 0/0:15
 prefix 427
!
dial-peer voice 400 voip
 destination-pattern 525....
 session target ipv4:1.10.10.2
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Multiple-Serial-Data WAN: Example

This example shows the configuration of a router whose E1 (0/0) controller is used voice and serial data traffic and whose E1 (0/1) controller is used completely for data traffic.

```
Router# show running-config

Building configuration...
Current configuration : 1492 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "buick-hc"
!
network-clock-participate wic 0
network-clock-participate aim 0
network-clock-select 1 E1 0/0
voice-card 5
 dspfarm
!
ip subnet-zero
!
isdn switch-type primary-qsig
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
controller E1 0/0
 channel-group 1 timeslots 1-11 aim 0
 pri-group timeslots 12-31
!
controller E1 0/1
 channel-group 1 timeslots 1-31 aim 0
!
controller E1 0/3
!
controller E1 0/2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0:1
 ip address 172.0.0.1 255.0.0.0
 encapsulation ppp
!
interface Serial0/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 no cdp enable
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.0.0.0
 speed 100
```

```
 full-duplex
!
interface Serial0/1:1
 ip address 175.5.0.1 255.0.0.0
 encapsulation frame-relay
!
ip http server
ip classless
!
call rsvp-sync
!
voice-port 0/0:15
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 40 pots
 destination-pattern 427....
 direct-inward-dial
 port 0/0:15
 prefix 427
!
dial-peer voice 400 voip
 destination-pattern 525....
 session target ipv4:10.10.10.2
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

High-Complexity Codecs and Network Clock: Example

This example shows the configuration of a router in which the WIC at slot 0 and AIM at slot 0 are configured to received clock from the network (see the lines network-clock-participate). Also note that E1 0/0 controller is the source of the network clock (see the line network-clock-select). This example also shows that the voice card in slot 5 uses a high-complexity codec.

```
Router# show running-config

Building configuration...
Current configuration : 1276 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "router-hc"
!
network-clock-participate wic 0
network-clock-participate aim 0
network-clock-select 1 E1 0/0
voice-card 5
 codec complexity high
 dspfarm
!
```

```
ip subnet-zero
!
isdn switch-type primary-qsig
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
controller E1 0/0
 pri-group timeslots 1-16
!
controller E1 0/1
!
controller E1 0/3
!
controller E1 0/2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 no cdp enable
!
interface FastEthernet0/1
 ip address 1.10.10.1 255.0.0.0
 speed 100
 full-duplex
!
ip http server
ip classless
!
call rsvp-sync
!
voice-port 0/0:15
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 40 pots
 destination-pattern 427....
 direct-inward-dial
 port 0/0:15
 prefix 427
!
dial-peer voice 400 voip
 destination-pattern 525....
 session target ipv4:0.10.10.2
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- *AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04gin.htm
- *Cisco IOS Voice, Video, and Fax Command Reference* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/

Implementing ISDN GTD

This chapter describes how to implement the ISDN Generic Transparency Descriptor (GTD) for Setup Message feature. The feature provides support for mapping ISDN information elements (IEs) to corresponding GTD parameters. The following IEs and parameters are supported:

- Originating line information (OLI)
- Bearer capability (USI and TMR) called-party number (CPN)
- Calling-party number (CGN)
- Redirecting number (RGN, OCN and RNI)

This feature allows VoIP service providers to develop custom call treatments and enhanced service offerings based on call origination and to correctly identify the source of a call, bill appropriately, and settle accurately with other network providers.

Feature History for ISDN GTD for Setup Message

Release	Modification
12.2(15)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 141.

Contents

Prerequisites for Configuring ISDN GTD for Setup Message

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.
- Configure your VoIP network and Cisco IOS gateways to allow sending and processing of ISDN Q.931 setup messages.

Restrictions for Configuring ISDN GTD for Setup Message

Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4. In addition, the following applies:

- This feature does not support ISDN BRI calls.

Information About ISDN GTD for Setup Message

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

To implement this feature, you should understand the following concepts:

- Feature Design of ISDN GTD for Setup Messages, page 120
- Mapping of ISDN Information Elements to GTD Parameters, page 121

Feature Design of ISDN GTD for Setup Messages

The ISDN GTD for Setup Messages feature allows the delivery of information elements present in ISDN setup messages to Tool Command Language (Tcl) scripts, RADIUS accounting servers, and routing servers in VoIP networks. This allows Tcl scripts and routing servers to access ISDN signaling information to provide enhanced features and routing services. In particular, the OLI IE present in AT&T (TR-41459 ISDN PRI UNI Specification) and MCI setup messages can be passed to the originating-line-info VSA in RADIUS start-accounting messages to identify the originating caller.

FCC regulations mandate that pay-telephone operators be compensated by network operators for 1-800 calls made from their pay telephones. Before implementation of this feature, network operators had no way to identify calls made from their pay telephones. As a result, network operators had to compensate pay-telephone operators directly from their own revenues. In addition, network operators had no billing records to validate pay-telephone operators' settlement requests to prevent fraud. This feature provides Cisco network operators with the ability to correctly identify the source of a call. It allows networks to do the following:

- Extract originating-line information (OLI) to identify pay telephone calls and pass on applicable charges
- Generate billing records that can be used to validate pay telephone operator settlement requests.

Note For information on accounting records and RADIUS billing, see the *RADIUS VSA Voice Implementation Guide*.

This feature provides the flexibility to identify other types of originated calls (from prisons, hotels, and so forth) and allows you to use the Tcl interface to define custom services for these types of calls.

Note For more information on Tcl application programming, see the *Tcl IVR API Version 2.0 Programmer's Guide*.

In addition to passing OLI, this feature supports GTD mapping for Bearer Capability, Called Party Number, Calling Party Number, and Redirecting Number IEs.

Cisco implements this feature on Cisco IOS gateways by providing a mechanism to allow creating and passing the Q931 setup message and its parameters in a GTD format. The setup message, received by the gateway to initiate call establishment, is mapped to the GTD initial address message (IAM). Generic transparency descriptors represent parameters within signaling messages and enable transport of signaling data in a standard format across network components and applications. The GTD mechanism allows them to share signaling data and achieve interworking between different signaling types. This feature supports only ISDN PRI and non-facility associated signaling (NFAS) calls.

Mapping of ISDN Information Elements to GTD Parameters

ISDN messages, used to signal call control, are composed of information elements and follow the format specified in ITU-T Q.931. This feature supports only the mapping of Q931 setup messages to GTD IAM messages. This section defines the mapping of ISDN information elements to GTD parameters. Parameters are referred to by both parameter name and three-character GTD code.

Table 8 defines the mapping of ISDN IEs to GTD parameters. The GTD mechanism also passes the following parameters for which there are no corresponding ISDN IEs:

- Calling-party category (CPC)
- Forward-call indicators (FCI)
- Protocol name (PRN)

Table 8 ISDN IEs Mapped to GTD Parameters

ISDN Information Element	GTD Parameter
Bearer Capability	USI (user-service information), TMR (transmission-medium requirements)
Called Party Number	CPN (called party number)
Calling Party Number	CGN (calling-party number)
Originating Line Info	OLI (originating-line information)
Redirecting Number	RGN (redirecting number), OCN (original called number), RNI (redirection information)

GTD mapping allows up to two redirecting number (original called number) IEs per call as follows:

- If only one IE is present in the incoming setup message, then both RGN and OCN parameters are built by the ISDN stack and the RGN and OCN parameters contain the same values. Both the redirection reason (rr) field and original redirection reason (orr) field in the GTD RNI parameter contain the redirection reason indicated in the IE.
- If two IEs are present, then OCN contains information specified in the first IE and RGN contains information for the second IE. RNI contains redirection reasons. The GTD orr field indicates the redirection reason of the first IE and the GTD rr field indicates that of the second IE.

Mapping for CPN, CGN, and RGN

This section defines mapping for fields and values common to the called party number (CPN), calling party number (CGN), and redirecting information (RGN) GTD parameters carried in the GTD IAM message.

Table 9 defines mapping for ISDN type of number fields to GTD nature of address (noa) fields.

Table 9 Type of Number to Nature of Address Mapping

ISDN Type of Number	GTD Nature of Address (noa)
0—Unknown	00—Unknown (number present)
1— International number	06—Unique international number
2—National number	04—Unique national (significant) number
3—Network specific number	08—Network specific number
4—Subscriber number	02—Unique subscriber number
6—Abbreviated number	34—Abbreviated number

Table 10 defines mapping for ISDN numbering plan identification fields to GTD numbering plan indicator (npi) fields.

Table 10 Numbering Plan Identification to Numbering Plan Indicator Mapping

ISDN Numbering Plan Identification	GTD Numbering Plan Indicator (npi)
0—Unknown	u—Unknown
1—ISDN telephony numbering plan	1—ISDN numbering plan

Table 10 Numbering Plan Identification to Numbering Plan Indicator Mapping (continued)

ISDN Numbering Plan Identification	GTD Numbering Plan Indicator (npi)
2—Telephony numbering plan	1—ISDN numbering plan (best fit)
3—Data numbering plan	2—Data numbering plan
4—Telex numbering plan	3—Telex numbering plan
8—National standard numbering plan	5—National numbering plan
9—Private numbering plan	4—Private numbering plan

Table 11 defines mapping for ISDN and GTD presentation indicator (pi) fields.

Table 11 Presentation Indicator Mapping

ISDN Presentation Indicator	GTD Presentation Indicator (pi)
—	u—Unknown
0— Presentation allowed	y—Presentation allowed
1—Presentation restricted	n—Presentation not allowed
2—Number not available due to interworking	0—Address not available

Mapping for Calling Party Number (CGN)

Table 12 defines mapping for ISDN and GTD screening indicator (si) fields.

Table 12 Screening Indicator Mapping

ISDN Screening Indicator	GTD Screening Indicator (si)
—	u—Unknown
0— User-provided, not screened	1—User-provided, not screened
1—User-provided, verified and passed	2—User-provided screening passed
2—User-provided, verified and failed	3—User-provided screening failed

Mapping for Redirection Information (RNI)

Table 13 defines mapping for the ISDN reason for redirection fields to GTD original redirection reason (orr) and redirection reason (rr) fields in the GTD RNI parameter.

Table 13 Reason for Redirection to Original Redirection Reason and Redirection Reason Mapping

ISDN Reason for Redirection	GTD Original Redirection Reason (orr) and Redirection Reason (rr)
0—Unknown	u—Unknown
1—Call forwarding busy or called DTE busy	1—User busy
2—Call forwarding no reply	2—No reply
4—Call deflection	4—Deflection during alerting

Table 13 Reason for Redirection to Original Redirection Reason and Redirection Reason Mapping (continued)

ISDN Reason for Redirection	GTD Original Redirection Reason (orr) and Redirection Reason (rr)
5—Call deflection immediate response	5—Call deflection immediate response
9—Called DTE out of order	2—No reply (best fit)
10—Call forwarding by the called DTE	5—Call deflection immediate response (best fit)
13—Call transfer	5—Call deflection immediate response (best fit)
14—Call pickup	5—Call deflection immediate response (best fit)
15—Call forwarding unconditional	3—Unconditional

Mapping for Originating Line Information (OLI)

Table 14 defines mapping for OLI fields.

Table 14 Originating Line Information Mapping

ISDN Originating-Line Information	GTD Originating-Line Information (oli)
0— POTS	0—POTS
1—Multiparty line	1—Multiparty line
2—ANI failure	2—ANI failure
6—Station-level rating	6—Station-level rating
7—Special operator handling required	7—Special operator handling required
8—Inter-LATA restricted	8— Inter-LATA restricted
10—Test call	10—Test call
20—AIOD-listed DN sent	20—AIOD-listed DN sent
23—Coin or noncoin on calls using database access	23—Coin or noncoin on calls using database access
24—800 service call	24—800 service call
25— 800 service call from a pay station	25—800 service call from a pay station
27—Payphone using coin control signaling	27—Payphone using coin control signaling
29— Prison or inmate service	29—Prison or inmate service
30— Intercept (blank)	30—Intercept (blank)
31—Intercept (trouble)	31—Intercept (trouble)
32—Intercept (regular)	32—Intercept (regular)
34—Telco operator-handled call	34—Telco operator-handled call
36—CPE	36—CPE
52—OUTWATS	52—OUTWATS
60—TRS call from unrestricted line	60—TRS call from unrestricted line
61—Wireless or cellular PCS (type 1)	61—Wireless or cellular PCS (type 1)
62—Wireless or cellular PCS (type 2)	62—Wireless or cellular PCS (type 2)

Table 14 Originating Line Information Mapping (continued)

ISDN Originating-Line Information	GTD Originating-Line Information (oli)
63— Wireless or cellular PCS (roaming)	63—Wireless or cellular PCS (roaming)
66—TRS call from hotel	66—TRS call from hotel
67—TRS call from restricted line	67—TRS call from restricted line
68— Inter-LATA restricted hotel	68—Inter-LATA restricted hotel
78—Inter-LATA restricted coinless	78—Inter-LATA restricted coinless
70—Private paystations	70—Private paystations
93—Private virtual network	93—Private virtual network

Mapping for Bearer Capability (USI and TMR) Parameters

The ISDN Bearer Capability IE is mapped to the GTD User Service Information (USI) and Transmission Medium Requirements (TMR) parameters. Table 15 defines mapping for coding standard fields and values.

Table 15 ISDN to GTD Coding Standard Mapping

ISDN Coding Standard	GTD Coding Standard (cs)
0—CCITT standardized coding	c—CCITT/ITU standardized coding
1—Reserved for other international standard	i—ISO/IEC standard
2—National standard	n—National standard
3—Standard defined for the network	p—Standard defined for the network

Table 16 defines ISDN to GTD mapping for information transfer capability fields and values.

Table 16 Information Transfer Capability Mapping

ISDN Information Transfer Capability	GTD Information Transfer Capability (cap)
0—Speech	s—Speech
8—Unrestricted digital information	d—Unrestricted digital information
9—Restricted digital information	r—Restricted digital information
16—3.1-kHz audio	3—3.1-kbps audio
17—7-kHz audio	7—7-kbps audio
24—Video	v— Video

Table 17 defines mapping for transfer mode fields and values.

Table 17 Transfer Mode Mapping

ISDN Transfer Mode	GTD Transfer Mode (mode)
0—Circuit mode	c—Circuit mode
2—Packet mode	p—Packet mode

Table 18 defines mapping for information transfer rate fields and values.

Table 18 Information Transfer Rate Mapping

ISDN Information Transfer Rate	GTD Information Transfer Rate (rate)
0—Packet mode	0—Not applicable (used for packet call)
16—64 kbps	1—64 kbps
17—2x64 kbps	7—2x64 kbps
19—384 kbps	2—384 kbps
21—1536 kbps	4—1536 kbps
23—1920 kbps	5—1920 kbps

Table 19 defines mapping for transmission medium requirements.

Table 19 Transmission Medium Requirements Mapping

ISDN Information Transfer Capability	ISDN Information Transfer Rate	GTD Transmission Medium Requirements
0—Speech	—	00
8—Unrestricted digital information	16—64 kbps	01
8—Unrestricted digital information	17—2x64 kbps	04
8—Unrestricted digital information	19—384 kbps	05
8—Unrestricted digital information	21—1536 kbps	06
8—Unrestricted digital information	23—1920 kbps	07
16—3.1-kHz audio	—	02
17—7-kHz audio	—	08
24—Video	—	08

Table 20 defines mapping for structure fields and values.

Table 20 Structure Mappings

Structure	Structure (str)
0—Default	0—Default or unknown
1—8-kHz integrity	1—8-kHz integrity
4—Service data unit integrity	2—Service data unit integrity
7—Unstructured	3—Unstructured

Table 21 defines mapping for configuration fields and values.

Table 21 Configuration Field Mapping

ISDN Configuration	GTD Configuration (conf)
0—Point to point	0—Point to point

Table 22 defines mapping for establishment fields and values.

Table 22 Establishment Field Mapping

ISDN Establishment	GTD Establishment (estab)
0—Demand	d—Demand

Table 23 defines mapping for symmetry fields and values.

Table 23 Symmetry Field Mapping

ISDN Symmetry	GTD Symmetry (sym)
0—Bidirectional symmetric	sb—Symmetric bidirectional

Table 24 defines mapping for Layer 1 protocol fields and values.

Table 24 Layer 1 Protocol Mapping

ISDN Information Layer 1 Protocol	GTD Layer 1 Protocol (lay1)
1—CCITT standardized V110	v110—CCITT standardized V.110/X.30
2—G.711mu-law	ulaw—G711 mu-law
3—G.711A-law	alaw—G711 A-law
4—G.721 32 kbps	g721—G721 32 kbps
5—G.722 and G.725	g722—G.722 and G.725/G.724 7-kHz audio
6—G.7*xx* 384 video	g735—G.735 for 384 kbps video
7—Non-CCITT standardized	nonc—Non-CCITT rate adaptation
8—CCITT standardized V.120	v120—CCITT standardized V.120
9—CCITT standardized X.31	hdlc—CCITT standardized X.31

Table 25 defines mapping for synchronization fields and values.

Table 25 Synchronization Mapping

ISDN Synchronous/Asynchronous	GTD Synchronization (sync)
0—Synchronous	y—Synchronous
1—Asynchronous	n—Asynchronous

Table 26 defines mapping for negotiation fields and values.

Table 26 Negotiation Mapping

ISDN Negotiation	GTD Negotiation (neg)
0—In-band negotiation not possible	0—In-band negotiation not possible
1—In-band negotiation possible	1—In-band negotiation possible

Table 27 defines mapping for user rate fields and values.

Table 27 User-Rate Mapping

ISDN User Rate	ISDN User Rate (subrate)
0—rate is indicated by E-bits	0—rate is indicated by E-bits
1—0.6 kbps	1—0.6 kbps
2—1.2 kbps	2—1.2 kbps
3—2.4 kbps	3—2.4 kbps
4—3.6 kbps	4—3.6 kbps
5—4.8 kbps	5—4.8 kbps
6—7.2 kbps	6—7.2 kbps
7—8.0 kbps	7—8.0 kbps
8—9.6 kbps	8—9.6 kbps
9—14.4 kbps	9—14.4 kbps
10—16.0 kbps	10—16.0 kbps
11—19.2 kbps	11—19.2 kbps
12—32.0 kbps	12—32.0 kbps
14—48.0 kbps	13—48.0 kbps
15—56.0 kbps	14—56.0 kbps
16—64.0 kbps	14—56.0 kbps (best fit)
21—0.1345 kbps	15—0.1345 kbps
22—0.100 kbps	16—0.1000 kbps
23—0.075/1.2 kbps	17—0.075/1.2 kbps
24—1.2/0.075 kbps	18—1.2/0.075 kbps
25—0.050 kbps	19—0.050 kbps
26—0.075 kbps	20—0.075 kbps
27—0.110 kbps	21—0.110 kbps
28—0.150 kbps	22—0.150 kbps
29—0.200 kbps	23—0.200 kbps
30— 0.300 kbps	24—0.300 kbps
31—12 kbps	25—12 kbps

Table 28 defines mapping for intermediate rate fields and values.

Table 28 Intermediate Rate Mapping

ISDN Intermediate Rate	GTD Intermediate Rate (int)
1—8 kbps	08—8 kbps
2—16 kbps	16—16 kbps
3—32 kbps	32—32 kbps

Table 29 defines mapping for network independent clock on transmission fields and values.

Table 29 Mapping for Network Independent Clock on Transmission

ISDN Network Independent Clock on TX	ISDN Network Independent Clock on TX (txnic)
0—Not required to send data	n—Not required to send data
1—Required to send data	y—Required to send data

Table 30 defines mapping for network independent clock on reception fields and values.

Table 30 Mapping for Network Independent Clock on Reception

ISDN Network Independent Clock on RX	GTD Network Independent Clock on RX (rxnic)
0—Cannot accept data	n—Cannot accept data
1—Can accept data	y—Can accept data

Table 31 defines mapping for flow control on transmission fields and values.

Table 31 Mapping for Flow Control on Transmission

ISDN Flow Control on TX	GTD Flow Control on TX (txfl)
0—Not required to send data	n—Not required to send data
1—Required to send data	y—Required to send data

Table 32 defines mapping for flow control on reception fields and values.

Table 32 Mapping for Flow Control on Reception

ISDN Flow Control on RX	GTD Flow Control on RX (rxfl)
0—Cannot accept data	n—Cannot accept data
1—Can accept data	y—Can accept data

Table 33 defines mapping for rate adaptation header fields and values.

Table 33 Mapping for Rate Adaptation Header

ISDN Rate Adaptation Header/No Header	GTD Rate Adaptation Header (hdr)
0—Rate adaptation header not included	n—Rate adaptation header not included
1—Rate adaptation header included	y—Rate adaptation header included

Table 34 defines mapping for multiframe establishment support for data link fields and values.

Table 34 Mapping for Multiframe Establishment (MFE) Support

ISDN MFE Support in Data Link	GTD MFE Support in Data Link (mf)
0—MFE not supported	n—MFE not supported
1—MFE supported	y—MFE supported

Table 35 defines mapping for mode of operation fields and values.

Table 35 Mode of Operation Mapping

ISDN Mode of Operation	GTD Mode of Operation (mode)
0—Bit-transparent mode of operation	0—Bit-transparent mode of operation
1—Protocol-sensitive mode of operation	1—Protocol-sensitive mode of operation

Table 36 defines mapping for logical link identifier negotiation fields and values.

Table 36 Logical Link Identifier (LLI) Mapping

ISDN LLI Negotiation	GTD LLI Negotiation (lli)
0—Default	0—Default
1—Full protocol negotiation	1—Full-protocol negotiation

Table 37 defines mapping for assignor and assignee fields and values.

Table 37 Mapping for Assignor and Assignee

ISDN Assignor and Assignee	GTD Assignor and Assignee (asgn)
0—Message originator is default assignee	0—Message originator is default assignee
1—Message originator is assignor only	1—Message originator is assignor only

Table 38 defines mapping for in-band and out-of-band negotiation fields and values.

Table 38 Mapping for Inband and Out-of-Band Negotiation

ISDN In-band and Out-of-Band Negotiation	GTD In-band and Out-of-Band Negotiation (inbnd)
0—Negotiation done with USER INFO	0— Not applicable to this protocol
1—Negotiation done in-band	1— Negotiation done in-band

Table 39 defines mapping for fields and values for number of stop bits.

Table 39 Mapping for Number of Stop Bits

ISDN Number of Stop Bits	GTD Number of Stop Bits (stp)
1—1 bit	1—1 bit
2—1.5 bit	3—1.5 bit
3—2 bits	2—2 bits

Table 40 defines mapping for fields and values for number of data bits.

Table 40 Mapping for Number of Data Bits

ISDN Number of Data Bits	GTD Number of Data Bits (dat)
1—5 bits	5—5 bits
2—7 bits	7—7 bits
3—8 bits	8—8 bits

Table 41 defines mapping for parity information fields and values.

Table 41 Parity Mapping

ISDN Parity Information	GTD Parity (par)
0—Odd	o—Odd
2—Even	e—Even
3—None	n—None
4—Forced to 0	0—Forced to 0
5—Forced to 1	1— Forced to 1

Table 42 defines mapping for duplex mode fields and values.

Table 42 Duplex Mode Mapping

ISDN Duplex Mode	GTD Duplex (dup1)
0—Half duplex	h—Half duplex
1—Full duplex	f—Full duplex

Table 43 defines mapping for modem type fields and values.

Table 43 Modem Type Mapping

Modem Type	Modem Type (modm)
1—V.21	11—V.21
2—V.22	00—V.22
3—V.22 *bis*	01—V.22 *bis*
4—V.23	02—V.23
5—V.26	03—V.26
6—V.26 *bis*	04—V.26 *bis*
7—V.26 ter	05—V.26 ter
8 —V.27	06—V.27
9—V.27 *bis*	07—V.27 *bis*
10—V.27 ter	08—V.27 ter
11—V.29	09—V.29
12—V.32	10—V.32
13—V.35	12—V.34 (best fit)

Table 44 defines mapping for Layer 2 protocol fields and values.

Table 44 Layer 2 Protocol Mapping

ISDN User Information Layer 2 Protocol	GTD Layer 2 Protocol (lay2)
2—Q.921	2—Q.921
6—X.25	1—X.25

Table 45 defines mapping for Layer 3 protocol fields and values.

Table 45 Layer 3 Protocol Mapping

ISDN User Information Layer 3 Protocol	GTD Layer 3 Protocol (lay3)
2—Q.931	2—Q.931
6—X.25	1—X.25

How to Configure ISDN GTD for Setup Message

This section contains the following procedures:

- Configuring ISDN GTD for Setup Messages, page 133 (optional)
- Configuring the OLI IE to Interface with MCI Switches, page 133 (optional)
- Verifying ISDN GTD, page 134
- Troubleshooting Tips, page 135

Configuring ISDN GTD for Setup Messages

This feature is enabled by default; no configuration tasks are required to enable this feature. To reenable the feature if it was disabled by use of the **no isdn gtd** command, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface**
4. **isdn gtd**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** **Example:** `Router(config)# interface`	Enters interface configuration mode.
Step 4	**isdn gtd** **Example:** `Router(config-if)# isdn gtd`	Enables GTD parameter mapping for ISDN IEs.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configuring the OLI IE to Interface with MCI Switches

To configure OLI IE to interface with MCI switches, perform the following steps.

