

## **Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide**

### **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

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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.

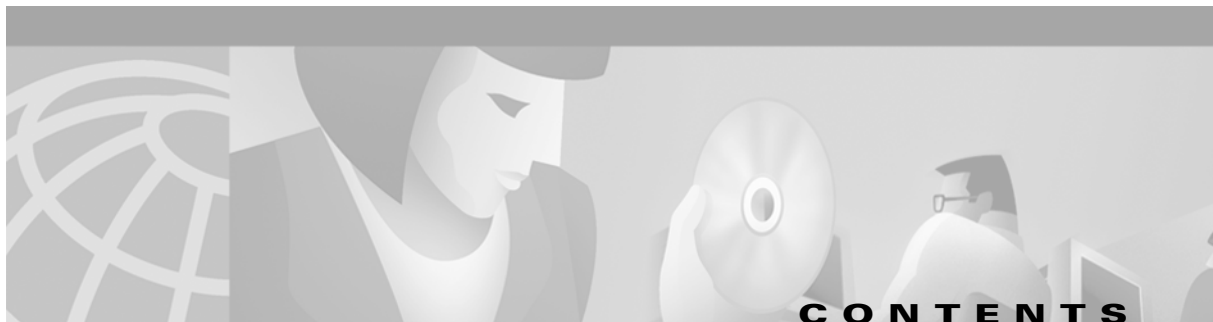
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0110R)

*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*  
Copyright ©2000-2001, Cisco Systems, Inc.  
All rights reserved.



## **Preface**    **vii**

- Document Objectives    **vii**
- Who Should Read This Guide    **vii**
- Organization    **viii**
- Document Conventions    **viii**
- Cisco Media Gateway Documentation Suite    **ix**
- Documentation Road Map    **x**
- Obtaining Documentation    **xi**
  - World Wide Web    **xi**
  - Documentation CD-ROM    **xi**
  - Ordering Documentation    **xi**
  - Documentation Feedback    **xi**
- Obtaining Technical Assistance    **xii**
  - Cisco.com    **xii**
  - Technical Assistance Center    **xii**
    - Contacting TAC by Using the Cisco TAC Website    **xii**
    - Contacting TAC by Telephone    **xiii**

---

## **CHAPTER 1**

### **Introduction to Media Gateways**    **1-1**

- Media Gateway Architecture    **1-2**
- Media Gateway Components    **1-3**
- Media Gateways and Supported Solutions    **1-4**
  - Cisco AS5300 Universal Access Server    **1-4**
  - Cisco AS5350 Universal Gateway    **1-5**
  - Cisco AS5400 Universal Gateway    **1-5**
  - Cisco AS5800 Universal Access Server    **1-5**
  - Cisco AS5850 Universal Gateway    **1-5**

---

## **CHAPTER 2**

### **Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution**    **2-1**

- Determining Software and Hardware Requirements    **2-1**
- Installing Media Gateways    **2-1**
  - Installing the Cisco AS5300 Universal Access Server    **2-2**

- Installing the Cisco AS5350 Universal Gateway 2-2
- Installing the Cisco AS5400 Universal Gateway 2-2
- Installing the Cisco AS5800 Universal Access Server 2-2
- Installing the Cisco AS5850 Universal Gateway 2-3
- Configuring Media Gateways 2-3
  - Setting the ISDN Switch Type 2-4
  - Configuring the Cisco AS5300 and Cisco AS5850 for B-Channel Negotiation 2-4
  - Configuring Redundant Link Manager 2-4
    - Configuring RLM on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Classic-Split Mode Cisco AS5850 2-6
    - Configuring RLM on a Handover-Split Mode Cisco AS5850 2-7
    - Verifying RLM Configuration 2-11
  - Completing VoIP Configuration 2-12
  - Configuring Number Translation 2-14
  - Configuring the Digit Strip 2-14
  - Configuring Dial Peer Call Legs Using Digit Translation Rules 2-15
    - Sample Configuration and Output for Voice-over-IP 2-17
  - Verifying the Configuration 2-20
- Sample Output for the Cisco SS7 Interconnect for Voice Gateways Solution 2-22

**CHAPTER 3**

**Configuring Media Gateways for the SS7 Interconnect for Access Servers Solution 3-1**

- Determining Software and Hardware Requirements 3-1
- Installing Media Gateways 3-1
  - Installing the Cisco AS5300 Universal Access Server 3-2
  - Installing the Cisco AS5350 Universal Gateway 3-2
  - Installing the Cisco AS5400 Universal Gateway 3-2
  - Installing the Cisco AS5800 Universal Access Server 3-2
- Configuring Media Gateways 3-3
  - Preparing the Media Gateway for Configuration 3-3
  - Setting the ISDN Switch Type 3-3
  - Configuring Redundant Link Manager 3-4
    - Verifying RLM Configuration 3-5
  - Configuring Resource Pool Manager (RPM) 3-6
    - RPM Configuration Examples 3-9
  - Verifying the Configuration 3-11
- Sample Output for the Cisco SS7 Interconnect for Access Servers Solution 3-13
- Configuring Call Hairpinning on the Cisco AS5800 3-17
  - Call Switching Using Dial Peers 3-17
  - Using Class of Restrictions 3-17