Note You must configure the Cisco IOS gateway to support the switch variant from which the gateway receives ISDN signaling. For a gateway that interfaces to an MCI switch or PBX, the OLI IE identifier for the MCI ISDN variant, as defined in *CPE Requirements for MCI ISDN Primary Rate Interface,* (014-0018-04.3D-ER, revision 4.3D), is configurable. Select the IE value that indicates OLI information to configure gateway support for the MCI ISDN variant.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface**
4. **isdn ie oli**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** **Example:** `Router(config)# interface`	Enters interface configuration mode.
Step 4	**isdn ie oli** *value* **Example:** `Router(config-if)# isdn ie oli 7F`	Configures the OLI IE identifier to allow the gateway to interface with an MCI switch. OLI IE identifier values are in hexadecimal format. Values range from 00 to 7F.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verifying ISDN GTD

To verify the interface, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show isdn status**
2. **show running-config**

DETAILED STEPS

Step 1 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 2 **show running-config**

Use this command to display the configuration for the ISDN GTD for Setup Messages feature. If GTD mapping is enabled (default), command output does not display the **isdn gtd** command.

Troubleshooting Tips

- Use the **debug gtd details** command to display GTD details.
- Use the **debug gtd error** command to display GTD errors.
- Use the **debug gtd events** command to display GTD events.

Examples

This section provides the following output example:

- Sample Output for the debug gtd events Command, page 135

Sample Output for the debug gtd events Command

```
Router# debug gtd events

00:05:19:%SYS-5-CONFIG_I:Configured from console by console
*Aug  8 06:32:20.915:ISDN Se3:23 Q931:RX <- SETUP pd = 8  callref = 0x0002
        Bearer Capability i = 0x8890
                Standard = CCITT
                Transer Capability = Unrestricted Digital
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA98397
                Exclusive, Channel 23
        Called Party Number i = 0x81, '9999'
                Plan:ISDN, Type:Unknown
*Aug  8 06:32:20.919:ISDN Se3:23:Built a GTD of size 86 octets for ISDN message type 0x5
*Aug  8 06:32:20.919:tsp_ccrawmsg_encap:calling cdapi_find_tsm
*Aug  8 06:32:20.919:cdapi_find_tsm:Found Tunnelled Signaling Msg with GTD:PROT_PTYPE_GTD
*Aug  8 06:32:20.919:cdapi_find_tsm:Found a gtd msg of length 86:
*Aug  8 06:32:20.919:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
```

```
CPC,09
FCI,,,,,,y,"

*Aug  8 06:32:20.923:ccGTDExtractParm:Starting
*Aug  8 06:32:20.923: tunnelledPtype = 2
*Aug  8 06:32:20.923: gtdInstance = 0
*Aug  8 06:32:20.923: gtdBitMap = 0xFFFFFFFF
*Aug  8 06:32:20.923:ccGTDExtractParm:TunnelledContent has GTD message
*Aug  8 06:32:20.923:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
CPC,09
FCI,,,,,,y,"

*Aug  8 06:32:20.927:ccGTDExtractParm:GTD Parm CPC obtained
*Aug  8 06:32:20.927:ccGTDExtractParm:GTD Parm TMR obtained
*Aug  8 06:32:20.927:ccGTDExtractParm:GTD Parm PRN obtained
*Aug  8 06:32:21.547:ccMapGCItoGUID:GTD Parm GCI not present
*Aug  8 06:32:21.547:ccMapGUIDtoGCI:Modified GTD string to include GCI
*Aug  8 06:32:21.547:ccMapGUIDtoGCI:Calling update_gtd_in_raw_msg_buffer
*Aug  8 06:32:21.547:update_gtd_in_raw_msg_buffer:Inserting 124 byte GTD string into
rawmsg buffer.
The new gtd string is:
*Aug  8 06:32:21.547:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
CPC,09
FCI,,,,,,y,
GCI,7ba32c886c2c11d48005b0f6ff40a2c1"

*Aug  8 06:32:21.547:update_gtd_in_raw_msg_buffer:Original rawmsg buf length is 115
the original gtd length was 86
the new gtd length is = 124
*Aug  8 06:32:21.547:update_gtd_in_raw_msg_buffer:New data and IE inserted in rawmsg buff,
rawmsg buf length is now 153
*Aug  8 06:32:21.551:Have gtd msg, length=124:
*Aug  8 06:32:21.551:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
CPC,09
FCI,,,,,,y,
GCI,7ba32c886c2c11d48005b0f6ff40a2c1"

*Aug  8 06:32:21.555:Have gtd msg, length=124:
*Aug  8 06:32:21.555:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
CPC,09
FCI,,,,,,y,
GCI,7ba32c886c2c11d48005b0f6ff40a2c1"

*Aug  8 06:32:21.559:ccMapGUIDtoGCI:GTD Parm GCI is
present:7ba32c886c2c11d48005b0f6ff40a2c1, just returning
*Aug  8 06:32:21.559:ccGTDExtractParm:Starting
*Aug  8 06:32:21.559: tunnelledPtype = 2
*Aug  8 06:32:21.559: gtdInstance = 0
```

```
*Aug  8 06:32:21.559: gtdBitMap = 0xFFFBFFFF
*Aug  8 06:32:21.559:ccGTDExtractParm:TunnelledContent has GTD message
*Aug  8 06:32:21.559:gtd msg = "IAM,
PRN,isdn*,,,
USI,rate,c,d,c,1
TMR,01
CPN,00,,1,9999
CPC,09
FCI,,,,,,,y,
GCI,7ba32c886c2c11d48005b0f6ff40a2c1"

*Aug  8 06:32:21.559:ccGTDExtractParm:GTD Parm CPC obtained
*Aug  8 06:32:21.559:ccGTDExtractParm:GTD Parm TMR obtained
*Aug  8 06:32:21.563:ccGTDExtractParm:GTD Parm PRN obtained
*Aug  8 06:32:21.563:ISDN Se3:23 Q931:TX -> CALL_PROC pd = 8  callref = 0x8002
        Channel ID i = 0xA98397
                Exclusive, Channel 23
```

Configuration Examples for ISDN Generic Transparency Descriptor (GTD) for Setup Message

This section contains the following configuration examples:

GTD Mapping: Example

Note The GTD feature is different from the **isdn map** command.

The following example shows that GTD mapping is enabled:

```
enable
configure terminal
interface
    isdn gtd
```

OLI IE: Example

The following example shows that the OLI IE identifier for interfacing to an MCI switch is set to 7F:

```
enable
configure terminal
interface
    isdn ie oli 7F
```

OLI IE and GTD: Example

The following example shows that isdn gtd command is disabled and that the OLI IE identifier is set to 1F in the D channel of the T1 line in slot 3 (serial3:23):

```
Router# show running-config

Building configuration...

Current configuration :4112 bytes
!
version 12.2
no parser cache
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot system flash:c5300-i-mz.122-4.2
no logging buffered
enable secret
enable password
!
username guam password
username user1 password
username user2 password
spe 2/0 2/7
 firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
!
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
ip host nlab-boot 172.21.200.2
ip host dirt 172.69.1.129
ip host dsbu-web.cisco.com 172.19.192.254 172.71.162.82
ip host lab 172.19.192.254
!
isdn switch-type primary-ni
isdn gateway-max-interworking
!
trunk group  1
 carrier-id cd1
 max-retry 2
 hunt-scheme random
!
trunk group  2
 max-retry 2
 hunt-scheme random
!
voice service voip
!
no voice hpi capture buffer
no voice hpi capture destination
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 0
 framing esf
 clock source line primary
```

```
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
 no yellow generation
 no yellow detection
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24 nfas_d backup nfas_int 1 nfas_group 0
 no yellow generation
 no yellow detection
!
controller T1 2
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 0
 no yellow generation
 no yellow detection
!
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
 no yellow generation
 no yellow detection
!
interface Ethernet0
 ip address 10.0.44.29 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 no cdp enable
!
interface Serial0:23
 ip address 10.1.1.2 255.255.255.0
 dialer map ip 10.1.1.1 name host 1111
 dialer-group 1
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn T310 30000
 isdn negotiate-bchan
 isdn bchan-number-order descending
 no cdp enable
!
interface Serial3:23
 ip address 10.9.9.9 255.255.255.0
 dialer map ip 10.8.8.8 name host 8888
 dialer map ip 10.8.8.8 255.255.255.0
 dialer-group 1
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice modem
 isdn disconnect-cause 126
 no isdn outgoing display-ie
 isdn ie oli 1F
 no isdn gtd
 no cdp enable
!
interface FastEthernet0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex auto
```

```
 speed auto
 no cdp enable
!
interface Group-Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer-group 1
 no keepalive
 group-range 1 96
!
interface Dialer1
 ip address 10.2.2.2 255.255.255.0
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer remote-name host
 dialer-group 1
 no fair-queue
!
interface Dialer2
 no ip address
 no cdp enable
!
interface Dialer5
 ip address 10.1.1.1 255.0.0.0
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer in-band
 dialer map ip 10.1.1.2 name host 1234567
 dialer-group 1
 ppp authentication chap
!
ip default-gateway 10.0.44.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.44.1
ip route 0.0.0.0 0.0.0.0 Ethernet0
no ip http server
!
access-list 101 permit ip any any
dialer-list 1 protocol ip permit
no cdp run
!
snmp-server enable traps tty
snmp-server enable traps isdn layer2
snmp-server host 10.1.1.1 public
!
call rsvp-sync
!
voice-port 0:D
!
voice-port 3:D
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 2 voip
 destination-pattern 111
 session target ipv4:10.0.45.87
!
dial-peer voice 10 pots
 destination-pattern 9999
```

```
 direct-inward-dial
 port 3:D
 prefix 9999
!
dial-peer voice 20 voip
 destination-pattern 000000002.
 session target ipv4:10.0.44.28
!
dial-peer voice 50 pots
 destination-pattern 2222
 direct-inward-dial
 port 0:D
 prefix 2222
!
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 logging synchronous
line 1 96
 no flush-at-activation
 modem InOut
 transport input all
 transport output lat pad telnet rlogin udptn v120 lapb-ta
line aux 0
line vty 0 4
 password
 login
!
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- *RADIUS VSA Voice Implementation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm
- *Tcl IVR API Version 2.0 Programmer's Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/index.htm

Implementing NFAS

This chapter describes how to implement the Non-Facility Associated Signaling (NFAS) with D-Channel Backup feature with two new switch types: DMS100 and NI2. ISDN NFAS allows a single D channel to control multiple ISDN PRI interfaces. You can configure a backup D channel for use when the primary NFAS D channel fails.

Once you configure channelized T1 controllers for ISDN PRI, you need configure to only the NFAS primary D channel; its configuration is distributed to all the members of the associated NFAS group.

Note A controller configured with backup D channel loses one B channel.

Use of a single D channel to control up to 10 PRI interfaces can free one B channel on each interface to carry other traffic.

Any hard failure causes a switchover to the backup D channel and currently connected calls remain connected. The backup D channel cannot be used for data transfer.

Note On the Nortel dms100 switch, when a single D channel is shared, multiple PRI interfaces may be configured in a single trunk group. The additional use of alternate route indexing, which is a feature of the dms100 switch, provides a rotary from one trunk group to another. This enables the capability of building large trunk groups in a public switched network.

Feature History for NFAS with D-Channel Backup

Release	Modification
12.1(5)XM	This feature was introduced.
12.2(11)T	This feature was implemented on the Cisco AS5850 platform.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 153.

Contents

Prerequisites for Configuring NFAS with D-Channel Backup

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.
- Configure your router's channelized T1 controllers for ISDN, as described in the "Configuring ISDN PRI" section of the "Configuring Channelized E1 and Channelized T1" chapter in the *Dial Solutions Quick Configuration Guide*.

Restrictions for Configuring NFAS with D-Channel Backup

Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4. In addition, the following apply:

- NFAS is supported with only a channelized T1 controller and, as a result, is ISDN PRI capable.
- The router must connect to either a 4ess, dms250, dms100, or National ISDN switch type. Table 46 shows applicable ISDN switch types and supported NFAS types.

Table 46 ISDN Switch Types and Supported NFAS Types

ISDN Switch Type	NFAS Type
Lucent 4ESS	Custom NFAS
Nortel DMS250	Custom NFAS
Nortel DMS100	Custom NFAS
Lucent 5ESS	Custom; does not support NFAS

Table 46 ISDN Switch Types and Supported NFAS Types (continued)

ISDN Switch Type	NFAS Type
Lucent 5ESS	NI-2 NFAS
AGCS GTD5	NI-2 NFAS
Other switch types	NI-2 NFAS

Information about NFAS

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

Non-Facility Associated Signaling is a classification of signalling protocols that provide the signalling channel in a separate physical line from the bearer channels.

How to Configure NFAS with D-Channel Backup

This section contains the following procedures:

Configuring NFAS on PRI Groups

To configure NFAS on PRI groups, perform the following steps.

Note When a backup NFAS D channel is configured and the primary NFAS D channel fails, rollover to the backup D channel is automatic and all connected calls stay connected. If the primary NFAS D channel recovers, the backup NFAS D channel remains active and does not switch over again unless the backup NFAS D channel fails.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **pri-group timeslots nfas_d primary nfas_interface nfas_group**
5. **pri-group timeslots nfas_d backup nfas_interface nfas_group**
6. **pri-group timeslots 1-24 nfas_d none nfas_int nfas_group**

7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**controller** {**t1** | **e1**} *controller-number* **Example:** `Router(config)# controller t1 3`	Enters controller configuration mode for the specified controller number.
Step 4	**pri-group timeslots** *range* **nfas_d primary nfas_interface** *number* **nfas_group** *number* **Example:** `Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_interface 1 nfas_group 1`	Configures, on one channelized T1 controller, the NFAS primary D channel. Keywords are as follows: • **nfas_interface** *number*—Value assigned by the service provider to ensure unique identification of a PRI interface. • **nfas_group** *number*—Group identifier unique on the router. Multiple NFAS groups can exist on the router. The interface number is the number of the interface assigned to an interface that is part of an nfas group. All interfaces that are part of an nfas group have the same group number and each is identified uniquely within the group by the interface number.
Step 5	**pri-group timeslots** *range* **nfas_d backup nfas_interface** *number* **nfas_group** *number* **Example:** `Router(config-controller)# pri-group timeslots 1-24 nfas_d backup nfas_interface 2 nfas_group 1`	Configures, on a different channelized T1 controller, the NFAS backup D channel to be used if the primary D channel fails. Keywords are as above. Repeat this step on other channelized T1 controllers, as appropriate.
Step 6	**pri-group timeslots 1-24 nfas_d none nfas_int** *number* **nfas_group** *number* **Example:** `Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 3 nfas_group 1`	(Optional) Configures, on other channelized T1 controllers, a 24 B channel interface, if desired.
Step 7	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configuring a VoIP Dial Peer for NFAS Voice

To configure a VoIP dial peer for NFAS voice, perform the following steps.

Note Dial peers are used by the Cisco IOS voice stack for handling calls going from the PSTN to the VoIP side or vice versa. The dial-peer configuration for each NFAS controller should contain the primary of the NFAS group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice voip**
4. **port**
5. **exit**

DETAILED STEPS

	Commands	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 99 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	**port** *controller*:**D** **Example:** `Router(config-dial-peer)# port 4:D`	Associates the dial peer with a specific voice port—in this case, the D channel associated with ISDN PRI for the NFAS primary.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Disabling a Channel or Interface

To disable a channel or interface, perform the following steps.

Note You can disable a specified channel or an entire PRI, thus taking it out of service or put it into one of the other states that is passed in to the switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn service dsl b_channel state**
4. **isdn service dsl b_channel 0 state**
5. **exit**

DETAILED STEPS

	Commands	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**isdn service** [**dsl** *number* | **nfas_int** *number*] **b_channel** *number* **state** {**0** | **1** | **2**} **Example:** `Router(config)# isdn service nfas_int 3 b_channel 1 state 1`	Takes an individual B channel out of service or sets it to a different state. State values are as follows: • **0**—In service • **1**—Maintenance • **2**—Out of service
Step 4	**isdn service** [**dsl** *number* | **nfas_int** *number*] **b_channel 0 state** {**0** | **1** | **2**} **Example:** `Router(config)# isdn service nfas_int 3 b_channel 0 state 1`	As above. Setting the b-channel number to 0 sets the entire PRI interface to a specified state value.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Verifying NFAS Configuration

To verify NFAS configuration, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show dial-peer voice**
2. **show isdn nfas group**
3. **show isdn service**
4. **show isdn status**
5. **show running-config**

DETAILED STEPS

Step 1 show dial-peer voice

Use this command to display the configuration information for dial peers.

```
Router# show dial-peer voice

VoiceOverIpPeer1
        information type = voice,
        tag = 1, destination-pattern = `',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1, Admin state is up, Operation state is down,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem passthrough = system,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = voip, session-target = `',
        technology prefix:
        settle-call = disabled
        ip precedence = 0, UDP checksum = disabled,
        session-protocol = cisco, session-transport = udp, req-qos = best-effor
        acc-qos = best-effort,
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout: Mode adaptive,
        Expect factor = 0,
        Max Redirects = 1, Icpif = 20,signaling-type = cas,
        CLID Restrict = disabled
        VAD = enabled, Poor QOV Trap = disabled,
        voice class perm tag = `'
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
```

Step 2 show isdn nfas group

Use this command to display information about members of an NFAS group.

```
Router# show isdn nfas group 1

ISDN NFAS GROUP 1 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.
There are 3 total nfas members.
There are 93 total available B channels.
The primary D-channel is DSL 0 in state INITIALIZED.
The backup D-channel is DSL 1 in state INITIALIZED.
The current active layer 2 DSL is 1.
```

Step 3 **show isdn service**

Use this command to display information about ISDN channels and the service states.

Step 4 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 5 **show running-config**

Use this command to display the basic router configuration.

Examples

This section provides the following output examples:

- Sample Output for the show isdn nfas group Command, page 150

Sample Output for the show isdn nfas group Command

The following three examples show D channel state changes when rollover occurs from the primary NFAS D channel to the backup D channel. The first example shows the output with the primary D channel in service and the backup D channel in standby.

```
Router# show isdn nfas group 0

ISDN NFAS GROUP 0 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.
There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state IN SERVICE.
The backup D-channel is DSL 1 in state STANDBY.
The current active layer 2 DSL is 0.
```

The following example shows output during rollover. The configured primary D channel is in maintenance busy state and the backup D channel is waiting.

```
Router# show isdn nfas group 0

ISDN NFAS GROUP 0 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.
There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state MAINTENANCE BUSY.
The backup D-channel is DSL 1 in state WAIT.
```

```
The current active layer 2 DSL is 1.
```

The following example shows output when rollover is complete. The configured primary D channel is now in standby and the backup D channel is in service.

```
Router# show isdn nfas group 0

ISDN NFAS GROUP 0 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.
There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state STANDBY.
The backup D-channel is DSL 1 in state IN SERVICE.
The current active layer 2 DSL is 1.
```

Configuration Examples for NFAS with D-Channel Backup

This section contains the following configuration examples:

NFAS Primary and Backup D Channels: Example

The following example configures ISDN PRI and NFAS on multiple T1 controllers of a Cisco 7500 series router. The D-channel of T1 1/0/0 is configured as primary D-channel and T1 1/0/1 is configured as backup D-channel. Once you configure the NFAS primary D channel, that channel is the only interface you see and have to configure.

```
version 12.x
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname travis-nas-01
!
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHENT none
aaa authorization exec default local if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default local if-authenticated
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default start-stop group tacacs+
aaa accounting exec NO_ACCOUNT none
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting commands 15 NO_ACCOUNT none
enable secret 5 $1$LsoW$K/qBH9Ih2WstUxvazDgmY/
!
username admin privilege 15 password 7 06455E365E471D1C17
username gmcmilla password 7 071824404D06140044
username krist privilege 15 password 7 0832454D01181118
!
call rsvp-sync
shelf-id 0 router-shelf
```

```
shelf-id 1 dial-shelf
!
resource-pool disable
!
modem-pool Default
 pool-range 1/2/0-1/2/143,1/3/0-1/3/143
!
clock timezone CST -6
clock summer-time CST recurring
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 172.22.53.210
ip name-server 171.69.2.133
ip name-server 171.69.2.132
ip name-server 171.69.11.48
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
!
controller T1 1/0/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_interface 1 nfas_group 1
 description PacBell 3241933
!

controller T1 1/0/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d backup nfas_interface 2 nfas_group 1
 description PacBell 3241933
!
interface Loopback0
 ip address 172.21.10.1 255.255.255.255
!
interface FastEthernet0/0/0
 ip address 172.21.101.20 255.255.255.0
 half-duplex
!
interface Serial1/0/0:23
 no ip address
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Group-Async0
 no ip address
 group-range 1/2/00 1/3/143
!
router eigrp 1
 network 172.21.0.0
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.101.1
ip http server
ip http authentication aaa
!
snmp-server engineID local 0000000902000030F2F51400
snmp-server community 5urf5h0p RO
snmp-server community 5crapmeta1 RW
snmp-server community SNMPv1 view v1default RO
```

POTS Dial-Peer Configuration: Example

The following example shows configuration of a POTS dial peer with the primary controller of an NFAS group:

```
dial-peer voice 35 pots
           incoming called-number 45...
    destination-pattern 35...
    direct-inward-dial
    port 1/0/0:D
    prefix 35
```

PRI Service State: Example

The following example reenables the entire PRI after it was disabled:

```
isdn service dsl 0 b-channel 0 state 0
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

Implementing SCTP Features

This chapter describes how to implement Stream Control Transmission Protocol (SCTP) features. SCTP is not explicitly configured on routers, but it underlies several Cisco applications. This chapter describes how to configure several features that use SCTP and how to troubleshoot SCTP problems.

SCTP is used with the following Cisco IOS software features:

- PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer
- Support for IUA with SCTP for Cisco Access Servers

Feature History for PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer

Release	Modification
12.1(1)T	This feature was introduced on the Cisco AS5300.
12.2(4)T	This feature was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.2(2)XB1	This feature was implemented on the Cisco AS5850.

Feature History for Support for IUA with SCTP for Cisco Access Servers

Release	Modification
12.2(15)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 210.

Contents

Prerequisites for Implementing SCTP Features

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.

PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer Feature

- Configure ISDN to backhaul Q.921 signaling to the media gateway controller
- For Cisco AS5850, install or implement the following:
  - MGCP 1.0
  - IUA 0.4
  - ISDN network-side support to terminate multiple voice PRIs

Restrictions for Implementing SCTP Features

Restrictions are described in the "Restrictions for Configuring ISDN Voice Interfaces" section on page 4. In addition, the following apply.

PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer Feature

- Backhaul: Does not support backhauling for Basic Rate Interface (BRI).
- Capacity: Supports only two application-server processes (ASPs) per application server. Supports only three explicit IP addresses per SCTP association endpoint.
- IUA messages: Does not support new-traffic failover.

Note The IUA specification describes an optional feature known as New Traffic Failover. In this process, all messages for calls pending completion during failover are sent to the inactive media-gateway controller, and messages for new calls are sent to the newly active controller. These IUA messages for new calls are not supported.

- Load balancing: Does not support load balancing between ASPs on a per-call basis.
- Platforms: Is not supported on the Cisco 2600XM series, Cisco 2691, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.

- Signaling: Supports Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) PRI D-channel signaling only; does not support any other signaling protocols, including NFAS with backup D-channel signaling.

Support for IUA with SCTP for Cisco Access Servers Feature

- Backhaul: Does not support Q.931 PRI backhaul on the Cisco PGW 2200.
- Platforms: Is not supported on the Cisco 2600XM series or Cisco 2691.
- Transport: Does not support concurrent Redundant Link Manager (RLM) and SCTP transport on the access-server gateway. You can configure one or the other but not both at the same time.

Note

- For more information about the Cisco PGW 2200, see *Support for IUA with SCTP*.
- For more information about IUA with SCTP, see *Support for IUA with SCTP for Cisco Access Servers*.

Information About SCTP and SCTP Features

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

To configure SCTP, you should understand the following concepts:

SCTP Topology

SCTP is a reliable datagram-oriented IP transport protocol specified by RFC 2960. It provides the layer between an SCTP user application and an unreliable end-to-end datagram service such as IP. The basic service offered by SCTP is the reliable transfer of user datagrams between peer SCTP users, within the context of an association between two SCTP hosts. SCTP is connection-oriented, but SCTP association is a broader concept than, for example, TCP connection.

SCTP provides the means for each SCTP endpoint to provide its peer with a list of transport addresses during association startup (address and UDP port combinations, for example) through which that endpoint can be reached and from which messages originate. The association spans transfer over all of the possible source and destination combinations that might be generated from the two endpoint lists (also known as multihoming).

SCTP provides the following services and features:

- Acknowledged reliable nonduplicated transfer of user data
- Application-level segmentation to conform to the maximum transmission unit (MTU) size

- Sequenced delivery of user datagrams within multiple streams
- Optional multiplexing of user datagrams into SCTP datagrams
- Enhanced reliability through support of multihoming at either end or both ends of the association
- Congestion avoidance and resistance to flooding and masquerade attacks
- Interoperability with third-party call agents

SCTP allows you to terminate multiple switches and trunk groups on a gateway to add scalability. Adding trunk groups does not require more memory or processing resources because SCTP supports multiple streams in a single SCTP association. SCTP is a reliable transport protocol for message-oriented communications; SCTP is specifically designed to support PSTN signaling messages over IP networks.

SCTP allows you to configure at least one trunk group per T1 or E1 interface available on a given platform. A gateway platform with four T1 or E1 interfaces, for example, can control four unique trunk groups per device. Certain platforms, such as the Cisco AS5800 and Cisco AS5850, can deliver the individual T1 or E1 trunk groups over a high-speed interface, such as T3, which operates at 45 Mbps.

Table 47 shows the number of trunk groups supported per gateway platform.

Table 47 SS7 Interconnect for Voice-Gateway Trunk Groups per Gateway

Platform	Supported Trunk Groups	Comments
Cisco AS5300	4	Verify both T1 and E1 cards.
Cisco AS5350	8	Verify both T1 and E1 cards. Verify with Integrated SLT option. **Note** For more information, see *Integrated Signaling Link Terminal*, Cisco IOS Release 12.2(11)T.
Cisco AS5350 CT3	28	Verify CT3 DS-3 card. Verify with Integrated SLT option.
Cisco AS5400	16	Verify both T1 and E1 cards. Verify with Integrated SLT option.
Cisco AS5400 CT3	28	Verify CT3 DS-3 card. Verify with Integrated SLT option.
Cisco AS5850	112	Verify E1 cards and CT3 DS-3 cards. **Note** T1 ports and the 112 supported trunk groups are available only with CT3 cards.

In a typical network topology, only one SCTP association is configured between a signaling controller and a gateway. Multiple IP addresses on either side can be designated to the same association to achieve link redundancy. On a gateway, signaling messages for all trunk groups are carried over on the same SCTP association to the same signaling controller. Trunk groups on a gateway can also be controlled through different signaling controllers. In such cases, you can configure multiple associations on a gateway and direct them to different signaling controllers.

IUA

IUA is the adaptation layer that makes SCTP services available to Q.921 services users, such as Q.931, Q Signaling (QSIG), and National ISDN-2 with Cisco extensions (Cisco NI2+). IUA supports the standard interlayer primitives provided by Q.921. As a result, an upper-layer protocol (ULP) that typically used Q.921 services can easily migrate to IUA.

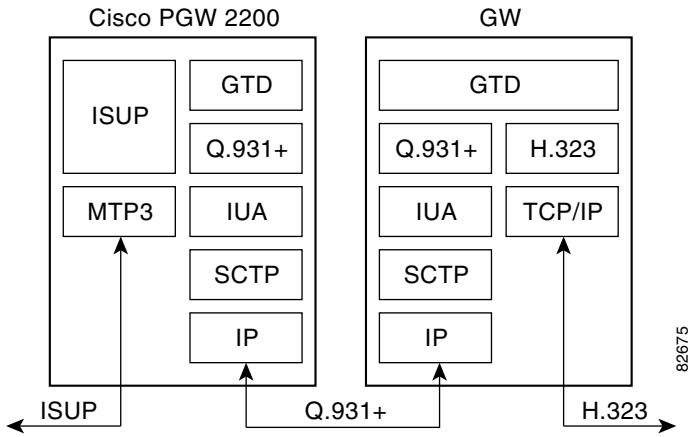
IUA service points are represented to the upper-layer protocol as application servers. Each application server is bound to an SCTP local endpoint managed by an SCTP instance. A remote signaling controller is known as an ASP. An ASP is connected to the local endpoint through a single SCTP association.

The IUA module creates associations between the signaling gateway and the MGC based on configuration requests. It also manages multiple ASPs as defined in the IETF IUA specification. IUA performs the following functions:

- Requests SCTP associations based on configuration information.
- Manages the destination address list and requests a new primary destination in the event of a failure.
- Manages the ASP state machine for each association.
- Manages the application-server state machine across all ASPs associated with a single application.
- Provides service for multiple applications simultaneously to handle different Layer 3 signaling protocols (Q.931 and Q.SIG, for example), or to communicate with different sets of call agents.

Figure 7 shows IUA with SCTP transport stack.

Figure 7 IUA with SCTP Transport Stack



To use IUA services, you must make the application server and ASP available and bind a trunk group to an application server for its Layer 2 server. For configuration information, see the "Configure IUA" section on page 166.

Multiple NFAS Groups

On a gateway, trunk groups are defined as Non-Facility Associated Signaling (NFAS) groups. An NFAS group is a group of ISDN PRI trunks with a single dedicated D channel. In a voice-gateway solution, the D channel in a trunk group is symbolic because SS7 is used as the signaling mechanism. The D channels defined for each NFAS group are actually DS0 bearer channels for voice or modem calls. Therefore, each NFAS has a corresponding D channel for which it is allocated.

A symbolic D-channel interface is dedicated to a trunk group. Each D-channel interface is bound to an application server and a dedicated stream is associated with this interface. Thus, the NFAS group identification can be recovered on each side of the SCTP association through this two-stage mapping as long as both sides share the same configuration information. Multiplexing of multiple trunk groups through a single association is accomplished this way, for example. If all interfaces on a gateway are controlled through a single SC, all interfaces are bound to the same application server.

The SCTP stream is a logical identification of the grouping of messages and consumes little additional memory and processing power. Each association can support as many as 65,355 streams.

Figure 8 shows the mapping between the trunk group, D-channel interface, and SCTP stream.

Figure 8 Mapping Between Trunk Group, Interface, and Stream

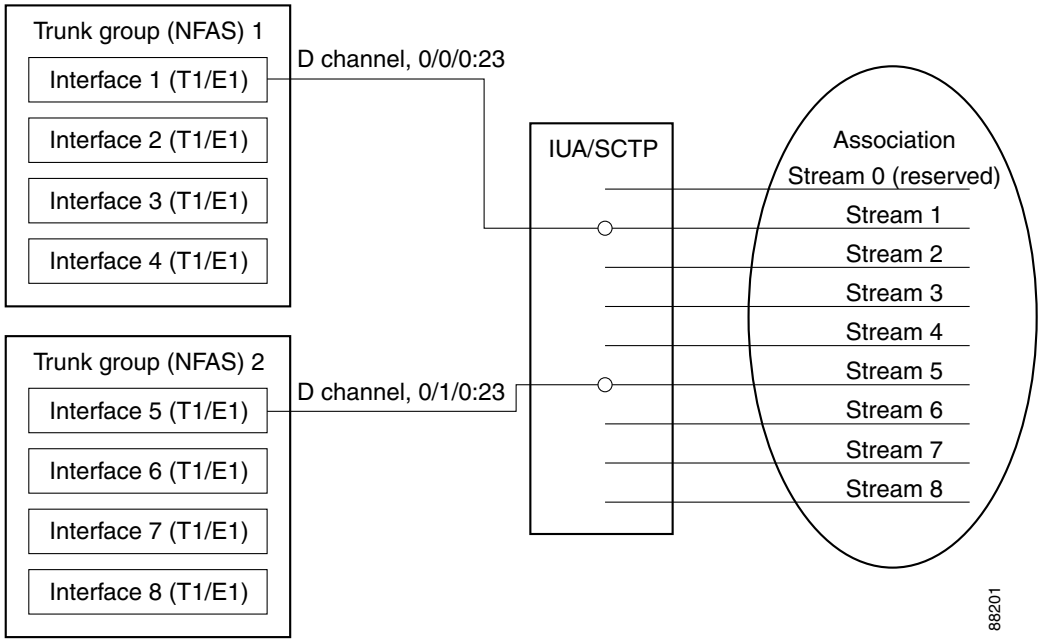
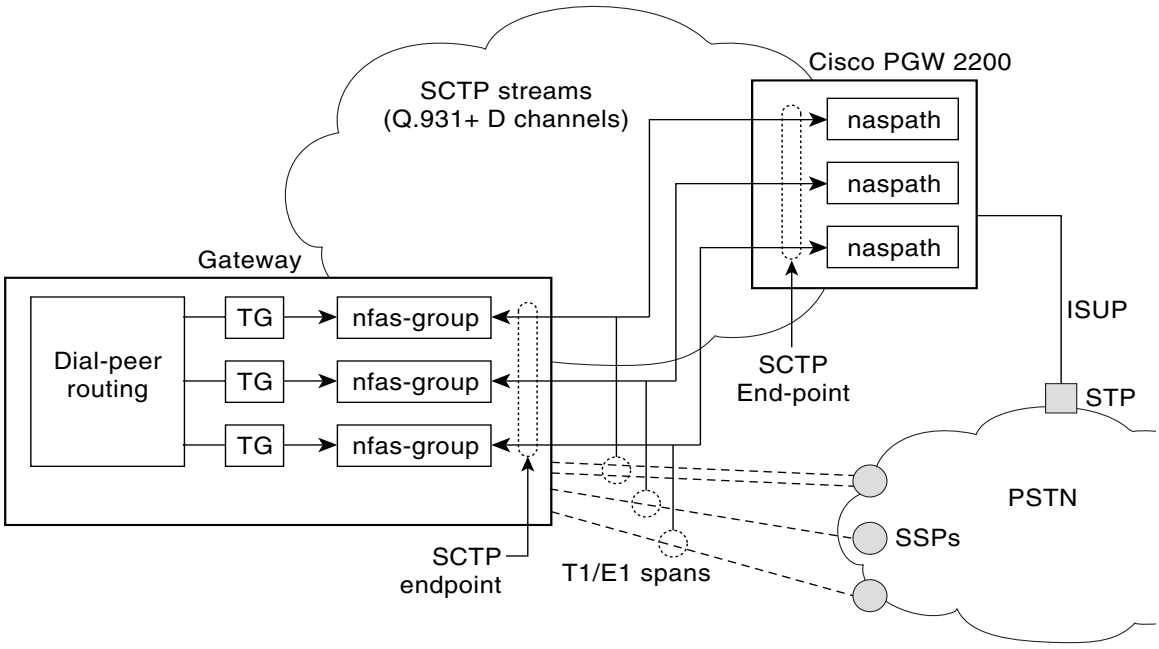


Figure 9 shows the NFAS group and SCTP association.

Figure 9 NFAS Group and SCTP Association



The IUA transport protocol using SCTP is supported on the Cisco PGW 2200; the Cisco PGW 2200 now uses IUA to communicate with Cisco access servers.

IUA with SCTP on the Cisco PGW 2200 provides the following services:

- Eliminates the scaling limitations in previous releases of Cisco MGC software for the number of NFAS-groups allowed per RLM.
- Supports upgrading from RLM-based communication to IUA-based communication without losing stable active calls.
- RLM-based communication is still supported. However, since this is a new functionality, the backward compatibility of the SCTP-based transports is not applicable.
- IUA interface can be used with Cisco access servers that support NAS and Digital Private Network Signaling System (DPNSS) signaling.
- Introduces IUA and SCTP operational measurements.

Note For more information about IUA and SCTP on the Cisco PGW 2200, see *Support for IUA with SCTP*.

Features That Use SCTP

The following features use SCTP:

- PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer, page 162
- Support for IUA with SCTP for Cisco Access Servers, page 164

PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer

This feature (sometimes called PRI Q.921 Signaling Backhaul) provides standards-based ISDN signaling backhaul capability on Cisco IOS gateways. It fills the need for PRI Q.921 signaling backhaul that works with third-party call agents or media-gateway controllers (MGCs) where call processing for voice calls is carried out by call-control servers, and packet-network connections are made using protocols such as Media Gateway Control Protocol (MGCP) and Simple Gateway Control Protocol (SGCP). It enables solutions such as Integrated Access, IP PBX, and Telecommuter on the Cisco 3600 series, Cisco AS5300, and Cisco AS5850. It provides a configuration interface for Cisco IOS software implementation and implements protocol message flows for SCTP and IUA.

This feature provides the following:

- PRI backhaul—Specific implementation for backhauling PRI

Note For more information about PRI backhaul using SCTP, see *PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer*.

- SCTP—New general-transport protocol that can be used for backhauling signaling messages
- IDSN User Adaptation Layer (IUA)—Mechanism for backhauling any Layer 3 protocol that normally uses Q.921

This feature supports interoperability with third-party call agents. It also supports the following solutions that require signaling backhaul:

- IP PBX
- IP Centrex
- Enterprise toll bypass
- IXC/tandem bypass

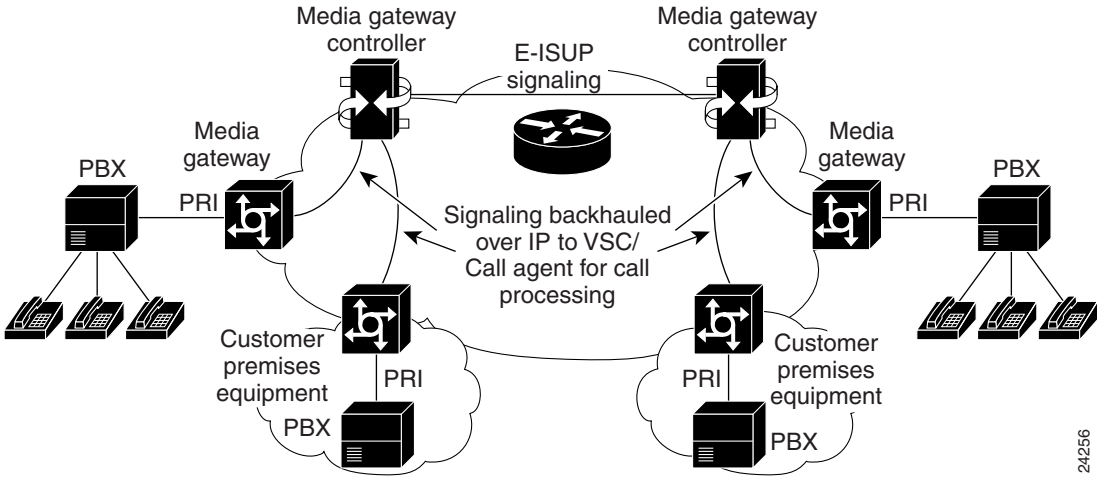
Signaling backhaul facilitates the handling of voice traffic coming from the signaling endpoints that communicate using facility-associated signaling. Facility-associated signaling requires the signaling channel (channel that carries call-signaling information) to share a digital facility with the bearer channels. ISDN PRI is one example of facility-associated signaling. ISDN signaling backhaul is required in the MGCP-based call-control architecture to enable end-to-end voice solutions.

This feature implements the IETF standards-based signaling backhaul protocols. This standards-based signaling transport support enables any third-party call agent that supports the standards to work with Cisco gateways. ISDN signaling backhaul is required in the MGCP-based call-control architecture to enable end-to-end voice solutions.

This feature migrates the proprietary PRI backhaul infrastructure to open standards. Backhaul is carried out using industry-standard SCTPs and ISDN IUA protocols as defined by the SIGTRAN working group of the IETF. It supports backhauling for ISDN-based signaling protocols only.

Figure 10 shows an example of PRI signaling backhaul. The MGC provides call processing and gateway control.

Figure 10 PRI Signaling Backhaul

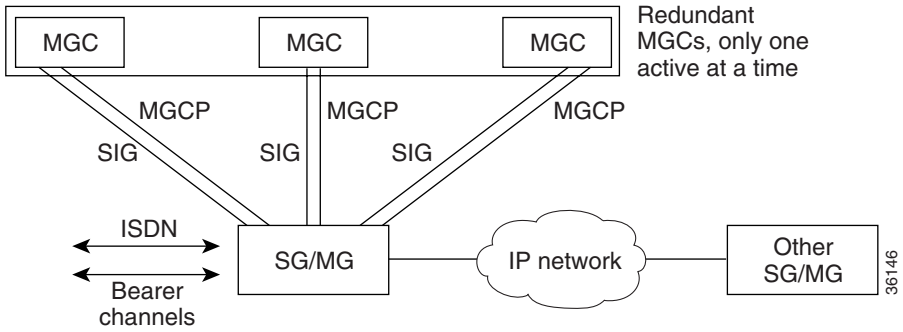


Ordinarily, signaling backhaul occurs at a common boundary for all protocols. For ISDN, signaling backhaul occurs at the Layer 2 (Q.921) and Layer 3 (Q.931) boundaries. The lower layers of the protocol (Q.921) are terminated and processed on the gateway, while the upper layers (Q.931) are backhauled to the MGC using SCTP. Signaling backhaul provides the advantage of distributed protocol processing. This permits greater expandability and scalability while offloading lower-layer protocol processing from the MGC.

Signaling transport between entities is applied to ensure that signaling information is transported with the required functionality and performance. The signaling gateway or MGC receives both ISDN signaling and bearer-channel data. ISDN signaling is backhauled up to an MGC or call agent using the SIG protocol stack. You can configure each signaling gateway to use up to three MGCs within an application server for redundancy. Multiple application servers can also be supported on a signaling gateway. MGCP is then used to control the bearer channels.

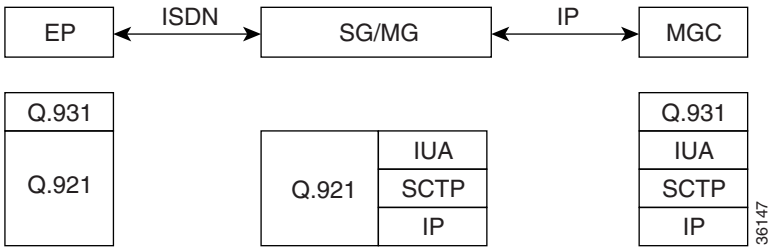
Figure 11 shows the functional model for PRI signaling transport.

Figure 11 Signaling Transport Model



SCTP is a peer-to-peer protocol; IUA is a client-server protocol. Figure 12 shows the protocol flow from an ISDN endpoint, through the signaling gateway, and then to a call agent or media gateway controller.

Figure 12 Protocol Flow



PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer on the Cisco 3660 supports the following on a Cisco 3660:

- 20 calls per hour per DS-0 bearer circuit (3-minute average call duration)
- 460 calls per hour per PRI circuit (23 bearer channels): 20 x 23 = 460
- 5520 calls per hour per Cisco 3660 (12 PRI trunks): 460 x 12 = 5520
- 1.5333 calls per Cisco 3660 per second. 5520 divided by (60*60) = 1.5333
- 7 signaling messages per call (both setup and tear down)
- 10.8 signaling messages per second per Cisco 3660: 7 x 1.5333 = 10.8

Support for IUA with SCTP for Cisco Access Servers

This feature supports IUA with SCTP for the Cisco AS5x00, Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. It is to be used as an alternative to the existing IP-based User Datagram Protocol (UDP)-to-Reliable Link Manager (RLM) transport between the Cisco PGW 2200 and Cisco gateways.

IUA with SCTP acts as the call signaling IP transport mechanism in a voice-gateway solution. These combined protocols are also used for Signaling System 7 (SS7) Interconnect solutions, which allow required flexibility in connecting Intermachine trunks from more than one PSTN switch (multiple trunk groups) to the Cisco gateways. This feature also allows you to interconnect with multiple carriers on high-capacity Cisco AS5x00 gateways for load balancing and redundancy.

IUA and SCTP protocols provide the following services:

- Trunk groups are defined on a T1/E1 interface basis.
- All DS0 bearer channels in a specific T1/E1 interface are included in the same trunk group and cannot be split into different trunk groups.
- Multiple T1/E1 interfaces on the same gateway can be provisioned in a single trunk group or split into multiple trunk groups. The maximum number of trunk groups that a platform can support is equal to the maximum number of T1/E1 interfaces that the platform can configure.

This feature supports SCTP, multiple non-facility associated signaling, and IUA.

How to Configure SCTP Features

This section contains the following procedures:

Configuring PRI Backhaul Using the SCTP and the ISDN Q.921 User Adaptation Layer

Configuration Options

The following is an example of an application-server configuration on a gateway:

```
AS as1 10.4.8.69 10.4.9.69 2577
```

Application server as1 is configured to use two local IP addresses and port 2577. IP address values that are set apply to all IP addresses of the application-server process.

An application-server process can be viewed as a local representation of an SCTP association since it specifies a remote endpoint that communicates with an application-server local endpoint. An application-server process is defined for a given application server. For example, the following configuration defines remote signaling controller asp1 at two IP addresses for application server as1. The remote SCTP port number is 2577:

```
AS as1 10.4.8.69 10.4.9.69 2477
ASP asp1 AS as1 10.4.8.68 10.4.9.68 2577
```

Multiple application-server processes can be defined for a single application server for the purpose of redundancy, but only one process can be active. The other process is inactive and becomes active at failover.

In the Cisco media-gateway-controller solution, a signaling controller is always the client that initiates association with a gateway. During initiation, you can request outbound and inbound stream numbers, but the gateway allows only a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The number of streams to assign to a given association is implementation dependent. During initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple-trunk-group support, every interface can potentially be a separate D channel.

At startup, the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the GW and the media gateway controller. For the rare case that you are configuring multiple application server associations to various media gateway controllers, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during startup the IUA code adds one to the total number of interfaces (streams) found.

You can manually configure the number of streams per association. In the backhaul scenario, if the number of D-channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that will never be used. For multiple associations between a GW and multiple media gateway controllers, the configuration utility is useful in providing only the necessary number of streams per association. Overhead from the streams allocated but not used in the association is negligible.

If you manually configure the number of streams through the CLI, the IUA code cannot distinguish between a startup event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you configure the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword. Otherwise, IUA needs always to add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with the command-line interface, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA application server configuration and then configure it back as the same application server or a new one. The other option is to reload the router.

To configure the PRI Backhaul Using SCTP and the ISDN Q.921 User Adaptation Layer feature, perform the following tasks:

- Configure IUA, page 166
- Configure ISDN Signaling (PRI) Backhaul, page 168
- Verify PRI Backhaul, page 170

Caution When the Fast Ethernet interface is configured for auto negotiation, it can take up to two seconds to initialize. Two examples of the interface initializing is when the **no shutdown** command is entered, or if the cable is removed and then plugged back in. To avoid any problems, the Fast Ethernet interface should not be configured for auto negotiation. The duplex and speed parameters should be set according to the requirements of the network, and should not be set to auto.

Configure IUA

To configure IUA, perform the following steps.

Note The steps below direct you to configure an application server and the ASP first to allow an NI2+ to be bound to the IUA transport layer protocol. The application server is a logical representation of the SCTP local endpoint. The local endpoint can have more than one IP address but must use the same port number.

Prerequisites

- Ensure that Cisco IOS Release 12.2(15)T or later is installed and running on your system.
- Configure ISDN to backhaul Q.921 signaling to the third-party call agent (MGC).
- Ensure that your Cisco AS5850 has the following:
  - MGCP 1.0
  - IUA 0.4
  - ISDN network side support to terminate multiple voice PRIs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **iua**
4. **as**
5. **asp as**
6. **asp sctp-keepalives**
7. **asp ip-precedence**
8. **as fail-over-timer**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**iua** **Example:** `Router(config)# iua`	Enters IUA configuration mode and specifies backhaul using SCTP.
Step 4	**as** *as-name* {*local-ip1* [*local-ip2*]} [**local-sctp-port**] **Example:** `Router(config-iua)# as as5400-3 10.1.2.34 10.1.2.35 2577`	Defines an application server on a gateway. You can specify up to three local IP addresses (note that SCTP has built-in support for multihomed machines).
Step 5	**asp** *asp-name* **as** *as-name* {*remote-ip1* [*remote-ip2*]}[**remote-sctp-port**] **Example:** `Router(config-iua)# asp asp1 as as5400-3 10.4.8.68 10.4.9.68 2577`	Defines an ASP. Use this command to establish SCTP associations. **Note** A maximum of three ASPs can be configured per application server.
Step 6	**asp** *asp-name* **sctp-keepalives** *remote-ip keepalive-value* **Example:** `Router(config-iua)# asp asp1 sctp-keepalives 10.1.2.234 600`	(Optional) Sets SCTP keepalive behavior, in ms, for the specified ASP and IP address. Range: 1000 to 60000. Default: 500. **Note** Find the current value by examining the **show ip sctp association parameters** command output under heartbeats.

	Command or Action	Purpose
Step 7	**asp** *asp-name* **ip-precedence** *remote-ip ip-precedence-level* **Example:** `Router(config-iua)# asp asp1 ip-precedence 10.1.2.345 7`	(Optional) Sets the IP precedence level for protocol data units (PDUs) for the specified IP address. Range for a given address is 0 to 7. Default for normal IP precedence handling is 0.
Step 8	**as** *as-name* **fail-over-timer** *time* **Example:** `Router(config-iua)# as as5400-3 fail-over-timer 10000`	(Optional) Sets the failover timer value, in ms. IUA waits for this amount of time for one ASP to take over from another ASP during failover. **Note** Find the current failover timer value by examining the **show iua as all** command output.
Step 9	**exit** **Example:** `Router(config-iua)# exit`	Exits the current mode.

Configure ISDN Signaling (PRI) Backhaul

To configure ISDN signaling (PRI) backhaul, perform the following steps.

Prerequisites

- Ensure that Cisco IOS Release 12.2(4)T or later is installed and running on your system.

SUMMARY STEPS

1. **enable**
2. **configuration terminal**
3. **controller**
4. **pri-group timeslots service**
5. **exit**
6. **interface serial**
7. **isdn switch-type**
8. **isdn bind-l3 IUA-backhaul as**
9. Repeat as needed.
10. **exit**

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t1 0** **Example:** `Router(config)# controller t1 0`	Enters controller configuration mode for slot 0.
Step 4	**pri-group timeslots 1-24 service mgcp** **Example:** `Router(config-control)# pri-group timeslots 1-24 service mgcp`	Sets the control protocol used for backhaul to MGCP. You cannot share controller timeslots between backhaul and other Layer 3 protocols.
Step 5	**exit** **Example:** `Router(config-control)# exit`	Exits the current mode.
Step 6	**interface serial 0:23** **Example:** `Router(config)# interface serial 0:23`	Enters serial-interface configuration mode for the specified controller and timeslot. The D-channel timeslot is (channelized T1): 23 or (channelized E1):15.
Step 7	**isdn switch-type** *switch-type* **Example:** `Router(config-if)# isdn switch-type primary-4ess`	Specifies the ISDN switch type (can be done in either global configuration mode or interface mode).
Step 8	**isdn bind-l3 IUA-backhaul as** *as-name* **Example:** `Router(config-if)# isdn bind-l3 IUA-backhaul as server1`	Configures ISDN to backhaul Q.931 to the media gateway controller.
Step 9	Repeat the preceding steps for each T1 interface that uses backhaul.	—
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verify PRI Backhaul

To verify PRI backhaul, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show iua as**
2. **show iua asp**
3. **show isdn status**
4. **show running-config**

DETAILED STEPS

Step 1 **show iua as** {**all** | **name** *as-name*}

Use this command to display the current state of the active application server and show the PRI interfaces configured on the application server.

The following output shows that the current state of the application server (as1) is active and that there are four PRI interfaces configured to use this application server:

```
Router# show iua as all

Name of AS :as1
        Total num of ASPs configured :2
        Current state :  ACTIVE
        Active ASP :asp1
        Number of ASPs up :1
        Fail-Over time : 4000 milli seconds
        Local address list : 10.21.0.2
        Local port  9900
        Interface IDs registered with this AS
                 Interface ID            stream #
                 256 (serial1/0:23)      1
                 257 (serial1/1:23)      2
                 512 (serial2/0:23)      3
                 513 (serial2/1:23)      4
```

Step 2 **show iua asp** {**all** | **name** *asp-name*}

Use this command to display the current state of the active ASP and show information about the SCTP association being used by this ASP.

The following output shows that the current state of the ASP (asp1) is active. It also shows information about the SCTP association being used by this ASP.

```
Router# show iua asp all

Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc  id
0
SCTP Association information :
         Local Receive window :9000
         Remote Receive window :9000
         Primary Dest address requested by IUA 10.23.0.16
         Effective Primary Dest address 10.23.0.16
Remote  address list : 10.23.0.16
Remote Port :9900
Statistics :
```

```
        Invalid SCTP signals Total :0  Since last  0
        SCTP Send failures :0

Name of ASP :asp2
Current State of ASP:ASP-Down
Current state of underlying SCTP Association IUA_ASSOC_INIT , assoc  id
0
Remote  address list : 10.23.0.16
Remote Port :9911
Statistics :
        Invalid SCTP signals Total :0  Since last  0
        SCTP Send failures :0
```

Step 3 show isdn status

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Use it also to display the status of ISDN backhaul. If connection to the media gateway controller is lost, the router shuts down Layer 2 so that it cannot receive calls. When the connection is back up, you can use this command to verify that Layer 2 was also brought back up correctly.

The following sample output shows Layer 2 status, as defined by the MULTIPLE_FRAME_ESTABLISHED message, to be up. The L3 protocol and state status are highlighted:

```
Router# show isdn status

Global ISDN Switchtype = primary-5ess
ISDN Serial1/0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
        L2 Protocol = Q.921  L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask: 0x807FFFFF
ISDN Serial1/1:23 interface
        dsl 1, interface ISDN Switchtype = primary-5ess
        L2 Protocol = Q.921  L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 1 CCBs = 0
    The Free Channel Mask: 0x807FFFFF
ISDN Serial2/0:23 interface
        dsl 2, interface ISDN Switchtype = primary-5ess
        L2 Protocol = Q.921  L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask: 0x807FFFFF
ISDN Serial2/1:23 interface
        dsl 3, interface ISDN Switchtype = primary-5ess
```

```
L2 Protocol = Q.921  L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 3 CCBs = 0
    The Free Channel Mask: 0x807FFFFF
    Total Allocated ISDN CCBs = 0
```

Step 4 **show running-config**

Use this command to display basic router configuration.

Note For troubleshooting tips, see the "Troubleshooting Tips" section on page 183.

Configuring Support for IUA with SCTP for Cisco Access Servers Feature

This section contains the following procedures:

Configure IUA for Cisco Access Servers

To configure IUA for Cisco access servers, follow the steps for configuring IUA for PRI Q.921 backhaul, as described in the "Configure IUA" section on page 166.

Configure the SCTP T1 Initiation Timer

To configure the SCTP T1 initiation timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **iua**
4. **as**
5. **as fail-over-timer**
6. **as sctp-startup-rtx**

7. **as sctp-streams**
8. **as sctp-t1init**
9. **asp as**
10. **asp ip-precedence**
11. **asp as**
12. **asp sctp-keepalive**
13. **asp sctp-max-association**
14. **asp sctp-path-retransmission**
15. **asp sctp-t3-timeout**
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**iua** **Example:** `Router(config)# iua`	Enters IUA configuration mode and specifies backhaul using SCTP.
Step 4	**as** *as-name* {*localip1* [*localip2*]} [**local-sctp-port**] **Example:** `Router(config-iua)# as as5400-3 10.1.2.34 10.1.2.35 2577`	Defines an application server on a gateway.
Step 5	**as** *as-name* **fail-over-timer** *time* **Example:** `Router(config-iua)# as as5400-3 fail-over 10000`	(Optional) Sets the failover timer value, in ms. **Note** Find the failover timer value by examining the **show iua as all** command output.
Step 6	**as** *as-name* **sctp-startup-rtx** *number* **Example:** `Router(config-iua)# as as5400-3 sctp-startup-rtx 8`	Configures the SCTP startup retransmission interval.

	Command or Action	Purpose
Step 7	**as** *as-name* **sctp-streams** *number* **Example:** `Router(config-iua)# as as5400-3 sctp-streams 56`	Configures the number of SCTP streams for this application server. Although the gateway help function displays a range of 2 to 57, the upper end of the range (also the default) is determined by your hardware, and is equal to the number of controllers on that gateway and NAS one plus. If you enter a number higher than that, the system assumes the default. **Note** If you want to set this value to something other than the default, add one to the number of D channel interfaces that you want to use concurrently.
Step 8	**as** *as-name* **sctp-t1init** *number* **Example:** `Router(config-iua)# as as1 sctp-t1init 1000`	Sets the SCTP T1 initiation timer, in ms.
Step 9	**asp** *asp-name* **as** *as-name ip-address* **Example:** `Router(config-iua)# asp asp1 as as1 10.4.8.68 10.4.9.68`	Creates an ASP and specifies to which application server it belongs.
Step 10	**asp** *asp-name* **ip-precedence** *remote-ip-address number* **Example:** `Router(config-iua)# asp asp1 ip-precedence 10.1.2.345 7`	Specifies the IP precedence level for protocol data units (PDUs) for a given IP address. Default for normal IP precedence handling is 0.
Step 11	**asp** *asp-name* **as** *as-name* {*remote-ip* [*remote-ip2*]}[**remote-sctp-port**] **Example:** `Router(config-iua)# asp asp1 as as5400-3 10.4.8.68 10.4.9.68 2577`	Defines an ASP. Use this command to establish SCTP associations.
Step 12	**asp** *asp-name* **sctp-keepalive** *remote-ip-address number* **Example:** `Router(config-iua)# asp asp1 sctp-keepalive 10.1.2.234 1000`	(Optional) Specifies the IP address to enable and disable keepalives and control SCTP keepalives on destination IP addresses.
Step 13	**asp** *asp-name* **sctp-max-association** *ip-address number* **Example:** `Router(config-iua)# asp asp1 sctp-max-association 10.10.10.10 20`	Sets the maximum association retransmissions for this ASP.

	Command or Action	Purpose
Step 14	**asp** *asp-name* **sctp-path-retransmission** *ip-address number* **Example:** `Router(config-iua)# asp asp1 sctp-path-retransmission 10.10.10.10 2`	Sets the SCTP path retransmissions for this ASP.
Step 15	**asp** *asp-name* **sctp-t3-timeout** *ip-address number* **Example:** `Router(config-iua)# asp asp1 sctp-t3-timeout 10.10.10.10 60000`	Enters IUA-SCTP configuration mode and sets the SCTP T3 retransmission timeout for this ASP.
Step 16	**exit** **Example:** `Router(config-iua-sctp)# exit`	Exits the current mode.

Create NFAS Groups and Bind Them to the Application Server

To create NFAS groups and bind them to the application server, perform the following steps.

Note

- This procedure configures two T1 interfaces into two NFAS groups or trunk groups that are served by the same application server with two different SCTP streams (ASPs). It allows you to configure the NFAS primary D channel and bind the channel to an IUA application server.
- The steps for configuring the T1/E1 interface are the same as the steps using RLM, but multiple NFAS groups can now be defined to support multiple trunk groups. All interfaces in an NFAS are treated as one trunk group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t1 1/0/0**
4. **pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group iua**
5. **exit**
6. **controller t1 1/0/1**
7. **pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group iua**
8. **exit**

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t1 1/0/0** **Example:** `Router(config)# controller t1 1/0/0`	Enters controller configuration mode on the first T1 controller.
Step 4	**pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group** *number* **iua** *as-name* **Example:** `Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1 iua as-1`	Configures the NFAS primary D channel on one channelized T1 controller and binds the D channel to an IUA application server. You can choose any timeslot other than 24 to be the virtual container for the D channel parameters for ISDN. Keywords and arguments are as follows: • **nfas-group** *number*—NFAS group • **iua** *as-name*—Must match the name of an application server that was set up during IUA configuration. **Note** For more information, see the "Configure IUA" section on page 166.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode on the first controller.
Step 6	**controller t1 1/0/1** **Example:** `Router# controller t1 1/0/1`	Enters controller configuration mode on the second T1 controller.
Step 7	**pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group** *number* **iua** *as-name* **Example:** `Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1 iua as-1`	Configures the NFAS primary D channel on another channelized T1 controller and binds the D channel to an IUA application server. Keywords and arguments are as above. The argument *as-name* must match the name of an application server that was set up during IUA configuration.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Migrate from RLM to IUA with SCTP

To migrate from RLM to IUA with SCTP, perform the following steps.

Note The following changes have been made between RLM and IUA with SCTP:

- Application server and ASP configuration lines must precede the controller configuration lines in the configuration text file.
- RLM group configuration must be removed from the D channel configuration.
- For the D channel, the **interface serial** commands are now replaced by **interface D channel** commands.
- Any **isdn bind** commands must be removed from the D channel. Binding of the NFAS groups now takes place when you use the **pri-group** commands for IUA with SCTP.

For more information, see the "SCTP Migration from RLM to IUA: Example" section on page 209.

SUMMARY STEPS

1. **enable**
2. **copy run tftp**
3. Remove the "isdn rlm-group 1" line
4. **copy tftp start**
5. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**copy run tftp** **Example:** `Router# copy run tftp`	Copies the running configuration to a TFTP server. Make a backup copy of the running configuration. Enter the IP address and destination filename when prompted. **Note** Make all edits to the configuration text file that you have copied over to your TFTP server. Some TFTP servers might require that the name of the file that you intend to copy over is already existing and has write permissions on the TFTP server onto which you are copying.

	Command or Action	Purpose

Step 3	For RLM, remove the "isdn rlm-group 1" line shown in bold.
	
	Example:
	`interface Serial3/0:1:23`
	` no ip address`
	` isdn switch-type primary-ni`
	` isdn incoming-voice modem`
	` isdn T321 30000`
	` isdn T303 20000`
	` isdn T200 2000`
	` **isdn rlm-group 1**`
	` isdn negotiate-bchan resend-setup`
	` isdn bchan-number-order ascending`
	` no cdp enable`
		Links IUA instead of RLM by removing the "isdn rlm-group 1" line from the interface serial output.

Step 4	**`copy tftp start`** **Example:** `Router# copy tftp start`	Copies the new configuration to the startup configuration.
Step 5	**`reload`** **Example:** `Router# reload`	Reloads the router.

Modify a PRI Group on an MGC

To modify a PRI group on an MGC, perform the following steps.

Prerequisites

- Remove **isdn bind** commands from the D channel. Binding of the NFAS groups takes place when you use the **pri-group** commands for IUA with SCTP.

Note For more information, see the "Trunk Group Bound to an Application Server: Example" section on page 210.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface Dchannel3/0:1**
4. **shutdown**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface Dchannel3/0:1** **Example:** `Router(config)# interface Dchannel3/0:1`	Enters interface configuration mode for the specified D channel that is to be shut down. This is the format used for IUA.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the D channel.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verify Support for IUA with SCTP

To verify support for IUA with SCTP, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show ip sctp association list**
2. **show ip sctp association parameters**
3. **show ip sctp association statistics**
4. **show ip sctp errors**
5. **show ip sctp instances**
6. **show ip sctp statistics**
7. **show isdn service**
8. **show isdn status**
9. **show running-config**

DETAILED STEPS

Step 1 **show ip sctp association list**

Use this command to display current SCTP association and instance identifiers, current state of SCTP associations, and local and remote port numbers and addresses that are used in the associations.

The example below shows two current associations that are in the established state. Each association belongs to a different instance, as noted by their instance identifiers.

```
Router# show ip sctp association list

*** SCTP Association List ****

AssocID: 0,  Instance ID: 0
Current state: ESTABLISHED
Local port: 8787, Addrs: 10.1.0.2 10.2.0.2
Remote port: 8787, Addrs: 10.5.0.4 10.6.0.4

AssocID: 1,  Instance ID: 1
Current state: ESTABLISHED
Local port: 6790, Addrs: 10.1.0.2 10.2.0.2
Remote port: 6789, Addrs: 10.5.0.4 10.6.0.4
```

Step 2 show ip sctp association parameters

Use this command to display parameter values for the specified association. This command requires an association identifier as an argument. Association identifiers can be obtained from the output of the **show ip sctp association list** command.

Many parameters are defined for each association, some of them configured and some of them calculated. They fall into the following main groupings:

- Association configuration parameters
- Destination address parameters
- Association boundary parameters
- Current association congestion parameters

```
Router# show ip sctp association parameters 0

** SCTP Association Parameters **

AssocID: 0  Context: 0  InstanceID: 0
Assoc state: ESTABLISHED  Uptime: 00:00:34.280
Local port: 8787
Local addresses: 10.1.0.2 10.2.0.2

Remote port: 8787
Primary dest addr: 10.5.0.4
Effective primary dest addr: 10.5.0.4
Destination addresses:

10.5.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/0/0 ms   TOS: 0  MTU: 1500
  cwnd: 5000  ssthresh: 18000  outstand: 0
  Num retrans: 0  Max retrans: 5  Num times failed: 0

10.6.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/0/0 ms   TOS: 0  MTU: 1500
  cwnd: 3000  ssthresh: 18000  outstand: 0
  Num retrans: 0  Max retrans: 5  Num times failed: 0

Local vertag: DA3C3BD  Remote vertag: 4D95E3A
Num inbound streams: 13  outbound streams: 13
```

```
Max assoc retrans: 5  Max init retrans: 8
CumSack timeout: 200 ms  Bundle timeout: 100 ms
Min RTO: 1000 ms  Max RTO: 60000 ms
LocalRwnd: 9000  Low: 6400   RemoteRwnd: 16800  Low: 14900
Congest levels: 0  current level: 0  high mark: 1
```

Step 3 show ip sctp association statistics

Use this command to display statistics about the specified association, including the following: The first numbers show the total number of chunks, both data and control, sent and received. The second group of statistics focuses on the data chunks sent, showing the total number sent, the number retransmitted, the number that were ordered and unordered, the average number that were bundled together, and the total bytes sent. The third group of statistics focuses on the data chunks received. It displays the total number received and the number discarded (because of duplicates), the number of ordered and unordered chunks received, the average number of chunks that were bundled, the number of bytes received, and the number of sequenced chunks that were received out of order. The last section indicates how many datagrams have been sent, received, or are ready to be received by the calling application or ULP. The ULP statistics may be different from the chunk statistics if the datagrams are large and have been segmented by SCTP.

Note This command requires an association identifier argument, which you can obtain from output of the **show ip sctp association list** command.

The following example was taken from a network with known dropped packets in one direction. The number of total chunks sent and received is larger than the number of data chunks sent and received because it also includes the control chunks sent. The number of chunks received out of sequence indicates that there are some chunks not being received in the correct order. However, the number of chunks discarded is zero, indicating that only one copy of each is arriving at this peer (some chunks are probably being dropped and the peer is retransmitting them, but there are no duplicates being received). The number of chunks being retransmitted is zero, indicating that there is no network problem in the direction of sending from this peer to the remote.

```
Router# show ip sctp association statistics 0

** SCTP Association Statistics **

AssocID/InstanceID: 0/0
Current State: ESTABLISHED
Control Chunks
  Sent: 1009  Rcvd: 988
Data Chunks Sent
  Total: 18073  Retransmitted: 0
  Ordered: 9095  Unordered: 8978
  Avg bundled: 9  Total Bytes: 1807300
Data Chunks Rcvd
  Total: 18073  Discarded: 0
  Ordered: 9095  Unordered: 8978
  Avg bundled: 9  Total Bytes: 1807300
  Out of Seq TSN: 586
ULP Dgrams
  Sent: 18073  Ready: 18073  Rcvd: 18073
```

Step 4 show ip sctp errors

Use this command to display errors logged since last time that the statistics were cleared.

The following output shows one example in which no errors have been logged, and another in which there have been several different types of errors.

```
Router# show ip sctp errors

*** SCTP Error Statistics ****

No SCTP errors logged.

Router# show ip sctp errors

*** SCTP Error Statistics ****

Communication Lost:              95
Unknown INIT params rcvd:        8
Missing parameters:              18
No room for incoming data:       11
```

Step 5 **show ip sctp instances**

Use this command to display information for each of the currently configured instances. The instance number, local port, and address information is displayed. The instance state is either *available* or *deletion pending*. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers are used for establishing incoming associations, and the maximum number of associations allowed for this instance is shown. Finally, a snapshot of each existing association is shown, if any exist.

In this example, two current instances are active and available. The first is using local port 8787, and the second is using local port 6790. Instance identifier 0 has one current association, and instance identifier 1 has no current associations.

```
Router# show ip sctp instances

*** SCTP Instances ****

Instance ID: 0  Local port: 8787
Instance state: available
Local addrs: 10.1.0.2 10.2.0.2
Default streams inbound: 1  outbound: 1
  Current associations:  (max allowed: 6)
  AssocID: 0  State: ESTABLISHED  Remote port: 8787
    Dest addrs: 10.5.0.4 10.6.0.4

Instance ID: 1  Local port: 6790
Instance state: available
Local addrs: 10.1.0.2 10.2.0.2
Default streams inbound: 13  outbound: 13

No current associations established for this instance.
Max allowed: 6
```

Step 6 **show ip sctp statistics**

Use this command to display the overall SCTP statistics accumulated since the last **clear ip sctp statistics** command for currently established associations and those that have terminated. The command also displays the number of aborts and shutdowns received and the number of times the T1 (initialization) and T2 (shutdown) timers expired.

```
Router# show ip sctp statistics

** SCTP Overall Statistics **
```

```
Control Chunks
  Sent: 7872  Rcvd: 8547
Data Chunks Sent
  Total: 98681  Retransmitted: 5
  Ordered: 50241  Unordered: 48435
  Total Bytes: 9868100
Data Chunks Rcvd
  Total: 98676  Discarded: 0
  Ordered: 50241  Unordered: 48435
  Total Bytes: 9867600
  Out of Seq TSN: 2845
SCTP Dgrams
  Sent: 17504  Rcvd: 19741
ULP Dgrams
  Sent: 98676  Ready: 98676  Rcvd: 98676

Additional Stats
  Assocs Currently Estab: 0
  Active Estab: 0  Passive Estab: 2
  Aborts: 0  Shutdowns: 0
  T1 Expired: 11  T2 Expired: 0
```

Step 7 **show isdn service**

Use this command to display information about ISDN channels and the service states.

Step 8 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 9 **show running-config**

Use this command to display the basic router configuration.

Troubleshooting Tips

In a live system, debug commands for performance, state, signal, and warnings are most useful. These commands show any association or destination address failures and can be used to monitor the stability of any established associations.

Caution Use debug commands with extreme caution or not at all in live systems, depending on the amount of traffic. Debug commands other than those for performance, state, signal, and warnings can generate a great deal of output and therefore cause associations to fail. Use these commands only in test environments or during times of very low traffic volume.

Note

- SCTP debug commands display information for all current SCTP associations and cannot be limited to particular associations.
- SCTP debug commands that display statistical information show only the information that is available since the last time a **clear ip sctp statistics** command was executed. The **clear ip sctp statistics** command clears all SCTP statistics, both those compiled for individual associations and those compiled overall.
- Sample outputs for the debug commands are shown in the "Examples" section on page 185.

- You can use debugs with timestamps enabled to see the relevant timing of the events indicated. To add timestamps to debug output, use the **service timestamps** commands (**service timestamps debug** and **service timestamps log**), optionally with the **msec** keyword. Output is in the format MMM DD HH:MM:SS, which indicates the date and time according to the system clock. If the system clock is not set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.
- For more information on SCTP debug commands, see *Stream Control Transmission Protocol (SCTP)*.

- Use the **debug ip sctp api** command to show all SCTP calls to the application programming interface (API) that are being executed and the parameters associated with these calls.
- Use the **debug ip sctp congestion** command to display various events related to calculating the current congestion parameters, including congestion window (cwnd) values per destination address and local and remote receiver window (rwnd) parameters. Information is displayed when bundling and sending data chunks, indicating the current cwnd and rwnd values and remote rwnd values, thus showing when data can or can not be sent or bundled. When chunks are acknowledged by the remote peer, the number of bytes outstanding and remote rwnd values are updated. Information is also displayed when new chunks are received, thus decreasing the local rwnd space, and when chunks are freed because the ULP is receiving datagrams from SCTP and thus freeing local rwnd space.
- Use the **debug ip sctp init** command to display datagrams and other information related to the initializing of new associations. All initialization chunks are shown, including the INIT, INIT_ACK, COOKIE_ECHO, and COOKIE_ACK chunks. You can use this command to see the chunks associated with any initialization sequence, but it does not display data chunks sent once the association is established. Therefore, it is safe to use in a live system that has traffic flowing when you have trouble with associations that fail and have to be reestablished.
- Use the **debug ip sctp multihome** command to display the source and destination of datagrams in order to monitor use of the multihome addresses. More than one IP address parameter can be included in an INIT chunk when the INIT sender is multihomed. Datagrams should mostly be sent to the primary destination addresses unless the network is experiencing problems, in which case they can be sent to the secondary addresses.
- Use the **debug ip sctp performance** command to display the average number of chunks and datagrams being sent and received per second once every 10 seconds. Averages are cumulative since the last time the statistics were cleared and so may not accurately reflect the number of datagrams and chunks currently being sent and received.
- Use the **debug ip sctp rcvchunks** command to display information about chunks that are received, including the following: stream number, sequence number, chunk length, and chunk transmission sequence number (TSN) for each chunk received; and whether the chunk is for a new datagram or a datagram that is already being reassembled. Command output shows whether the datagram is complete after receiving this chunk or not and, if complete, whether it is in sequence within the specified stream and can be delivered to the ULP. It shows the SACKs that are sent back to the remote, indicating the cumulative TSN acknowledged, the number of fragments included, and that the datagram is received by the ULP.
- Use the **debug ip sctp rto** command to display adjustments to the retransmission (retrans) timeout value due to retransmission of data chunks or unacknowledged heartbeats.
- Use the **debug ip sctp segments** command to display every datagram that is sent or received and the chunks that are contained in each. The command has two forms: simple and verbose. This simple form of the command shows basic information for each chunk type.

- Use the **debug ip sctp segmentv** command to show every datagram that is sent or received and the chunks that are contained in each. The command has two forms: simple and verbose. This verbose form of the output shows detailed information for each chunk type.
- Use the **debug ip sctp signal** command to display signals that are sent from SCTP to the application or ULP. These signals inform the ULP of state transitions for associations or destination addresses. Signal s sent to the ULP when new data is available to be received may not be shown because they occur infrequently. You can use this command to determine whether or not the current associations are stable. Because it does not generate output except on state transitions, it is safe to use in a live environment. It still should be used with caution, however, depending on the number of associations being handled by the system and the stability of the network.

Note The **debug ip sctp state** and **debug ip sctp signal** commands are often used together to provide insight into the stability of associations.

- Use the **debug ip sctp sndchunks** command to display the following types of information about all chunks that are being sent to remote SCTP peers:
  - Application send requests from the local SCTP peer
  - Chunks being bundled and sent to the remote peer
  - Processing of the SACKs from the remote peer, indicating which chunks were successfully received
  - Chunks that are marked for retransmission
- Use the **debug ip sctp state** command with the **debug ip sctp signal** command to provide insight into the stability of associations.
- Use the **debug ip sctp timer** command to display information about all started, stopped, and triggering SCTP timers. Many SCTP timers, after they are started, are not restarted until they expire or are stopped; the first call starts the timer, and subsequent calls do nothing until the timer either expires or is stopped.
- Use the **debug ip sctp warnings** command to display information on any unusual situation that is encountered. These situations may or may not indicate problems, depending on the particulars of the situation.
- Use the **debug iua as** command to display debug messages for the IUA application server when an ISDN backhaul connection is initially established.
- Use the **debug iua asp** command to display debug messages for the IUA ASP when an ISDN backhaul connection is initially established.

Examples

This section contains the following output examples (commands are listed alphabetically):

Sample Output for the debug ip sctp api Command

Caution Do not use this command in a live system that has any significant amount of traffic running. It can generate significant traffic, and cause associations to fail.

```
Router# debug ip sctp api

*Mar  1 00:31:14.211: SCTP: sctp_send: Assoc ID: 1
*Mar  1 00:31:14.211: SCTP:            stream num: 10
*Mar  1 00:31:14.211: SCTP:            bptr: 62EE332C, dptr: 4F7B598
*Mar  1 00:31:14.211: SCTP:            datalen: 100
*Mar  1 00:31:14.211: SCTP:            context: 1
*Mar  1 00:31:14.211: SCTP:            lifetime: 0
*Mar  1 00:31:14.211: SCTP:            unorder flag: FALSE
*Mar  1 00:31:14.211: SCTP:            bundle flag: TRUE
*Mar  1 00:31:14.211: SCTP: sctp_send successful return
*Mar  1 00:31:14.211: SCTP: sctp_receive: Assoc ID: 1
*Mar  1 00:31:14.215: SCTP:               max data len: 100
*Mar  1 00:31:14.215: SCTP: sctp_receive successful return
*Mar  1 00:31:14.215: SCTP: Process Send Request
*Mar  1 00:31:14.951: SCTP: sctp_receive: Assoc ID: 0
*Mar  1 00:31:14.951: SCTP:               max data len: 100
*Mar  1 00:31:14.951: SCTP: sctp_receive successful return
*Mar  1 00:31:14.951: SCTP: sctp_send: Assoc ID: 0
*Mar  1 00:31:14.951: SCTP:            stream num: 12
*Mar  1 00:31:14.951: SCTP:            bptr: 62EE00CC, dptr: 4F65158
*Mar  1 00:31:14.951: SCTP:            datalen: 100
*Mar  1 00:31:14.951: SCTP:            context: 0
*Mar  1 00:31:14.951: SCTP:            lifetime: 0
*Mar  1 00:31:14.951: SCTP:            unorder flag: FALSE
*Mar  1 00:31:14.951: SCTP:            bundle flag: TRUE
*Mar  1 00:31:14.951: SCTP: sctp_send successful return
*Mar  1 00:31:14.951: SCTP: sctp_receive: Assoc ID: 0
*Mar  1 00:31:14.951: SCTP:               max data len: 100
*Mar  1 00:31:14.951: SCTP: sctp_receive successful return
```

Sample Output for the debug ip sctp congestion Command

```
Router# debug ip sctp congestion

SCTP: Assoc 0: Slow start 10.6.0.4, cwnd 3000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 8200
SCTP: Assoc 0: Add Sack, local a_rwnd 8200
SCTP: Assoc 0: Free chunks, local rwnd 9000
```

```
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 7000
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 14000, cwnd 19500, outstand 0
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 12800, outstand 1200
SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 12800, cwnd 19500, outstand 1200
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 11600, outstand 2400
SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 11600, cwnd 19500, outstand 2400
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 10400, outstand 3600
SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 10400, cwnd 19500, outstand 3600
SCTP: Assoc 0: Bundled 4 chunks, remote rwnd 10000, outstand 4000
SCTP: Assoc 0: No additional chunks waiting.
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 7000
SCTP: Assoc 0: Chunk A22F3B45 ack'd, dest 10.5.0.4, outstanding 3900
SCTP: Assoc 0: Chunk A22F3B46 ack'd, dest 10.5.0.4, outstanding 3800
SCTP: Assoc 0: Chunk A22F3B47 ack'd, dest 10.5.0.4, outstanding 3700
SCTP: Assoc 0: Chunk A22F3B48 ack'd, dest 10.5.0.4, outstanding 3600
SCTP: Assoc 0: Chunk A22F3B49 ack'd, dest 10.5.0.4, outstanding 3500
SCTP: Assoc 0: Chunk A22F3B4A ack'd, dest 10.5.0.4, outstanding 3400
SCTP: Assoc 0: Chunk A22F3B4B ack'd, dest 10.5.0.4, outstanding 3300
SCTP: Assoc 0: Chunk A22F3B4C ack'd, dest 10.5.0.4, outstanding 3200
SCTP: Assoc 0: Chunk A22F3B4D ack'd, dest 10.5.0.4, outstanding 3100
SCTP: Assoc 0: Chunk A22F3B4E ack'd, dest 10.5.0.4, outstanding 3000
SCTP: Assoc 0: Chunk A22F3B4F ack'd, dest 10.5.0.4, outstanding 2900
SCTP: Assoc 0: Chunk A22F3B50 ack'd, dest 10.5.0.4, outstanding 2800
SCTP: Assoc 0: Chunk A22F3B51 ack'd, dest 10.5.0.4, outstanding 2700
SCTP: Assoc 0: Chunk A22F3B52 ack'd, dest 10.5.0.4, outstanding 2600
SCTP: Assoc 0: Chunk A22F3B53 ack'd, dest 10.5.0.4, outstanding 2500
SCTP: Assoc 0: Chunk A22F3B54 ack'd, dest 10.5.0.4, outstanding 2400
SCTP: Assoc 0: Chunk A22F3B55 ack'd, dest 10.5.0.4, outstanding 2300
SCTP: Assoc 0: Chunk A22F3B56 ack'd, dest 10.5.0.4, outstanding 2200
```

Sample Output for the debug ip sctp init Command

```
Router# debug ip sctp init

*Mar  1 00:53:07.279: SCTP Test: Attempting to open assoc to remote port 8787...assoc ID is 0
*Mar  1 00:53:07.279: SCTP: Process Assoc Request
*Mar  1 00:53:07.279: SCTP: Assoc 0: dest addr list:
*Mar  1 00:53:07.279: SCTP:                 addr 10.5.0.4
*Mar  1 00:53:07.279: SCTP:                 addr 10.6.0.4
*Mar  1 00:53:07.279:
...
*Mar  1 00:53:13.279: SCTP: Assoc 0: Send Init
*Mar  1 00:53:13.279: SCTP:        INIT_CHUNK, len 42
*Mar  1 00:53:13.279: SCTP:        Initiate Tag: B4A10C4D, Initial TSN: B4A10C4D, rwnd 9000
*Mar  1 00:53:13.279: SCTP:        Streams Inbound: 13, Outbound: 13
*Mar  1 00:53:13.279: SCTP:        IP Addr: 10.1.0.2
*Mar  1 00:53:13.279: SCTP:        IP Addr: 10.2.0.2
*Mar  1 00:53:13.279: SCTP:        Supported addr types: 5
*Mar  1 00:53:13.307: SCTP: Process Init
*Mar  1 00:53:13.307: SCTP:        INIT_CHUNK, len 42
*Mar  1 00:53:13.307: SCTP:        Initiate Tag: 3C2D8327, Initial TSN: 3C2D8327, rwnd 18000
*Mar  1 00:53:13.307: SCTP:        Streams Inbound: 13, Outbound: 13
*Mar  1 00:53:13.307: SCTP:        IP Addr: 10.5.0.4
*Mar  1 00:53:13.307: SCTP:        IP Addr: 10.6.0.4
*Mar  1 00:53:13.307: SCTP:        Supported addr types: 5
*Mar  1 00:53:13.307: SCTP: Assoc 0: Send InitAck
```

```
*Mar  1 00:53:13.307: SCTP:        INIT_ACK_CHUNK, len 124
*Mar  1 00:53:13.307: SCTP:        Initiate Tag: B4A10C4D, Initial TSN: B4A10C4D, rwnd 9000
*Mar  1 00:53:13.307: SCTP:        Streams Inbound: 13, Outbound: 13
*Mar  1 00:53:13.307: SCTP:        Responder cookie len 88
*Mar  1 00:53:13.307: SCTP:        IP Addr: 10.1.0.2
*Mar  1 00:53:13.307: SCTP:        IP Addr: 10.2.0.2
*Mar  1 00:53:13.311: SCTP: Assoc 0: Process Cookie
*Mar  1 00:53:13.311: SCTP:        COOKIE_ECHO_CHUNK, len 88
*Mar  1 00:53:13.311: SCTP: Assoc 0: dest addr list:
*Mar  1 00:53:13.311: SCTP:                addr 10.5.0.4
*Mar  1 00:53:13.311: SCTP:                addr 10.6.0.4
*Mar  1 00:53:13.311:
*Mar  1 00:53:13.311: SCTP: Instance 0 dest addr list:
*Mar  1 00:53:13.311: SCTP:                addr 10.5.0.4
*Mar  1 00:53:13.311: SCTP:                addr 10.6.0.4
*Mar  1 00:53:13.311:
*Mar  1 00:53:13.311: SCTP: Assoc 0: Send CookieAck
*Mar  1 00:53:13.311: SCTP:        COOKIE_ACK_CHUNK
```

Sample Output for the debug ip sctp multihome Command

Caution This command generates one debug line for each datagram sent or received. Use with extreme caution in a live network.

```
Router# debug ip sctp multihome

SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 476
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP: Assoc 0: Send Data to dest 10.5.0.4
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 476
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 476
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP: Assoc 0: Send Data to dest 10.5.0.4
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 476
SCTP: Rcvd s=10.6.0.4  8787, d=10.2.0.2  8787, len 44
SCTP: Sent:  Assoc 0: s=10.2.0.2  8787, d=10.6.0.4  8787, len 44
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 1404
SCTP: Rcvd s=10.5.0.4  8787, d=10.1.0.2  8787, len 476
```

Sample Output for the debug ip sctp performance Command

In the following example, when the performance debug was first enabled, it showed a very low rate of traffic. However, it was expected that these numbers were not accurate, so a **clear ip sctp** command was executed. The average numbers adjusted quickly to reflect the accurate amount of flowing traffic.

```
Router# debug ip sctp performance

SCTP Sent: SCTP Dgrams 5, Chunks 28, Data Chunks 29, ULP Dgrams 29
SCTP Rcvd: SCTP Dgrams 7, Chunks 28, Data Chunks 29, ULP Dgrams 29
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 29, Data Chunks 30, ULP Dgrams 30
SCTP Rcvd: SCTP Dgrams 7, Chunks 29, Data Chunks 30, ULP Dgrams 30
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 29, Data Chunks 31, ULP Dgrams 31
SCTP Rcvd: SCTP Dgrams 7, Chunks 30, Data Chunks 31, ULP Dgrams 31
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 30, Data Chunks 31, ULP Dgrams 31
SCTP Rcvd: SCTP Dgrams 7, Chunks 31, Data Chunks 32, ULP Dgrams 31
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 31, Data Chunks 32, ULP Dgrams 32
SCTP Rcvd: SCTP Dgrams 7, Chunks 32, Data Chunks 32, ULP Dgrams 32
Chunks Discarded: 0,  Retransmitted 0

Router# clear ip sctp statistics

SCTP Sent: SCTP Dgrams 30, Chunks 210, Data Chunks 199, ULP Dgrams 201
SCTP Rcvd: SCTP Dgrams 30, Chunks 208, Data Chunks 198, ULP Dgrams 198
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 30, Chunks 210, Data Chunks 199, ULP Dgrams 200
SCTP Rcvd: SCTP Dgrams 30, Chunks 209, Data Chunks 199, ULP Dgrams 199
Chunks Discarded: 0,  Retransmitted 0

SCTP Sent: SCTP Dgrams 30, Chunks 211, Data Chunks 200, ULP Dgrams 199
SCTP Rcvd: SCTP Dgrams 30, Chunks 209, Data Chunks 198, ULP Dgrams 198
Chunks Discarded: 0,  Retransmitted 0
```

Sample Output for the debug ip sctp rcvchunks Command

Caution This command generates multiple debug lines for each chunk received. Use with extreme caution in a live network.

In the following example, a segmented datagram is received in two chunks, for stream 0 and sequence number 0. The length of the first chunk is 1452, and the second is 1 byte. The first chunk indicates that it is for a new datagram, but the second chunk indicates that it is part of an existing datagram that is already being reassembled. When the first chunk is processed, it is noted to be in sequence, but is not complete and so cannot be delivered yet. When the second chunk is received, the datagram is both in sequence and complete. The application receives the datagram, and a SACK is shown to acknowledge that both chunks were received with no missing chunks indicated (that is, with no fragments).

```
Router# debug ip sctp rcvchunks

SCTP: Assoc 0: New chunk (0/0/1452/2C33D822) for new dgram (0)
SCTP: Assoc 0: dgram (0) is in seq
SCTP: Assoc 0: Add Sack Chunk, CumTSN=2C33D822, numFrags=0
SCTP: Assoc 0: New chunk (0/0/1/2C33D823) for existing dgram (0)
```

```
SCTP: Assoc 0: dgram (0) is complete
SCTP: Assoc 0: ApplRecv chunk 0/0/1452/2C33D822
SCTP: Assoc 0: ApplRecv chunk 0/0/1/2C33D823
SCTP: Assoc 0: Add Sack Chunk, CumTSN=2C33D823, numFrags=0
```

The following example is taken from a specific test in which chunks are both sent out of sequence and duplicated. The first chunk received is for stream 0, with sequence number 5. The datagram is complete, but is not in sequence because the previously received datagram was sequence number 3. A SACK chunk is sent, indicating that there is a gap after TSN 15755E58. This same chunk is received again, and the debug indicates that this chunk is a duplicate and so is not processed. The next chunk received is sequence number 7, also complete but not in sequence. The number of fragments specified is now 2, because both datagrams 4 and 6 have not been received. The duplicate chunk is discarded again. Sequence number 6 is then received, also complete, but not in sequence. The next earliest datagram received is 5, and even though that is in sequence, datagram 5 is not in sequence because datagram 4 has not been received and so neither 5 nor 6 can be delivered. Thus, there are occasions when the previous sequence number shown is in sequence, but the datagram itself is specified as not in sequence. The SACK sent at that point indicates just one fragment, because datagrams 5 through 7 are all in sequence in a block. Finally, datagram 4 is received. It is complete and in sequence, and datagrams 5 through 7 become in sequence as well, and all the datagrams can be received by the application.

```
Router# debug ip sctp rcvchunks

SCTP: Assoc 0: New chunk (0/5/50/15755E5A) for new dgram (5)
SCTP: Assoc 0: dgram (5) is complete
SCTP: Assoc 0: dgram (5) is not in seq, prev seq (3)
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=1
SCTP: Assoc 0: Rcvd duplicate chunk: 0/5/50/15755E5A
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=1
SCTP: Assoc 0: New chunk (0/7/50/15755E5C) for new dgram (7)
SCTP: Assoc 0: dgram (7) is complete
SCTP: Assoc 0: dgram (7) is not in seq, prev seq (5)
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=2
SCTP: Assoc 0: Rcvd duplicate chunk: 0/7/50/15755E5C
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=2
SCTP: Assoc 0: New chunk (0/6/50/15755E5B) for new dgram (6)
SCTP: Assoc 0: dgram (6) is complete
SCTP: Assoc 0: dgram (6) is not in seq, prev seq (5)
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=1
SCTP: Assoc 0: Rcvd duplicate chunk: 0/6/50/15755E5B
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E58, numFrags=1
SCTP: Assoc 0: New chunk (0/4/50/15755E59) for new dgram (4)
SCTP: Assoc 0: dgram (4) is complete
SCTP: Assoc 0: dgram (4) is in seq
SCTP: Assoc 0: dgram (5) is now in seq
SCTP: Assoc 0: dgram (6) is now in seq
SCTP: Assoc 0: dgram (7) is now in seq
SCTP: Assoc 0: Rcvd duplicate chunk: 0/4/50/15755E59
SCTP: Assoc 0: Add Sack Chunk, CumTSN=15755E5C, numFrags=0
SCTP: Assoc 0: ApplRecv chunk 0/4/50/15755E59
SCTP: Assoc 0: ApplRecv chunk 0/5/50/15755E5A
SCTP: Assoc 0: ApplRecv chunk 0/6/50/15755E5C
SCTP: Assoc 0: ApplRecv chunk 0/7/50/15755E5B
```

Sample Output for the debug ip sctp rto Command

Caution This command can generate a great deal of output. Use with extreme caution in a live network.

In the following example, there is only one destination address available. Each time the chunk needs to be retransmitted, the retransmission timeout (RTO) value is doubled.

```
Router# debug ip sctp rto

SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 2000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 4000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 8000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 16000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 32000 ms
```

In the next example, there is again only one destination address available. The data chunk is retransmitted several times, and the heartbeat timer also expires, causing the RTO timer to back off as well. Note that the heartbeat timer is expiring along with the data chunk retransmission timer, because SCTP is continually trying to send a chunk on which it can calculate the current round trip time (RTT). Because the data chunk is being retransmitted, an RTT calculation cannot be made on it, and the heartbeat is used instead.

```
Router# debug ip sctp rto

SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 98432842
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 2000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 98432842
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 4000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 98432842
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 8000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, heartbeat rto backoff 16000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 98432842
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 32000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, heartbeat rto backoff 60000 ms
```

Sample Output for the debug ip sctp segments Command

Caution This command generates several lines of output for each datagram sent or received. Use with extreme caution in a live network.

The following output shows an example in which an association is established, a few heartbeats are sent, the remote endpoint fails, and the association is restarted.

```
Router# debug ip sctp segments

SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 56
SCTP:        INIT_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 56
SCTP:        INIT_CHUNK, Tag: 13E5AD6C, TSN: 13E5AD6C
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 136
SCTP:        INIT_ACK_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 100
SCTP:        COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 16
SCTP:        COOKIE_ACK_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:        HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:        HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:        HEARTBEAT_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 56
SCTP:        INIT_CHUNK, Tag: 4F2D8235, TSN: 4F2D8235
```

```
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 136
SCTP:        INIT_ACK_CHUNK, Tag: 7DD7E424, TSN: 7DD7E424
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 100
SCTP:        COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 16
SCTP:        COOKIE_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 144
SCTP:        SACK_CHUNK, TSN ack: 7DD7E423, rwnd 18000, num frags 0
SCTP:        DATA_CHUNK, 4/0/100/4F2D8235
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP:        SACK_CHUNK, TSN ack: 4F2D8235, rwnd 8900, num frags 0
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 128
SCTP:        DATA_CHUNK, 4/0/100/7DD7E424
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:        SACK_CHUNK, TSN ack: 7DD7E424, rwnd 17900, num frags 0
SCTP: Recv:  Assoc 0: s=10.6.0.4  8787, d=10.2.0.2  8787, len 44
SCTP:        HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.2.0.2  8787, d=10.6.0.4  8787, len 44
SCTP:        HEARTBEAT_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 128
SCTP:        DATA_CHUNK, 7/0/100/4F2D8236
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 144
SCTP:        SACK_CHUNK, TSN ack: 4F2D8236, rwnd 9000, num frags 0
SCTP:        DATA_CHUNK, 7/0/100/7DD7E425
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:        SACK_CHUNK, TSN ack: 7DD7E424, rwnd 18000, num frags 0
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:        SACK_CHUNK, TSN ack: 7DD7E425, rwnd 17900, num frags 0
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 128
SCTP:        DATA_CHUNK, 4/1/100/4F2D8237
```

Sample Output for the debug ip sctp segmentv Command

Caution This command generates multiple lines of output for each datagram sent and received.Use with extreme caution in a live network.

The following output shows an example in which an association is established, a few heartbeats are sent, the remote endpoint fails, and the association is restarted.

```
Router# debug ip sctp segmentv

SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 56, ver tag 0
SCTP:        INIT_CHUNK, len 42
SCTP:        Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:        Streams Inbound: 13, Outbound: 13
SCTP:        IP Addr: 10.1.0.2
SCTP:        IP Addr: 10.2.0.2
SCTP:        Supported addr types: 5
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 56, ver tag 0
SCTP:        INIT_CHUNK, len 42
SCTP:        Initiate Tag: 5516B2F3, Initial TSN: 5516B2F3, rwnd 18000
SCTP:        Streams Inbound: 13, Outbound: 13
SCTP:        IP Addr: 10.5.0.4
SCTP:        IP Addr: 10.6.0.4
SCTP:        Supported addr types: 5
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 136, ver tag 5516B2F3
SCTP:        INIT_ACK_CHUNK, len 124
SCTP:        Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:        Streams Inbound: 13, Outbound: 13
SCTP:        Responder cookie len 88
SCTP:        IP Addr: 10.1.0.2
```

```
SCTP:        IP Addr: 10.2.0.2
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 100, ver tag B131ED6A
SCTP:        COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 16, ver tag 5516B2F3
SCTP:        COOKIE_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 144, ver tag B131ED6A
SCTP:        SACK_CHUNK, len 16
SCTP:        TSN ack: (0xB131ED69)
SCTP:        Rcv win credit: 18000
SCTP:        Num frags: 0
SCTP:        DATA_CHUNK, flags 3, chunkLen 116
SCTP:        DATA_CHUNK, 0/0/100/5516B2F3
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28, ver tag 5516B2F3
SCTP:        SACK_CHUNK, len 16
SCTP:        TSN ack: (0x5516B2F3)
SCTP:        Rcv win credit: 8900
SCTP:        Num frags: 0
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 128, ver tag 5516B2F3
SCTP:        DATA_CHUNK, flags 3, chunkLen 116
SCTP:        DATA_CHUNK, 0/0/100/B131ED6A
SCTP: Recv:  Assoc 0: s=10.6.0.4  8787, d=10.2.0.2  8787, len 44, ver tag B131ED6A
SCTP:        HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.2.0.2  8787, d=10.6.0.4  8787, len 44, ver tag 5516B2F3
SCTP:        HEARTBEAT_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28, ver tag B131ED6A
SCTP:        SACK_CHUNK, len 16
```

Sample Output for the debug ip sctp signal Command and the debug ip sctp state Command

This example shows signals that are sent from SCTP to the application or ULP. A signal is also sent to the ULP when new data is available to be received, but this signal is not shown in the output below because it occurs infrequently.

In the following example, a new association is requested and established. The peer then restarts the association and notes that the association failed and is being reestablished. The local peer then indicates that the association has failed because it has tried to retransmit the specified chunk more than the maximum number of times without success. As a result, the association fails (because of communication loss) and is terminated. The ULP requests that the association be attempted again, and this attempt succeeds. A shutdown is then received from the remote peer, and the local peer enters the shutdown acknowledge sent state, which is followed by the association being terminated. Again, another association attempt is made and succeeds.

```
Router# debug ip sctp signal
Router# debug ip sctp state

<new assoc attempt>
00:20:08: SCTP: Assoc 0:  state CLOSED -> COOKIE_WAIT
00:20:15: SCTP: Assoc 0:  state COOKIE_WAIT -> ESTABLISHED
00:20:15: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:03: SCTP: Assoc 0: Restart rcvd from peer
00:21:03: SCTP: Assoc 0: Sent ASSOC_RESTART signal
00:21:04: SCTP: Assoc 0: chunk 62EA7F40 retransmitted more than max times, failing assoc
00:21:04: SCTP: Assoc 0: Sent ASSOC_FAILED signal, reason: SCTP_COMM_LOST
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0:  state ESTABLISHED -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0:  state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0:  state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0:  state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:04: SCTP: Assoc 0: Sent TERMINATE_PENDING signal
00:21:04: SCTP: Assoc 0:  state ESTABLISHED -> SHUTDOWN_ACKSENT
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
```

```
00:21:04: SCTP: Assoc 0:  state SHUTDOWN_ACKSENT -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0:  state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0:  state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0:  state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
```

In the following example, the associations themselves are stable, but a particular destination address fails. Because both currently established associations are using the same destination addresses (with different ports), both of the associations indicate the destination address failure. When the destination address again becomes active, the upper-layer protocols are informed.

```
Router#
00:26:27: SCTP: Assoc 1: Sent DESTADDR_FAILED signal for destaddr 10.6.0.4
00:26:28: SCTP: Assoc 0: Sent DESTADDR_FAILED signal for destaddr 10.6.0.4
Router#
00:30:41: SCTP: Assoc 1: Sent DESTADDR_ACTIVE signal for destaddr 10.6.0.4
00:30:41: SCTP: Assoc 0: Sent DESTADDR_ACTIVE signal for destaddr 10.6.0.4
```

Sample Output for the debug ip sctp sndchunks Command

Caution This command generates significant data if there is any significant amount of traffic flowing. Use with extreme caution in live networks.

```
Router# debug ip sctp sndchunks

SCTP: Assoc 0: ApplSend, chunk: 0/10412/100/A23134F8 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10443/100/A23134F9 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10448/100/A231355C to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A23134F8
SCTP: Assoc 0: Bundling data, added 0/10412/100/A23134F8, outstanding 100
SCTP: Assoc 0: Bundling data, added 5/10443/100/A23134F9, outstanding 200
SCTP: Assoc 0: Bundling data, added 4/10545/100/A23134FA, outstanding 300
SCTP: Assoc 0: Bundling data, added 10/10371/100/A23134FB, outstanding 400
SCTP: Assoc 0: Bundling data, added 11/10382/100/A23134FC, outstanding 500
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231350F, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313510
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313527, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313528
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231353F, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313540
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313557, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313558
SCTP: Assoc 0: ApplSend, chunk: 10/10385/100/A23135BE to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 8/10230/100/A23135BF to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10459/100/A23135C0 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 4/10558/100/A23135C1 to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A231355D
SCTP: Assoc 0: Bundling data, added 5/10449/100/A231355D, outstanding 100
SCTP: Assoc 0: Bundling data, added 3/10490/100/A231355E, outstanding 200
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135A4, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135A5
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135BC, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135BD
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135C1, numFrags=0
SCTP: Assoc 0: ApplSend, chunk: 5/10460/100/A23135C2 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10461/100/A23135C3 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 11/10403/100/A2313626 to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A23135C2
SCTP: Assoc 0: Bundling data, added 5/10460/100/A23135C2, outstanding 100
SCTP: Assoc 0: Bundling data, added 5/10461/100/A23135C3, outstanding 200
```

```
SCTP: Assoc 0: Bundling data, added 5/10462/100/A23135C4, outstanding 300
SCTP: Assoc 0: Bundling data, added 4/10559/100/A23135C5, outstanding 400
SCTP: Assoc 0: Bundling data, added 4/10560/100/A23135C6, outstanding 500
SCTP: Assoc 0: Bundled 12 chunk(s) in next dgram to 10.5.0.4
SCTP: Assoc 0: Bundling data, added 1/10418/100/A2313622, outstanding 9700
SCTP: Assoc 0: Bundling data, added 3/10502/100/A2313623, outstanding 9800
SCTP: Assoc 0: Bundling data, added 7/10482/100/A2313624, outstanding 9900
SCTP: Assoc 0: Bundling data, added 3/10503/100/A2313625, outstanding 10000
SCTP: Assoc 0: Bundling data, added 11/10403/100/A2313626, outstanding 10100
SCTP: Assoc 0: Bundled 5 chunk(s) in next dgram to 10.5.0.4
SCTP: Assoc 0: Mark chunk A23135C2 for retrans
SCTP: Assoc 0: Mark chunk A23135C3 for retrans
SCTP: Assoc 0: Mark chunk A23135C4 for retrans
SCTP: Assoc 0: Mark chunk A23135C5 for retrans
SCTP: Assoc 0: Mark chunk A23135C6 for retrans
SCTP: Assoc 0: Mark chunk A23135C7 for retrans
SCTP: Assoc 0: Mark chunk A23135C8 for retrans
SCTP: Assoc 0: Mark chunk A23135C9 for retrans
SCTP: Assoc 0: Mark chunk A23135CA for retrans
SCTP: Assoc 0: Bundled 6 chunk(s) in next dgram to 10.6.0.4
SCTP: Assoc 0: Mark chunk A23135C2 for retrans
SCTP: Assoc 0: Mark chunk A23135C3 for retrans
SCTP: Assoc 0: Mark chunk A23135C4 for retrans
```

Sample Output for the debug ip sctp timer Command

Caution This command generates a significant amount of output. Use with extreme caution in a live network.

```
Router# debug ip sctp timer

SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Timer BUNDLE triggered
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Stopping RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Stopping RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Stopping CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
```

Sample Output for the debug ip sctp warnings Command

```
Router# debug ip sctp warnings

SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: Incoming INIT_ACK: inbound streams reqd 15, allowed 13
SCTP: Assoc 0: Incoming INIT_ACK request: outbound streams req'd 13, allowed 1
SCTP: Assoc 0: Remote verification tag in init ack is zero, discarding
SCTP: Remote verification tag in init is zero, discarding
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 0
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 1499
SCTP: Rwnd in INIT too small (0), discarding
SCTP: Rwnd in INIT too small (1499), discarding
SCTP: Unknown INIT param 16537 (0x4099), length 8
SCTP: Assoc 0: Unknown INITACK param 153 (0x99), length 8
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Processing INIT, invalid param len 0, discarding...
SCTP: Assoc 0: Processing INITACK, invalid param len 0, discarding...
```

Sample Output for the debug iua Command

The following example shows that state debugging is turned on for all application servers and that the application server is active:

```
Router# debug iua as state all

IUA :state debug turned ON for ALL AS

00:11:52:IUA:AS as1 number of ASPs up is 1
00:11:57:IUA:AS as1 xsition AS-Up -->  AS-Active, cause - ASP asp1
```

The following example shows that peer message debugging is turned on for all digital signal processors (DSPs) and that the ASP is active:

```
Router# debug iua asp peer-msg all

IUA :peer message debug turned ON for ALL ASPs

Router#
00:04:58:IUA :recieved ASP_UP message on ASP asp1
00:04:58:IUA:ASP asp1 xsition ASP-Down -->  ASP-Up , cause -  rcv peer
msg
ASP-UP
00:04:58:IUA:sending ACK of type 0x304 to asp asp1
00:05:03:IUA:recv ASP_ACTIVE message for ASP asp1
00:05:03:IUA:ASP asp1 xsition ASP-Up -->  ASP-Active, cause - rcv peer
msg
ASP-Active
```

Configuration Examples for SCTP Options

Application-Server and Application-Server-Process: Example

The following shows sample SCTP configuration options using the help menu for the **as** and **asp** commands:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# iua

Router(config-iua)# as as1 ?

  A.B.C.D           Specify (up to two) Local IP address
  Fail-Over-Timer   Configure the Fail-Over timer for this AS
  sctp-startup-rtx  Configure the SCTP max startup retransmission timer
  sctp-streams      Configure the number of SCTP streams for this AS
  sctp-t1init       Configure the SCTP T1 init timer

Router(config-iua)# as as1 sctp-startup-rtx ?

  <2-20>  Set SCTP Maximum Startup Retransmission Interval

Router(config-iua)# as as1 sctp-streams ?

  <1-56>  Specify number of SCTP streams for association

Router(config-iua)# as as1 sctp-t1init ?

  <1000-60000>  Set SCTP T1 init timer (in milliseconds)

Router(config-iua)# asp asp1 as as1 ?

  A.B.C.D  Specify (up to two) IP addresses of the call-agent

Router(config-iua)# asp asp1 ?

  AS                Specify which AS this ASP belongs to
  IP-Precedence     Set IP precedence bits for a IP address in this ASP
  sctp-keepalives   Modify the keep-alive behaviour of an IP address in this
                    ASP
  sctp-max-assoc    Set SCTP max association retransmissions for this ASP
  sctp-path-retran  Set SCTP path retransmissions for this ASP
  sctp-t3-timeout   Set SCTP T3 retransmission timeout for this ASP

Router(config-iua)# asp asp1 sctp-keep ?

  A.B.C.D  specify the IP address to enable/disable keep alives

Router(config-iua)# asp asp1 sctp-keepalive 10.10.10.10 ?

  <1000-60000>  specify keep alive interval (in milliseconds)

Router(config-iua)# asp asp1 sctp-max-assoc ?

  A.B.C.D  specify the IP address

Router(config-iua)# asp asp1 sctp-max-assoc 10.10.10.10 ?
```

```
  <2-20>   specify maximum associations
  default  use default value of max associations for this address

Router(config-iua)# asp asp1 sctp-path-retran ?

  A.B.C.D  specify the IP address

Router(config-iua)# asp asp1 sctp-path-retran 10.10.10.10 ?

  <2-10>   specify maximum path retransmissions
  default  use default value of max path retrans for this address

Router(config-iua)# asp asp1 sctp-t3-timeout ?

  A.B.C.D  specify the IP address

Router(config-iua)# asp asp1 sctp-t3-timeout 10.10.10.10 ?

  <300-60000>  specify T3 retransmission timeout (in milliseconds)
  default      use default value of T3 for this address
```

Application-Server and Application-Server-Process with IUA: Example

The following example shows a running application-server configuration with IUA configured with one application server (as1) and two application-server processes (asp1 and asp2). Four T1s (T1 1/0, 1/1, 2/0, 2/1) are configured to use IUA backhaul.

```
Router# show running-config

Building configuration...

Current configuration :2868 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname iua_3660_b
!
logging rate-limit console 10 except errors
!
memory-size iomem 30
voice-card 1
!
voice-card 2
!
voice-card 3
!
voice-card 4
!
voice-card 5
!
voice-card 6
!
ip subnet-zero
!
no ip domain-lookup
!
```

```
no ip dhcp-client network-discovery
iua
  AS as1 10.21.0.2 9900
   ASP asp1 AS as1 10.23.0.16 9900
   ASP asp2 AS as1 10.23.0.16 9911
isdn switch-type primary-5ess
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 1/0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 2/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 3/0
 framing sf
 linecode ami
!
controller T1 3/1
 framing sf
 linecode ami
!
controller T1 4/0
 framing sf
 linecode ami
!
controller T1 4/1
 framing sf
 linecode ami
!
controller T1 5/0
 framing sf
 linecode ami
!
controller T1 5/1
 framing sf
 linecode ami
!
controller T1 6/0
 framing sf
 linecode ami
!
controller T1 6/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
```

```
 ip address 10.21.0.3 255.255.0.0 secondary
 ip address 10.21.0.2 255.255.0.0
 speed 10
 half-duplex
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial1/1:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn guard-timer 3000
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial2/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn guard-timer 3000
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial2/1:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.21.0.17
ip route 11.0.0.10 255.255.255.255 FastEthernet0/0
ip route 172.0.0.0 255.0.0.0 172.18.194.1
ip http server
!
snmp-server manager
!
call rsvp-sync
!
voice-port 1/0:23
!
```

```
voice-port 1/1:23
!
voice-port 2/0:23
!
voice-port 2/1:23
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
 transport input none

line aux 0
line vty 0 4
 login
!
end
```

ISDN Signaling Backhaul: Example

The following sample output shows that Layers 1, 2, and 3 are enabled and active. Layer 3 shows the number of active ISDN calls.

Notice that the Layer 2 protocol is Q.921 and the Layer 3 protocol is BACKHAUL. This verifies that the system is configured to backhaul ISDN.

If you are connected to a live line, you should see that Layer 1 is active and Layer 2 is MULTIPLE_FRAME_ESTABLISHED, meaning that the ISDN line is up and active.

```
Router# show isdn status

*00:03:34.423 UTC Sat Jan 1 2000
Global ISDN Switchtype = primary-net5
ISDN Serial1:23 interface
        dsl 0, interface ISDN Switchtype = primary-net5
        L2 Protocol = Q.921  L3 Protocol(s) = BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
        NLCB:callid=0x0, callref=0x0, state=0, ces=1 event=0x0
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Number of active calls = 0
    Number of available B-channels = 23
    Total Allocated ISDN CCBs = 0
```

IUA Configuration: Example

The following is an example of an application-server configuration on a gateway:

```
as as5400-3 10.4.8.69 10.4.9.69 2577
```

In the configuration above, an application server named as-named as5400-3 is configured to use two local IP addresses and a port number of 2577. IP address values that are set apply to all IP addresses of the ASP.

The following configuration example defines a remote signaling controller *asp1* at two IP addresses for the application server named as5400-3. The remote SCTP port number is 2577:

```
Router(config-iua)# as as5400-3 10.4.8.69 10.4.9.69 2477

Router(config-iua)# asp asp1 as as5400-3 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single application server for the purpose of redundancy, but only one ASP can be active. The other ASP is inactive and only becomes active after fail-over.

In the Cisco MGC solution, a signaling controller is always the client that initiates the association with a gateway. During the initiation phase, you can request outbound and inbound stream numbers, but the gateway only allows a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The number of streams to assign to a given association is implementation dependent. During the initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple trunk group support, every interface can potentially be a separate D channel.

At startup, the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the GW and the MGC. For the rare case that you are configuring multiple application-server associations to various MGCs, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during startup the IUA code adds one to the total number of interfaces (streams) found.

You have the option to manually configure the number of streams per association. In the backhaul scenario, if the number of D channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that will never be used. For multiple associations between a GW and multiple MGCs, the configuration utility is useful in providing only the necessary number of streams per association. The overhead from the streams allocated but not used in the association is negligible.

If the number of streams is manually configured through the CLI, the IUA code cannot distinguish between a startup event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you are configuring the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword with the **as** command. Otherwise, IUA needs to always add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with the CLI, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA application-server configuration and then configure it back as the same application server or a new one. The other option is to reload the router.

The following is an example of an application-server configuration on a gateway. The configuration shows that an application server named as5400-3 is configured to use two local IP addresses and a port number of 2577:

```
Router(config-iua)# as as5400-3 10.1.2.34 10.1.2.35 2577
```

The following example sets the failover time (in milliseconds) between 1 and 10 seconds. Entering a value of 1000 would equal one second. Entering a value of 10000 would equal 10 seconds. In this example, the failover timer has been set to 10 seconds:

```
Router(config-iua)# as as5400-3 fail-over 10000
```

The following example specifies the number of SCTP streams for this association. In this example, 57 is the maximum number of SCTP streams allowed:

```
Router(config-iua)# as as5400-3 sctp-streams 57
```

The following example sets the SCTP maximum startup retransmission interval. In this example, 20 is the maximum interval allowed:

```
Router(config-iua)# as as5400-3 sctp-startup 20
```

The following example sets the SCTP T1 initiation timer in milliseconds. In this example, 60000 is the maximum time allowed:

```
Router(config-iua)# as as5400-3 sctp-t1init 60000
```

The following example specifies the IP address to enable and disable keepalives:

```
Router(config-iua)# asp asp1 sctp-keepalive 10.1.2.34
```

The following example specifies the keepalive interval in milliseconds. Valid values range from 1000 to 60000. In this example, the maximum value of 60000 ms is used:

```
Router(config-iua)# asp asp1 sctp-keepalive 10.10.10.10 60000
```

The following example specifies the IP address for the SCTP maximum association and the maximum association value. Valid values are from 2 to 20. The default is 20, which is the maximum value allowed:

```
Router(config-iua)# asp asp1 sctp-max-association 10.10.10.10 20
```

The following example specifies the IP address for the SCTP path retransmission and the maximum path retransmission value. Valid values are from 2 to 10. The default is 10, which is the maximum value allowed:

```
Router(config-iua)# asp asp1 sctp-path-retransmissions 10.10.10.10 10
```

The following examples specifies the IP address for SCTP T3 timeout and specifies the T3 timeout value in milliseconds. Valid timeout values are from 300 to 60000. The default is 60000, which is the maximum timeout value allowed:

```
Router(config-iua)# asp asp1 sctp-t3-timeout 10.10.10.10 60000
```

The following example configures the following:

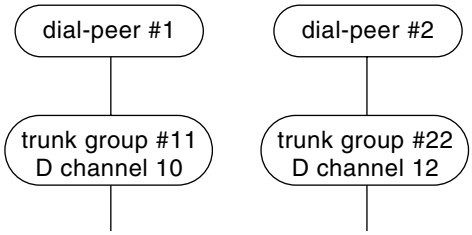
1. Creates an IUA application server (Cisco AS5300-17) that has two local IP addresses (10.0.0.07 and 10.1.1.17) and local port 2097.
2. IUA application server Cisco AS5300-17 is connected by two SCTP associations (ASP PGW A and ASP PGW B) to two hot-standby Cisco PGW 2200s (Cisco PGW 2200 PGW A and Cisco PGW 2200 PGW B). Cisco PGW 2200 PGW A has remote IP addresses 10.0.0.00 and 10.1.1.10, and Cisco PGW 2200 PGW B has remote IP addresses 10.0.0.06 and 10.1.1.16.
3. Two NFAS groups (nfas-group 1 and nfas-group 2), which are both bound to IUA application server as5300-17.
4. Two trunk groups (trunk-group 11 and trunk-group 22)—Trunk-group 11 is bound to interface Dchannel0 and trunk-group 22 is bound to interface Dchannel2.

```
Router(config-iua)# as as5300-17 10.0.0.07 10.1.1.17 2097
```

```
Router(config-iua)# asp pgwa AS as5300-17  10.0.0.00 10.1.1.10 2097
Router(config-iua)# asp pgwb AS as5300-17  10.0.0.06 10.1.1.16 2097
```

Figure 13 shows the configuration above in diagram form with two outgoing POTS dial-peers (dial-peer 1 and dial-peer 2)—dial-peer 1 points to trunk-group 11, and dial-peer 2 points to trunk-group 22.

Figure 13 Specific ASP Example Configuration



The following is example output from the above configuration:

```
iua
   AS as5300-17 10.0.0.07 10.1.1.17 2097
   ASP pgwa AS as5300-17  10.0.0.00 10.1.1.10 2097
   ASP pgwb AS as5300-17  10.0.0.06 10.1.1.16 2097
!
!
controller E1 0
 framing NO-CRC4
 clock source line primary
 pri-group timeslots 1-31 nfas-d primary nfas-int 0 nfas-group 1 iua as5300-17
!
controller E1 1
 framing NO-CRC4
 clock source line secondary 1
 pri-group timeslots 1-31 nfas-d none nfas-int 1 nfas-group 1
!
controller E1 2
 framing NO-CRC4
 pri-group timeslots 1-31 nfas-d primary nfas-int 0 nfas-group 2 iua as5300-17
!
controller E1 3
 framing NO-CRC4
 pri-group timeslots 1-31 nfas-d none nfas-int 1 nfas-group 2
!
```

```
!
interface Ethernet0
 description the ip is 10.0.0.06 for interface e0
 ip address 10.0.0.06 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0
 description the primary ip is 10.1.1.16 for interface f0
 ip address 10.1.1.10 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Dchannel0
 no ip address
 trunk-group 11
 isdn timer t309 100
 isdn timer t321 30000
 isdn incoming-voice modem
 isdn T303 20000
 isdn negotiate-bchan resend-setup
 no cdp enable
!
interface Dchannel2
 no ip address
 trunk-group 22
 isdn timer t309 100
 isdn timer t321 30000
 isdn incoming-voice modem
 isdn T303 20000
 isdn negotiate-bchan resend-setup
 no cdp enable
!
trunk group 11
!
trunk group 22
!
dial-peer voice 1 pots
 incoming called-number
 destination-pattern 997001
 direct-inward-dial
 trunk-group 11
 forward-digits all
!
dial-peer voice 2 pots
 incoming called-number
 destination-pattern 997002
 direct-inward-dial
 trunk-group 22
 forward-digits all
!
```

The following example shows a running application-server configuration with IUA configured with one application server (as1) and two ASPs (asp1 and asp2). Four T1s (T1 1/0, 1/1, 2/0, 2/1) are configured to use IUA backhaul.

```
Router# show running config

Building configuration...

Current configuration :2868 bytes
!
```

```
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname iua_3660_b
!
logging rate-limit console 10 except errors
!
memory-size iomem 30
voice-card 1
!
voice-card 2
!
voice-card 3
!
voice-card 4
!
voice-card 5
!
voice-card 6
!
ip subnet-zero
!
no ip domain-lookup
!
no ip dhcp-client network-discovery
iua
  AS as1 10.21.0.2 9900
   ASP asp1 AS as1 10.23.0.16 9900
   ASP asp2 AS as1 10.23.0.16 9911
isdn switch-type primary-5ess
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 1/0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 2/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 3/0
 framing sf
 linecode ami
!
controller T1 3/1
 framing sf
```

```
 linecode ami
!
controller T1 4/0
 framing sf
 linecode ami
!
controller T1 4/1
 framing sf
 linecode ami
!
controller T1 5/0
 framing sf
 linecode ami
!
controller T1 5/1
 framing sf
 linecode ami
!
controller T1 6/0
 framing sf
 linecode ami
!
controller T1 6/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.21.0.3 255.255.0.0 secondary
 ip address 10.21.0.2 255.255.0.0
 speed 10
 half-duplex
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial1/1:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn guard-timer 3000
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial2/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
```

```
 isdn guard-timer 3000
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
interface Serial2/1:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn T203 10000
 isdn bind-l3 iua-backhaul as1
 no cdp enable
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.21.0.17
ip route 11.0.0.10 255.255.255.255 FastEthernet0/0
ip route 172.0.0.0 255.0.0.0 172.18.194.1
ip http server
!
snmp-server manager
!
call rsvp-sync
!
voice-port 1/0:23
!
voice-port 1/1:23
!
voice-port 2/0:23
!
voice-port 2/1:23
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
 transport input none

line aux 0
line vty 0 4
 login
!
end
```

PRI Group on an MGC: Example

To modify a PRI group on a third-party call agent (MGC), the **isdn bind** commands must be removed from the D channel. The binding of the NFAS groups now takes place when you use the **pri-group (pri-slt)** command for IUA with SCTP.

Use the following examples to help you with your configuration:

- Controller configuration for primary span in an NFAS group for RLM. You can choose any time slot other than 24 to be the virtual container for the D channel parameters for ISDN:

```
controller T1 3/0:1
 framing esf
 pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1
```

- Controller configuration for primary span in an NFAS group for IUA:

```
controller T1 3/0:1
 framing esf
 pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1 iua as-1
```

SCTP Configuration: Example

You can implicitly configure the number of streams in SCTP by specifying only the serial interfaces that are configured to use IUA. The number of streams is bound to the actual number of interfaces supporting IUA. To support Cisco MGC solutions, you can configure any number of streams for each NFAS D channel, up to the total number of interfaces available in a given GW. For platforms using the PRI backhaul with SCTP and the ISDN Q.921 User Adaptation Layer (UAL), such as the Cisco 3660, you can configure the number of streams to match the number of PRIs that are actually backhauled to the Telcordia session manager.

The following example sets the failover time (in milliseconds) between 1 and 10 seconds. Entering a value of 1000 would equal one second. Entering a value of 10000 would equal 10 seconds. In this example, the failover timer has been set to 10 seconds. The default value is 4000 msec. Once you have set the failover timer to a value, you can return it to its default of 4000 msec by using the **no** form of this command.

```
Router(config-iua)# as as5400-3 fail-over 10000
```

The following example sets the SCTP maximum startup retransmission interval. Valid values are from 2 to 20:

```
Router(config-iua)# as as1 sctp-startup-rtx 20
```

The following example specifies the number of SCTP streams for an association. Valid values are from 1 to 56:

```
Router(config-iua)# as as1 sctp-streams 56
```

The following example sets the SCTP T1 initiation timer in milliseconds. Valid values are from 1000 to 60000:

```
Router(config-iua)# as as1 sctp-t1init 60000
```

SCTP Migration from RLM to IUA: Example

The following changes have been made between RLM and IUA with SCTP. Use the examples in this section to help you with your configuration:

- The D channel **interface serial** commands are now replaced by **interface D channel** commands.

  For RLM, the following format was used:

  ```
  interface Serial3/0:1:23
  ```

Note The :23 in the RLM example above, which typically corresponds with T1 configuration (:15 for E1 configuration), is no longer used.

For IUA, the following format is used:

```
interface Dchannel3/0:1
```

- The RLM group configuration must be removed from the D channel configuration.

  For RLM, remove the "isdn rlm-group 1" line shown in bold:

```
interface Serial3/0:1:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 isdn T321 30000
 isdn T303 20000
 isdn T200 2000
 isdn rlm-group 1
 isdn negotiate-bchan resend-setup
 isdn bchan-number-order ascending
 no cdp enable
```

  For IUA, use the following format:

```
interface Dchannel3/0:1
 no ip address
 isdn timer t309 100
 isdn timer t321 30000
 isdn incoming-voice modem
 isdn T303 20000
 no isdn send-status-enquiry
 isdn negotiate-bchan resend-setup
 isdn bchan-number-order ascending
 no cdp enable
```

Trunk Group Bound to an Application Server: Example

You can configure the NFAS primary D channel on one channelized T1 controller, and bind the D channel to an IUA application server by using the **pri-group (pri-slt)** command.

This example uses a Cisco AS5400 and applies to T1, which has 24 timeslots and is used mainly in North America and Japan. You can choose any timeslot other than 24 to be the virtual container for the D channel parameters for ISDN.

```
Router(config-controller)# pri-group timeslots 1-23 nfas-d primary nfas-int 0 nfas-group 1
iua as5400-4-1
```

The following example applies to E1, which has 32 timeslots and is used by countries other than North America and Japan. You can choose any timeslot other than 32 to be the virtual container for the D channel parameters for ISDN.

```
Router(config-controller)# pri-group timeslots 1-31 nfas-d primary nfas-int 0 nfas-group 1
iua as5400-4-1
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- Cisco 2600 Series Routers documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm
- Cisco 3600 Series Routers documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm
- Cisco 3700 Series Routers documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/index.htm
- Cisco AS5300 documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/index.htm
- Cisco AS5400 documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm
- Cisco IAD2420 Series IADs documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/iad/iad2420/index.htm
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2 T at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_r/index.htm
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2T at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/index.htm
- *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/swinstl/index.htm
- *Cisco Media Gateway Controller Software Release 9 Messages Reference Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/errmsg/index.htm
- *Cisco Media Gateway Controller Software Release 9 MML Command Reference* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mmlref/index.htm
- *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/index.htm
- *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/prvgde/index.htm
- *Integrated Signaling Link Terminal*, Cisco IOS Release 12.2(11)T at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftintslt.htm
- *IP Transfer Point (ITP)*, Cisco IOS Release 12.2(2)MB at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122mb2/itp20/index.htm
- *PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_0546.htm
- *Stream Control Transmission Protocol (SCTP)* feature at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sctp2.htm
- *Stream Control Transmission Protocol (SCTP)*, RFC 2960, at http://rfc2960.x42.com/
- *Support for IUA with SCTP* at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgcfm/941fm/fmiua.htm

- *Support for IUA with SCTP for Cisco Access Servers* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftgkrup.htm
- *Troubleshooting and Fault Management Commands* (chapter in the System Management Commands part of the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2) at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf013.htm

Implementing QSIG for Tcl IVR

This chapter describes how to implement the QSIG for Tool Command Language Interactive Voice Response (Tcl IVR) 2.0 feature. Q.SIG support is required for European countries to interconnect enterprise customers to a wholesale voice solution. The feature provides transparent Q.SIG interworking with a Tcl IVR 2.0 voice application on a Cisco IOS voice gateway. This functionality can be enabled using a new CLI on the POTS or VoIP dial-peer. Prior to this feature, Q.SIG messages were interpreted by the Tcl IVR 2.0 application, rather than passed transparently to the remote endpoint.

Feature benefits include the following:

- Increased interconnection options for VoIP wholesale providers
- Elimination of unnecessary decoding

Feature History for QSIG for Tcl IVR 2.0

Release	Modification
12.2(11)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 221.

Contents

Prerequisites for Configuring QSIG for Tcl IVR 2.0

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an ISDN Voice Interface" section on page 15.
- Establish a working IP network. For more information, see the Cisco IOS documentation set. See specifically the *Cisco IOS IP and IP Routing Configuration Guide* and the *Cisco IOS Voice, Video, and Fax Configuration Guide*.
- Configure VoIP. For more information, see the *Cisco IOS Voice, Video, and Fax Configuration Guide*.
- Download the Tcl scripts required for this feature from the following website: http://www.cisco.com/cgi-bin/tablebuild.pl/tclware
- Ensure that the VCWare version used for the Cisco AS5300 is compatible with the Cisco IOS image being used.

Note VCWare applies only to the Cisco AS5300.

Before configuring IVR Version 2.0 features, do the following:

- Download the Tcl scripts and audio files to be used with this feature. Store them on a TFTP server configured to interact with your gateway access server.
- Create the IVR/Tcl application script to use when configuring IVR. Store it on a server or at a location where it can be retrieved by the gateway access server. Then configure the server to use IVR with the application that you created.
- Configure the dial peer on incoming POTS or VoIP dial peers.

Restrictions for Configuring QSIG for Tcl IVR 2.0

Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4. In addition, the following apply:

- This feature is applicable to only the following:
  - VoIP and POTS dial peers
  - Tcl IVR version 2.0 only; not version 1.0

Information About QSIG for Tcl IVR 2.0

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

Q.SIG support is required for European countries to interconnect enterprise customers to a wholesale voice solution. The Q.SIG for Tcl IVR 2.0 feature provides transparent Q.SIG interworking when using a Tcl IVR version 2.0 voice application on a Cisco IOS voice gateway. This functionality can be enabled using a new CLI on the POTS or VoIP dial-peer. Prior to this feature, Q.SIG messages were interpreted by the Tcl IVR 2.0 application, rather than passed transparently to the remote endpoint.

How to Configure QSIG for Tcl IVR 2.0

This section contains the following procedures:

- Configuring QSIG (required)
- Configuring Supplementary Service for a POTS Dial Peer (optional)
- Configuring Supplementary Service for a VoIP Dial Peer (optional)
- Verifying QSIG and Supplementary Service (optional)

Configuring QSIG

To configure QSIG, perform the following steps.

Note You must create the application that is to be called to interact with the dial peer (that collects the digits from the caller) before you configure the dial peer that will call this application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call application voice**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**call application voice** *application-name location* **Example:** `Router(config)# call application voice ap1 172.16.4.4`	Creates the application to be used with your IVR script and indicates the location of the corresponding Tcl files that implement this application. The location can be a URL, directory, or TFTP server.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring Supplementary Service for a POTS Dial Peer

To configure supplementary service for a POTS dial peer, perform the following steps.

Note

- The **supplementary-service pass-through** command controls the interpretation of supplementary service (QSIG, H.450, and so on) on a gateway. When the CLI is enabled (that is, set to passthrough mode), the supplementary service message (usually in Q.931 facility message) is transparently sent to the destination gateway without any interpretation (raw). When the CLI is not enabled (the default), the supplementary service message is decoded and interpreted by the gateway. This CLI is available under VoIP or POTS dial peers.
- This CLI has effect only if a Tcl IVR 2.0 application is configured on the same dial peer. The default session application always performs transparent Q.SIG interworking. Tcl IVR 1.0 applications always interpret and consume the Q.SIG supplementary services messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice pots**
4. **application**

5. **supplementary-service pass-through**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 99 pots`	Enters voice dial-peer configuration mode for the specified POTS dial peer.
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application ap1`	Specifies the application that handles incoming voice calls associated with this dial-peer.
Step 5	**supplementary-service pass-through** **Example:** `Router(config-dial-peer)# supplementary-service pass-through`	Configures supplementary service feature to transparently pass supplementary service to the next gateway.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Supplementary Service for a VoIP Dial Peer

To configure supplementary service for a VoIP dial peer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice voip**
4. **application**
5. **supplementary-service pass-through**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 96 voip`	Enters voice dial-peer configuration mode for the specified VoIP dial peer.
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application ap5`	Specifies the application that handles incoming voice calls associated with this dial-peer.'

Step 5	**supplementary-service pass-through**
	
	Example:
	`Router(config-dial-peer)#`
	`supplementary-service pass-through`
		Configures supplementary service feature to transparently pass supplementary service to the next gateway.

Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Verifying QSIG and Supplementary Service

To verify QSIG and supplementary service, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show isdn status**
2. **show running-config**

DETAILED STEPS

Step 1 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

Step 2 **show running-config**

Use this command to display the basic router configuration.

Configuration Example for QSIG for TcI IVR 2.0

The following sample output is typical of that for implementation of supplementary service. ISDN supplementary service messages from PBX 1 are sent transparently to PBX 2 by routers 1 and 2 as if PBX 1 and PBX 2 were connected directly to each other.

Figure 14 QSIG for Tcl IVR 2.0: Sample Network Topology


```
Router# show running-config

Building configuration...

Current configuration :3531 bytes
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname router
!
no logging buffered
!
resource-pool disable
!
ip subnet-zero
ip host jurai 223.255.254.254
ip host dirt 223.255.254.254
ip host CALLGEN-SECURITY-V2 15.90.60.59 1.82.0.0
!
trunk group  323
!
isdn switch-type primary-ni
!
voice service pots
!
fax interface-type modem
mta receive maximum-recipients 0
partition flash 2 8 8
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 1 timeslots 1-4 type e&m-fgb dtmf dnis
 cas-custom 1
!
translation-rule 1
 Rule 1 ^.% 1
```

```
!
interface Ethernet0
 ip address 172.19.140.96 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 squelch reduced
!
interface Serial1:23
 no ip address
 no keepalive
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.140.1
ip route 223.255.254.254 255.255.255.255 1.8.0.1
no ip http server
!
snmp-server community public RW
snmp-server packetsize 4096
!
call rsvp-sync
!
voice-port 0:1
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 650 voip
 destination-pattern 650.......
 session target ipv4:1.8.50.14
!
dial-peer voice 100 pots
 application debit-card
 incoming called-number 650233....
 direct-inward-dial
 supplementary-service pass-through
 port 0:1
!
dial-peer voice 1001 voip
 incoming called-number 650233....
!
dial-peer voice 12345602 voip
 supplementary-service pass-through
!
dial-peer hunt 6
!
line con 0
 exec-timeout 0 0
 logging synchronous level all
line aux 0
line vty 0 4
 exec-timeout 60 0
 password lab
 login
!
end
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

References Mentioned in This Chapter

- *Cisco IOS IP and IP Routing Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulvoip1.htm
- *Cisco IOS Voice, Video, and Fax Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/index.htm
- Tcl scripts at http://www.cisco.com/cgi-bin/tablebuild.pl/tclware

Implementing T1 CAS

This chapter describes how to implement the T1 Channel-Associated Signaling (CAS) for VoIP feature. This feature adds support for T1 CAS and E1 R2 signaling with the voice feature card (VFC).

The T1 CAS interface is used for connection to both a private PBX and the PSTN. This feature is required by North American enterprise customers and service providers. For most enterprise customers, T1 CAS is the only type of line they use from the PSTN; E&M may be the only option for connecting to their PBX.

Feature History for T1 CAS for VoIP

Release	Modification
12.1(5)XM	This feature was introduced on the Cisco AS5800.
12.2(2)XB1	This feature was implemented on the Cisco AS5850.
12.2(11)T	This feature was integrated into this release.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 231.

Contents

Prerequisites for Configuring T1 CAS

- Perform the prerequisites that are listed in the "Prerequisites for Configuring ISDN Voice Interfaces" section on page 3.

Restrictions for Configuring T1 CAS

Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4. In addition, the following applies.

Internet service providers can provide switched 56-kbps access to their customers with this feature. The subset of T1 CAS (robbed-bit) supported features is as follows:

- Supervisory: line side
  - fxs-ground-start
  - fxs-loop-start
  - sas-ground-start
  - sas-loop-start
  - Modified R1
- Supervisory: trunk side
  - e&m-fgb
  - e&m-fgd

    Note e&m-fgd can receive calling-party number (ANI) and send called-party number (dialed-number identification service or DNIS) but cannot send ANI.

  - e&m immediate start
  - fgd-eana

    Note fgd-eana can send both ANI and DNIS but cannot receive ANI.

- Informational: line side
  - DTMF
- Informational: trunk side
  - DTMF
  - MF

Information About T1 CAS for VoIP

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

To implement this feature, you should understand the following concepts:

CAS Basics

CAS is the transmission of signaling information within the voice channel. In addition to receiving and placing calls, CAS also processes the receipt of DNIS and ANI information, which is used to support authentication and other functions.

Various types of CAS are available in the T1 world. The most common forms are loop-start, ground-start, Equal Access North American (EANA), and E&M.

The biggest disadvantage of CAS is its use of user bandwidth to perform signaling functions. CAS is often referred to as robbed-bit-signaling because user bandwidth is "robbed" by the network for other purposes.

Service-provider application for T1 CAS includes connectivity to the public network using T1 CAS from the Cisco router to the end-office switch. In this configuration, the router captures dialed-number or called-party-number information and passes it to the upper-level applications for IVR script selection, modem pooling, and other applications. Service providers also require access to ANI for user identification, billing account number, and, in the future, more complicated call routing.

Service providers who implement VoIP include traditional voice carriers, new voice and data carriers, and existing internet service providers. Some of these service providers might use subscriber-side lines for VoIP connectivity to the PSTN; others use tandem-type service-provider connections.

New CAS functionality for VoIP includes all CAS and E1/R2 signaling already supported for supported Cisco platforms in data applications, with the addition of dialed-number and calling-party-number capture whenever available.

E&M and Ground Start/FXS Protocols

This feature supports the following T1 CAS systems for VoIP applications:

- E&M—E&M robbed-bit signaling is typically used for trunks. It is generally the only way that a CO switch can provide two-way dialing with direct inward dialing. In all E&M protocols, off-hook is indicated by A=B=1 and on-hook is indicated by A=B=0. For dial-pulse dialing, the A and B bits are pulsed to indicate the addressing digits. There are several further important subclasses of E&M robbed-bit signaling:

  - E&M Wink Start—Feature Group B

    In the original Wink Start protocol, the terminating side responds to an off-hook from the originating side with a short wink (transition from on-hook to off-hook and back again). This wink indicates that the terminating side is ready to receive addressing digits. After receiving digits, the terminating side goes off-hook for the duration of the call. The originating side maintains off-hook for the duration of the call.

  - E&M Wink Start—Feature Group D

    In Feature Group D Wink Start with Wink Acknowledge Protocol, the terminating side responds to an off-hook from the originating side with a short wink just as in the original Wink Start. After receiving digits, the terminating side provides another wink (called an acknowledgment wink) to indicate that the terminating side has received the digits. The terminating side goes off-hook to indicate connection when the ultimate called endpoint has answered. The originating side maintains off-hook for the duration of the call.

  - E&M Immediate Start

    In the Immediate Start Protocol, the originating side does not wait for a wink before sending addressing digits. After receiving digits, the terminating side goes off-hook for the duration of the call. The originating side maintains off-hook for the duration of the call.

- Ground Start/FXS—Ground Start Signaling was developed to help resolve glare when two sides of the connection tried to go off-hook at the same time. This is a problem with loop start because the only way to indicate an incoming call from the network to the customer premises equipment (CPE) using loop start was to ring the phone. The six-second ring cycle left a lot of time for glare to occur. Ground Start Signaling eliminates this problem by providing an immediate-seizure indication from the network to the CPE. This indication tells the CPE that a particular channel has an incoming call on it. Ground Start Signaling differs from E&M because the A and B bits do not track each other (that is, A is not necessarily equal to B). When the CO delivers a call, it seizes a channel (goes off-hook) by setting A to 0. The CO equipment also simulates ringing by toggling the B bit. The terminating equipment goes off-hook when it is ready to answer the call. Digits are usually not delivered for incoming calls.

How to Configure T1 CAS for VoIP

This section contains the following procedures:

- Configuring T1 CAS for Use with VoIP, page 226 (required)
- Verifying T1 CAS Configuration, page 229 (optional)

Configuring T1 CAS for Use with VoIP

To configure T1 CAS for use with VoIP, perform the following steps.

Note The following shows how to configure the voice ports as ds0-*group* for channelized T1 lines.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **controller**
4. **framing**
5. **linecode**
6. **ds0-group timeslots type**
7. Repeat as needed.
8. **dial-peer voice** *tag type* **(destination-pattern, port, prefix)**
9. **dial-peer voice** *tag type* **(incoming called-number, destination-pattern, direct-inward-dial, port, prefix)**
10. Repeat as needed.
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller t1 1/0/0`	Enters controller configuration mode for the specified slot/port. The controller ports are labeled RI and E1/PRI cards.
Step 4	**framing** *type* **Example:** `Router(config-control)# framing esf`	Enters your telco framing type.
Step 5	**linecode** *type* **Example:** `Router(config-control)# linecode b8zs`	Enters your telco line code type.

	Command or Action	Purpose
Step 6	**ds0-group** *group-number* **timeslots** *range* **type** *type* {**dtmf** | **mf**} {**ani** | **dnis** | **ani-dnis**} **Example:** `Router(config-control)# ds0-group 1 timeslots 1-24 type e&m-fgb`	Configures all channels for E&M, FXS, and SAS analog signaling. T1 range: 1 to 24. E1 range: 1to 31. Some of the valid signaling types and keyword combinations are as follows: • Type: e&m-fgb – dtmf and dnis – mf and dnis • Type: e&m-fgd – dtmf and dnis – mf and ani-dnis or dnis • Type: fgd-eana – mf and ani-dnis **Note** Use the same type of signaling that your central office uses. For E1 using the Anadigicom converter, use e&m-fgb. See restrictions applicable to e&m-fgb and e&m-fgd in the "Restrictions for Configuring T1 CAS" section on page 224.
Step 7	Repeat steps 4 to 6 for each additional controller (there are 12). Be sure to increment the controller number and ds0-group number.	—

Step 8	**dial-peer voice** *tag type*
	destination-pattern
	port
	prefix
	
	Example:
	`Router(config-control)# dial-peer voice 3070 pots`
	`destination-pattern 30...`
	`port 1/0/0:D`
	`prefix 30`
		Enters dial-peer configuration mode and configures a POTS peer destination pattern.

Step 9	**dial-peer voice** *tag type*
	incoming called-number
	destination-pattern
	direct-inward-dial
	port
	prefix
	
	Example:
	`Router(config-control)# dial-peer voice 21 pots`
	`incoming called-number 11...`
	`destination-pattern 40...`
	`direct-inward-dial`
	`port 12/0:2:0`
	`prefix 21`
		Specifies, for each POTS peer, the following: incoming called number, destination pattern, and direct inward dial.

	Command or Action	Purpose
Step 10	Repeat steps 8 and 9 for each dial peer.	—
Step 11	**exit** **Example:** `Router(config-control)# exit`	Exits the current mode. **Note** The message "%SYS-5-CONFIG_I: Configured from console by console" is normal and does not indicate an error.

Verifying T1 CAS Configuration

To verify T1 CAS configuration, perform the following steps (listed alphabetically).

SUMMARY STEPS

1. **show controllers**
2. **show isdn status**
3. **show running-config**

DETAILED STEPS

Step 1 **show controllers {t1 | e1}** *dial-shelf/slot/port*

Use this command to display the controller and alarm status for the specified dial shelf/slot/port. Configuration is successful if the controller reports being up and no error are reported.

```
Router# show controllers t1 1/0/0

T1 1/0/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (180 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Step 2 **show isdn status**

Use this command to display the status of all ISDN interfaces, including active layers, timer information, and switch-type settings.

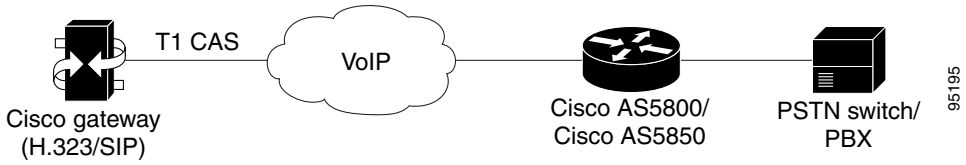
Step 3 **show running-config**

Use this command to display the basic router configuration.

Configuration Example for T1 CAS for VoIP

The sample configuration is only intended as an example of how to use the commands to configure T1 CAS. It is not an example of a complete configuration for setting up the entire signaling for a telco network.

Figure 15 T1 CAS for VoIP: Network Topology




```
Router# show running-config

version 12.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname travis-nas-01
!
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHENT none
aaa authorization exec default local if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default local if-authenticated
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default start-stop group tacacs+
aaa accounting exec NO_ACCOUNT none
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting commands 15 NO_ACCOUNT none
enable secret 5 $1$LsoW$K/qBH9Ih2WstUxvazDgmY/
!
username admin privilege 15 password 7 06455E365E471D1C17
username gmcmilla password 7 071824404D06140044
username krist privilege 15 password 7 0832454D01181118
!
call rsvp-sync
shelf-id 0 router-shelf
shelf-id 1 dial-shelf
!
resource-pool disable
!
modem-pool Default
 pool-range 1/2/0-1/2/143,1/3/0-1/3/143
!
modem-pool accounts
!
modem-pool accounts1
!
modem-pool accounts2
!
clock timezone CST -6
clock summer-time CST recurring
!
ip subnet-zero
ip domain-name cisco.com
```

```
ip name-server 172.22.53.210
ip name-server 171.69.2.133
ip name-server 171.69.2.132
ip name-server 171.69.11.48
!
isdn switch-type primary-5ess
!
controller T1 1/0/0
 framing esf
 linecode b8zs
ds0-group 1 timeslots 1-24 type e&m-fgb
!
controller T1 1/0/1
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-fgb
!
controller T1 1/0/2
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-fgb
!
controller T1 1/0/3
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
controller T1 1/0/4
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

Implementing FCCS (NEC Fusion)

This chapter describes how to implement Fusion Call-Control Signaling (FCCS), also known as NEC Fusion. FCCS allows a voice network to seamlessly integrate into an IP network, making it possible to add voice-networking capabilities to a LAN or WAN without major network restructuring.

The NEC Fusion Strategic Alliance Program facilitates development of integrated solutions, complementary to both NEC and other technology businesses, that provide telephony solutions for mutual customers.

FCCS, developed under this program, deploys a new transmission signaling protocol that is compatible with IP networks and Cisco routers and switches. It allows individual nodes anywhere within a network to operate as if they were part of a single integrated PBX system. Database storage, share, and access routines allow real-time access from any node to any other, allowing individual nodes to learn about the entire network configuration. This capability allows network-wide feature, functional, operational, and administration transparency.

Feature History for FCCS

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about related Cisco IOS voice features, see the following:

- "Overview of ISDN Voice Interfaces" on page 3
- Entire Cisco IOS Voice Configuration Library—including library preface and glossary, other feature documents, and troubleshooting documentation—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.

For a list of references cited in this chapter, see the "Additional References" section on page 239.

Contents

Prerequisites for Implementing FCCS

- Perform the prerequisites that are listed in the "Prerequisites for Configuring ISDN Voice Interfaces" section on page 3.

Restrictions for Implementing FCCS

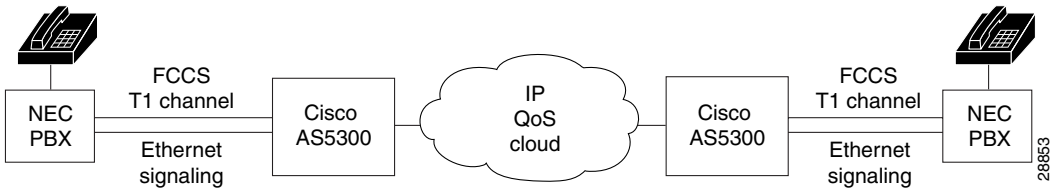
Restrictions are described in the Restrictions for Configuring ISDN Voice Interfaces, page 4.

Information About FCCS

Note General information about ISDN voice interfaces is presented in the "Information About ISDN Voice Interfaces" section on page 4.

If you have an NEC PBX in your network and also run FCCS, you must configure your access servers appropriately for QSIG and then for FCCS (NEC Fusion). Figure 16 shows an example of a Cisco AS5300 QSIG signaling configuration using an NEC PBX.

Figure 16 QSIG Signaling Configuration with NEC PBX



How to Configure FCCS

This section contains the following procedures:

Configuring VoIP QSIG

To configure VoIP QSIG, perform the following steps.

Note You can configure a switch type at either global level or interface level. For example, if you have a QSIG connection on one line and on the PRI port, you can use the **isdn-switch-type** command to configure the ISDN switch type in any of the following combinations:

- At the global level to support QSIGX, PRI 5ess, or another switch type such as VN3
- At the interface level to set a particular interface to support QSIG, to set a particular interface to a PRI setting such as 5ess, or to set one particular interface to a PRI setting and another interface to support QSIG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isdn switch-type primary-qsig**
4. **controller**
5. **pri-group**
6. **exit**
7. **interface**
8. **isdn switch-type primary-qsig**
9. **isdn protocol-emulate**
10. **isdn overlap-receiving**
11. **isdn incoming-voice modem**
12. **isdn network-failure-cause**
13. **isdn bchan-number-order**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**isdn switch-type primary-qsig** **Example:** `Router(config)# isdn switch-type primary-qsig`	(Optional) Globally configures the ISDN switch type to support QSIG signaling. **Note** Depending on your configuration, you can configure the ISDN switch type by using this command either in global configuration mode or interface configuration mode (see Step 8). If the PBX in your configuration is an NEC PBX and you use Fusion Call Control Signaling (FCCS), see the "Configuring FCCS" section on page 238.
Step 4	**controller** {**t1** | **e1**} *controller-number* **Example:** `Router(config)# controller t1 3`	Enters controller configuration mode for the specified controller.
Step 5	**pri-group** [**timeslot** *range*] **Example:** `Router(config-controller)# pri-group timeslot 1-23`	Configures the PRI group for either T1 or E1 to carry voice traffic. T1 time slots are 1 to 23. E1 time slots are 1 to 31. You can configure the PRI group to include either all available time slots or just a select group. For example, if only time slots 1 to 10 are in the PRI group, specify **timeslot 1-10**. If the PRI group includes all channels available for T1, specify **timeslot 1-23** command. If the PRI group includes all channels available for E1, specify **timeslot 1-31**.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 7	**interface serial 1:***channel-number* **Example:** `Router(config)# interface serial 1:23`	Enters interface configuration mode for the ISDN PRI interface. T1 channel number is 23. E1 channel number is 15.
Step 8	**isdn switch-type primary-qsig** **Example:** `Router(config-if)# isdn switch-type primary-qsig`	(Optional) Configures the ISDN switch type to support QSIG signaling for the specified interface. Use this command if you did not configure the ISDN switch type for QSIG support globally in Step 1. The same conditions that apply to this command in global configuration mode also apply to this command in interface configuration mode. **Note** For the selected interface, this command in interface configuration mode overrides the same command in global configuration mode.

	Command or Action	Purpose
Step 9	**isdn protocol-emulate** {**user** | **network**} **Example:** `Router(config-if)# isdn protocol-emulate {user | network}`	Configures the ISDN interface to serve as either the primary QSIG slave or the primary QSIG master. Keywords are as follows: • **user**—Slave • **network**—Master If the private integrated services network exchange (PINX) is the primary QSIG master, configure the access server as the primary QSIG slave. If the PINX is the primary QSIG slave, configure it as the primary QSIG master.
Step 10	**isdn overlap-receiving** [**T302** *value*] **Example:** `Router(config-if)# isdn overlap-receiving T302 500`	(Optional) Activates overlap signaling to send to the destination PBX using timer T302. The keyword are argument are as follows: • **T302** *value*—Value of timer T302, in ms.
Step 11	**isdn incoming-voice modem** **Example:** `Router(config-if)# isdn incoming-voice modem`	Routes incoming voice calls to the modem and treats them as analog data.
Step 12	**isdn network-failure-cause** [*value*] **Example:** `Router(config-if)# isdn network-failure-cause 5`	(Optional) Specifies the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures. The argument is as follows: • *value*—Cause code, from 1 to 127. All cause codes except Normal Call Clearing (16), User Busy (17), No User Responding (18), and No Answer from User (19) are changed to the specified cause code.
Step 13	**isdn bchan-number-order** {**ascending** | **descending**} **Example:** `Router(config-if)# isdn bchan-number-order ascending`	(Optional) Configures the ISDN PRI interface to make the outgoing call selection in ascending or descending order. Keywords are as follows: • **ascending**—Ascending order. • **descending**—Descending order. This is the default. For descending order, the first call from the access server uses (T1) channel 23 or (E1) channel 31. The second call then uses (T1) channel 22 or (E1) channel 30, and so on, in descending order. For ascending order, if the PRI group starts with 1, the first call uses channel 1, the second call uses channel 2, and so on, in ascending order. If the PRI group starts with a different time slot, the ascending order starts with the lowest time slot.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Configuring FCCS

To configure FCCS, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller**
4. **pri-group nec-fusion**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller t1** *controller-number* **Example:** `Router(config)# controller t1 5`	Enters controller configuration mode for the specified controller. **Note** NEC Fusion does not support fractional T1/E1; all 24 channels must be available or the configuration request fails.
Step 4	**pri-group nec-fusion** {*pbx-ip-address* | *pbx-ip-host-name*} **pbx-port** *number* **Example:** `Router(config-controller)# pri-group nec-fusion 172.16.0.0 pbx-port 55000`	Configures the controller to communicate with an NEC PBX using NEC Fusion. The argument is as follows: • *number*—PBX port number. If the specified value is already in use, the next greater value is used.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Verifying FCCS

To verify FCCS functionality, perform the following step.

SUMMARY STEPS

1. **show isdn status**

DETAILED STEPS

Step 1 **show isdn status**

Use this command to display the status of all ISDN interfaces or a specific ISDN interface.

```
Router# show isdn status

Global ISDN Switchtype = primary-qsig
ISDN Serial1:23 interface
        dsl 0, interface ISDN Switchtype = primary-qsig
         **** Slave side configuration ****
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask: 0x7FFFFF
```

Additional References

General ISDN References

- "ISDN Features Roadmap" on page 1—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, ISDN features for that release
- "Overview of ISDN Voice Interfaces" on page 3—Describes relevant underlying technology; lists related documents, standards, MIBs, and RFCs; and describes how to obtain technical assistance
- "Additional References" section on page 64—Lists additional ISDN references

Implementing the Digital J1 VIC

This chapter describes how to implement the Digital J1 Voice Interface Card (VIC) feature. The digital J1 VIC provides the proper interface for directly connecting Cisco multiservice access routers to PBXs throughout Japan that use a J1 (2.048-Mbps time-division-multiplexed [TDM]) interface.

Feature History for Digital J1 Voice Interface Card

Release	Modification
12.2(8)T	This feature was introduced on the Cisco 2600 series and Cisco 3600 series.

Contents

Prerequisites for Configuring the Digital J1 VIC

- Ensure that you have Cisco IOS Release 12.2(8)T or later.

Restrictions for Configuring the Digital J1 VIC

- Voice-only applications are supported.
- Separate clock output is not supported.
- Alarm-relay output is not supported.
- Per-channel loopback is not supported.
- Voice ports on the J1 interface cannot be configured using network-management software. They must be configured manually.

Information About the Digital J1 VIC

The digital J1 VIC provides the proper interface for directly connecting Cisco multiservice access routers to PBXs throughout Japan that use a J1 (2.048-Mbps TDM) interface.

It provides the software and hardware features required to connect to over 80 percent of the PBXs within Japan that use digital interfaces. This new J1 voice interface card (VIC) provides a TTC JJ-20.11 compliant interface between high-density voice network modules (NM-HDV) and a Japanese PBX.

The card supports 30 voice channels per port. It provides a single-port line interface in a VIC form factor. It is specifically designed to conform to the TTC JJ-20.10-12 standards that define the interface between a PBX and a time-division multiplexer.

Figure 17 shows the earlier solution offered to customers in Japan. A J1/T1 adapter box installed between the PBX and router provides the translation between J1 using coded mark inversion (CMI) line coding at a bit rate of 2.048 Mbps and a T1 line using either alternate mark inversion (AMI) or B8ZS line coding at a bit rate of 1.544 Mbps. Note that, with this solution, only 24 channels are supported instead of the full 30 channels of the J1 interface.

Figure 17 Solution Without J1 VIC

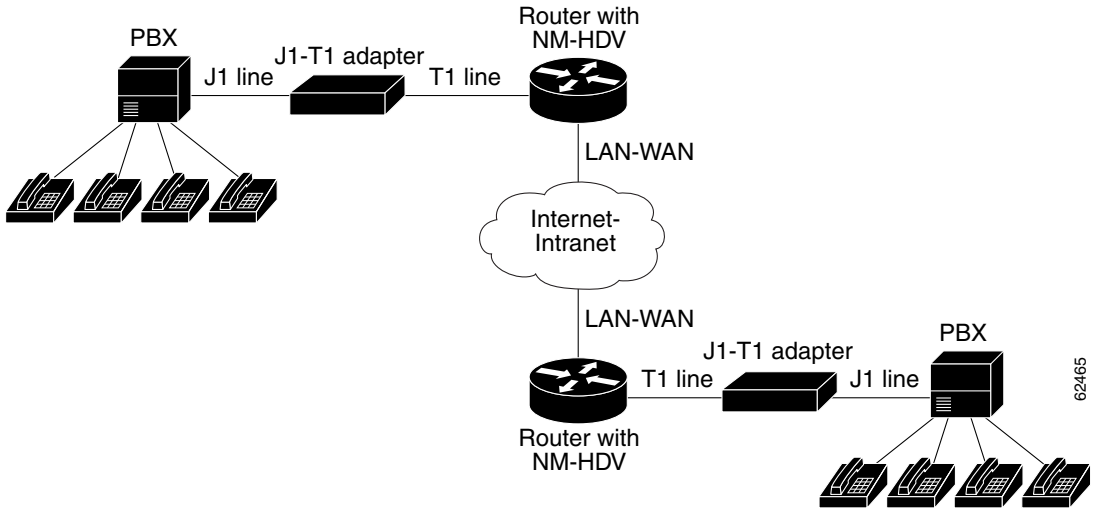
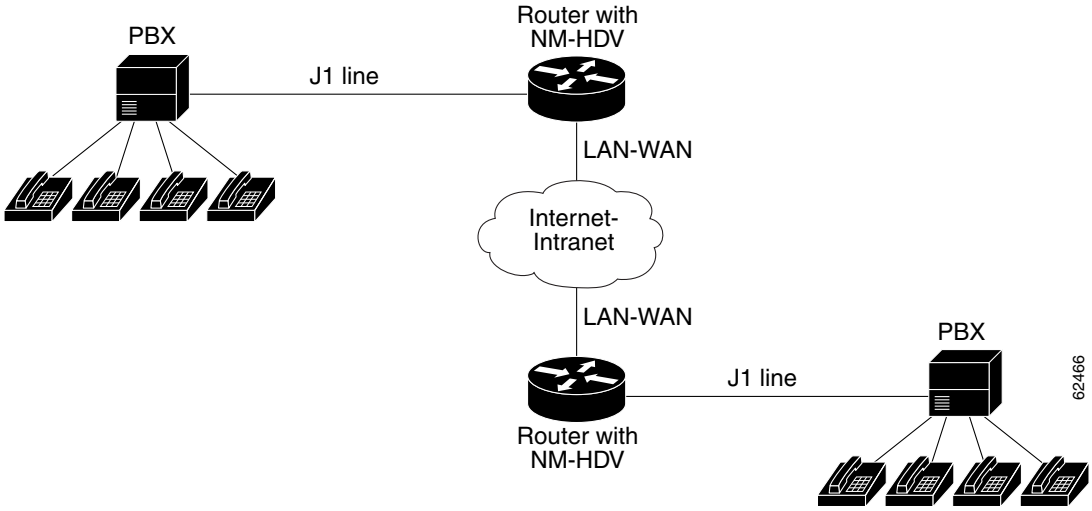


Figure 18 shows the solution using the digital J1 VIC. The interface is now between J1 and the VIC's TDM access (TDMA) bus. Note that now all 30 channels of the J1 interface are supported.

Figure 18 Solution with J1 VIC



Feature benefits include the following:

- Supports Media Gateway Control Protocol (MGCP), H.248, H.323 (versions 1, 2, and 3), Session Initiation Protocol (SIP), and Cisco CallManager (with Cisco IP phones) in association with VoIP, VoFR, and VoATM
- Provides Alarm Indication Signal (AIS) alarm signaling per TTC JJ-20.11
- Delivers the same performance as the existing 30-channel E1 NM-HDV
- Allows enabling and disabling of individual DS0s or channels

How to Configure the Digital J1 VIC

This section contains the following procedures:

Note For related information on VIC installation, see *Installing and Configuring 1-Port J1 Voice Interface Cards*.

Configuring the J1 VIC

To configure the digital J1 VIC, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller j1**
4. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller j1** *slot/port* **Example:** `Router(config)# controller j1 1/0`	Configures the J1 controller in the specified slot and port.
Step 4	**exit** **Example:** `Router(config-control)# exit`	Exits the current mode.

Configuring CAS

To configure the DS0 groups on the digital J1 VIC for voice applications, perform the following steps.

Note The J1 controller supports the E&M wink start and E&M immediate channel-associated signaling (CAS) protocols for the voice ports. The following parameters have default values for the J1 interface:

- Companding type: mu-law
- CP tone: JP

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **controller j1**
4. **ds0-group**
5. **exit**
6. Repeat as needed

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller j1** *slot/port* **Example:** `Router(config)# controller j1 1/0`	Enters controller configuration mode for the J1 controller in the specified slot and port.
Step 4	**ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *signaling-type* **Example:** `Router(config-controller)# ds0-group 1 timeslots 1-15,17-31 type e&m-wink-start`	Configures channelized J1 time slots for use by compressed voice calls and the signaling method for connecting to the PBX. The keywords and arguments are as follows: • *ds0-group-no*—DS0 group number. • **timeslots** *timeslot-list*—DS0 timeslot. Range: 1 to 31. Timeslot 16 is reserved for signaling. • **type** *signaling-type***—**Signaling type to be applied to the selected group: – **e&m-delay-dial**—Originating endpoint sends an off-hook signal and then and waits for an off-hook signal followed by an on-hook signal from the destination. – **e&m-immediate-start**—No specific off-hook and on-hook signaling. – **e&m-wink-start—**Originating endpoint sends an off-hook signal and waits for a wink signal from the destination. – **none**—Null signaling for external call control.

	Command	Purpose
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 6	Repeat if your router has more than one J1 controller to configure.	

Configuring the Clock Source

To configure the clock source for a digital J1 VIC, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller j1**
4. **clock source**
5. **exit**
6. Repeat as needed

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller j1** *slot/port* **Example:** `Router(config)# controller j1 1/0`	Enters controller configuration mode for the J1 controller in the specified slot and port.
Step 4	**clock source** {**line** | **internal**} **Example:** `Router(config-controller)# clock source line`	Specifies the clock source. Keywords are as follows: • **line**—Controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator. • **internal**—Controller synchronizes itself to the internal (system) clock. Default: **line**.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 6	Repeat if your router has more than one J1 controller to configure.	

Configuring Loopback

To configure loopback for testing a digital J1 VIC, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller j1**
4. **loopback**
5. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller j1** *slot/port* **Example:** `Router(config)# controller j1 1/0`	Enters controller configuration mode for the J1 controller in the specified slot and port.
Step 4	**loopback** {**local** | **line** | **isolation**} **Example:** `Router(config-controller)# loopback isolation`	Sets the loopback method for testing the J1 interface. Keywords are as follows: • **local**—Local loopback mode • **line**—External loopback mode at the line level • **isolation**—Both local and line loopback mode
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configuring T-CCS for a Clear-Channel Codec

To configure transparent common-channel signaling (T-CCS), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller j1**
4. **ds0-group**
5. **no shutdown**
6. **exit**
7. **dial-peer voice**
8. **destination-pattern**
9. **port**
10. **exit**
11. **dial-peer voice**
12. **codec clear-channel**
13. **vad**
14. **destination-pattern**
15. **session target**
16. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller j1** *slot/port* **Example:** `Router(config)# controller j1 1/0`	Enters controller configuration mode for the J1 controller in the specified slot and port.

	Command	Purpose
Step 4	**ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *signaling-type* **Example:** `Router(config-controller)# ds0-group 1 timeslots 1-15,17-31 type e&m-wink-start`	Configures channelized J1 time slots for use by compressed voice calls and the signaling method that the router uses to connect to the PBX. The keywords and arguments are as described earlier.
Step 5	**no shutdown** **Example:** `Router(config-controller)# no shutdown`	Activates the controller.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 7	**dial-peer voice** *number* **pots** **Example:** `Router(config)# dial-peer voice 20 pots`	Enters dial-peer configuration mode for the specified POTS dial peer.
Step 8	**destination-pattern** *string* [**T**] **Example:** `Router(config-dialpeer)# destination-pattern 3050 T`	Configures the dial peer's destination pattern so that the system can reconcile dialed digits with a telephone number. The keyword and argument are as follows: • *string*—Series of digits that specify the E.164 or private-dialing-plan phone number. Valid entries: digits 0 to 9 and letters A to D. The plus symbol (+) is not valid. You can enter the following special characters: – Star character (*) that appears on standard touch-tone dial pads—Can be in any dial string, but not as a leading character (for example, *650). – Period (.)—Acts as a wildcard character. – Comma (,)—In prefixes, inserts a one-second pause. • **T**—When included at the end of the destination pattern, causes the system to collect dialed digits as they are entered until the interdigit timer expires (default: 10 seconds) or the user dials the termination of end-of-dialing key (default: #). **Note** The timer character must be a capital T.
Step 9	**port** *slot/port:ds0-group-no* **Example:** `Router(config-dialpeer)# port 1/0:1`	Associates the dial peer with a specific logical interface. Arguments are as follows: • *slot*— Router location where the voice module is installed. Range: 0 to 3. • *port*—Voice interface card location. Range: 0 to 1. • *ds0-group-no*—DS0 group number. Each defined DS0 group number is represented on a separate voice port, allowing you to define individual DS0s.

	Command	Purpose
Step 10	**exit** **Example:** `Router(config-dialpeer)# exit`	Exits the current mode.
Step 11	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 20 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 12	**codec clear-channel** **Example:** `Router(config-dialpeer)# codec clear-channel`	Specifies use of the clear-channel codec.
Step 13	**vad** **Example:** `Router(config-dialpeer)# vad`	(Optional; enabled by default) Activates voice activity detection (VAD), which allows the system to reduce unnecessary voice transmissions caused by unfiltered background noise.
Step 14	**destination-pattern** *string* [**T**] **Example:** `Router(config-dialpeer)# destination-pattern 3050 T`	Configures the dial peer's destination pattern so that the system can reconcile dialed digits with a telephone number. The keyword are argument are as described above.

	Command	Purpose
Step 15	**session target** {**ipv4:***destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname*} **Example:** `Router(config-dialpeer)# session target {ipv4:10.168.1.1 serverA.mycompany.com}`	Configures the IP session target for the dial peer. Keywords and arguments are as follows: • **ipv4:***destination-address* —IP address of the dial peer to receive calls. • **dns:***hostname*—Domain-name server that resolves the name of the IP address. You can use wildcards by using source, destination, and dialed information in the hostname. Use one of the following macros with this keyword when defining the session target for VoIP peers: – **s.**—Source destination pattern is used as part of the domain name. – **d.**—Destination number is used as part of the domain name. – **e.**—Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. – **•u.**—Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name.
Step 16	**exit** **Example:** `Router(config-dialpeer)# exit`	Exits the current mode.

Verifying Digital J1 VIC Configuration

To verify that the digital J1 VIC is configured correctly, use the **show running-config** command as shown in the"Configuration Examples for the Digital J1 VIC" section on page 254.

Monitoring and Maintaining the Digital J1 VIC

To monitor and maintain the J1 VIC, use the following commands:

- **show controllers j1** *slot/port*—Displays statistics for the J1 link.
- **show dial-peer voice**—Displays configuration information for dial peers.

Troubleshooting Tips

Three digital loopback modes are possible for diagnostics and fault isolation:

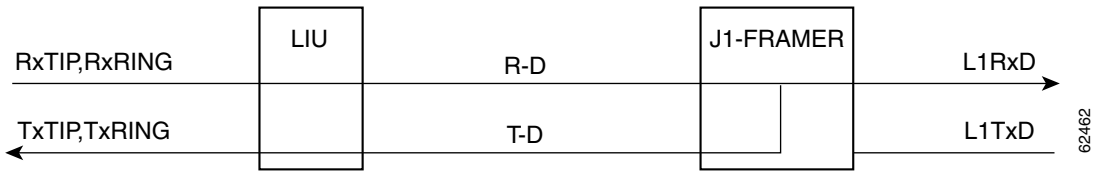
- Line loopback loops the received signal (R-D) from the PBX to the transmit going back to the PBX.
- Local loopback loops the transmitted signal (T-D) from the host to the receive going back to the host.
- Isolation loopback routes PBX and TDM generated traffic back to their respective sources.

Note In the following figures, Tx=transmit interface and Rx=receive interface. Tip / Ring leads carry audio between the signaling unit and the trunking circuit.

Line Loopback

To place the controller into line loopback, use the **loopback line** command (Figure 19). Line loopback loops the receiver inputs to the transmitter outputs. The receive path is not affected by the activation of this loopback.

Figure 19 Line Loopback

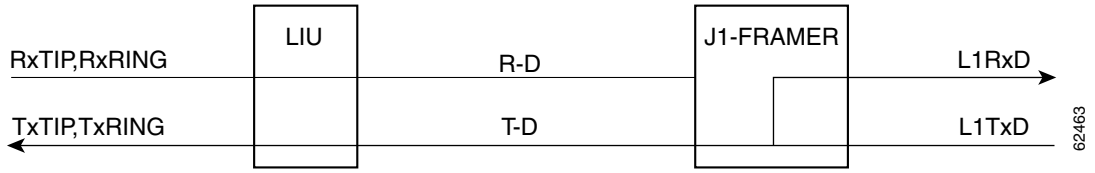


Local Loopback

To place the controller into local loopback, use the **loopback local** command (Figure 20). To turn off loopback, use the **no** form of the command. Local loopback loops the transmit line encoder outputs to the receive line encoder inputs. The transmit path is not affected by the activation of this loopback.

Note Use this command only for testing purposes.

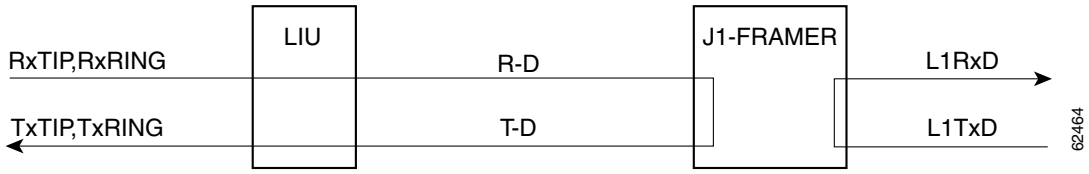
Figure 20 Local Loopback



Isolation Loopback

To place the controller into line loopback, use the **loopback isolation** command (Figure 21). Both line and local loopback are turned on.

Figure 21 Isolation Loopback



Configuration Examples for the Digital J1 VIC

The following displays the screen output using the **show running-config** command. Then it is broken down into specific examples:

- Controller (J1): Example, page 256
- Channel-Associated Signaling: Example, page 256
- Clock Source: Example, page 256
- Loopback: Example, page 257
- Transparent Common-Channel Signaling for a Clear-Channel Codec: Example, page 257

```
Router# show running-config

Building configuration...

Current configuration :2023 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname kmm-3660-1
!
boot system tftp /tftpboot/kmenon/c3660-is-mz 223.255.254.254
enable password lab
!
voice-card 1
!
voice-card 3
!
voice-card 4
!
ip subnet-zero
!
!
voice service pots
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller J1 1/0
 clock source line
!
controller E1 3/0
!
controller E1 3/1
```

```
!
controller T1 4/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 24
!
controller T1 4/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 24
!
!
interface Multilink1
 ip address 30.30.30.1 255.255.255.0
 keepalive 1
 no cdp enable
 ppp multilink
 no ppp multilink fragmentation
 multilink-group 1
!
interface FastEthernet0/0
 ip address 1.7.29.1 255.255.0.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.8.0.1 255.255.0.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial4/0:0
 no ip address
 encapsulation ppp
 no fair-queue
 no cdp enable
 ppp multilink
 multilink-group 1
!
interface Serial4/1:0
 no ip address
 encapsulation ppp
 no fair-queue
 no cdp enable
 ppp multilink
 multilink-group 1
!
ip default-gateway 1.7.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 1.9.0.1 255.255.255.255 30.30.30.2
ip route 223.255.254.254 255.255.255.255 1.7.0.1
no ip http server
ip pim bidir-enable
!
!
snmp-server engineID local 00000009020000044D0EF520
snmp-server packetsize 4096
!
call rsvp-sync
!
no mgcp timer receive-rtcp
!
```

```
mgcp profile default
!
dial-peer cor custom
!
!
dial-peer voice 1 pots
 destination-pattern 88
!
dial-peer voice 20 voip
 destination-pattern 3050
 session target ipv4:10.8.0.2
 codec clear-channel
!
dial-peer voice 77 pots
 destination-pattern 77
!
dial-peer voice 100 voip
 incoming called-number 100
 destination-pattern 100
 session target ipv4:10.8.0.2
 no vad
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

Controller (J1): Example

The following example shows the Cisco IOS interface card in slot 4, port 0 of a Cisco 3660 configured as a J1 controller:

```
controller J1 4/0
```

Channel-Associated Signaling: Example

The following example shows the DS0 groups on the J1 controller.

```
controller J1 4/0
 clock source line
 ds0-group 1 timeslots 1-15,17-31 type e&m-wink-start
```

Clock Source: Example

The following example shows the J1 controller clock source is configured to line, where the controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator.

```
controller J1 3/0
 clock source line
```

Loopback: Example

The following example shows the loopback method for testing the J1 controller is set at the line level.

```
controller J1 3/0
 clock source line
 loopback line
```

Transparent Common-Channel Signaling for a Clear-Channel Codec: Example

The following example shows the codec option set to clear-channel.

```
dial-peer voice 20 voip
 destination-pattern 3050
 session target ipv4:10.8.0.2
 codec clear-channel
```

P

Q

R

S

T

V