- Call Hairpinning Configuration Tasks [3-18](#)
  - Configuring Global or Interface Trunk Groups [3-18](#)
  - Configuring Dial Peer Classes of Restrictions [3-19](#)
- Complete Dial Plan Setup for Hairpinning [3-20](#)

**CHAPTER 4****Upgrading Cisco Media Gateway Software [4-1](#)**

- Determining Your Cisco IOS Version [4-1](#)
- Determining Memory Requirements [4-1](#)
- Upgrading the Cisco AS5300 Universal Access Server [4-2](#)
  - Blocking Voice Gateway Circuits [4-2](#)
  - Loading a Cisco IOS Upgrade on the Cisco AS5300 [4-2](#)
  - Upgrading Cisco VCWare [4-4](#)
- Upgrading the Cisco AS5350 or Cisco AS5400 Universal Gateway [4-4](#)
- Upgrading the Cisco AS5800 Universal Access Server [4-6](#)
  - Backing Up Your AS5800 Configuration [4-6](#)
  - Installing New IOS Software on the Cisco AS5800 [4-7](#)
    - Upgrading the DSC Software [4-8](#)
    - Upgrading the Router Shelf Boot Image [4-11](#)
  - Software Upgrade Verification [4-11](#)
- Upgrading the Cisco AS5850 Universal Gateway [4-12](#)
  - Upgrading from a High-Availability Image [4-13](#)
  - Upgrading from a Nonhigh-Availability Image [4-13](#)

**APPENDIX A****Cisco Media Gateway Cable Specifications [A-1](#)**

- Overview [A-1](#)
- Console and Auxiliary Port Cables and Pinouts for Access Servers [A-1](#)
  - Identifying a Rollover Cable [A-2](#)
  - Console Port Cables and Pinouts [A-2](#)
  - Auxiliary Port Signals and Pinouts [A-4](#)
  - Ethernet Port Pinouts [A-4](#)
  - T1/PRI and E1/PRI Card Port Pinouts [A-5](#)
  - T1/PRI and E1/PRI Card Cable Assemblies and Pinouts [A-5](#)

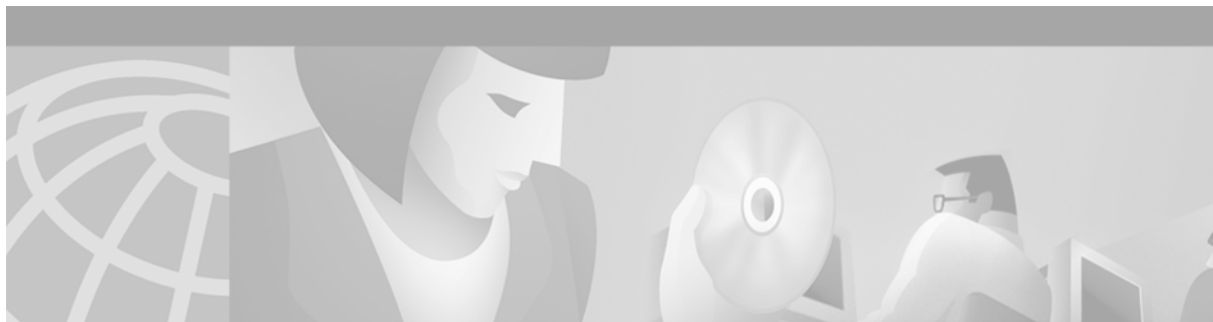
**APPENDIX B****Managing Cisco Media Gateway Software [B-1](#)**

- Software Management Change Process [B-2](#)
  - Making a Baseline of Your Software Library [B-2](#)
  - Synchronizing the Images in Your Software Library [B-3](#)
  - Creating an Approver List [B-3](#)

- Checking for Outstanding Software Defects **B-4**
- Performing Software Upgrades **B-4**
  - Planning the Upgrade **B-5**
    - Determining the Impact of an Upgrade **B-5**
    - Determining the Prerequisites for the Upgrade **B-5**
    - Determining the Upgrade Sequence and Timing **B-5**
  - Getting Software Images **B-7**
    - Getting Backup Images for the Rollback Option **B-7**
    - Software Downloading Processes **B-7**
- Directions for Browsing and Downloading from the Web **B-7**
- Retrieving Software Images Using the Cisco.com FTP **B-9**
- Setting Up a Software Image Upgrade **B-10**
- Setting Up a Device Upgrade **B-11**
- Job Control **B-12**
  - Rescheduling an Upgrade **B-12**
  - Tracking a Scheduled Software Upgrade **B-12**
  - Verifying the Upgrade **B-13**

---

**INDEX**



## Preface

---

This section describes the objectives, audience, organization, and conventions of the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*. The guide points to related publications and describes online sources of technical information.

## Document Objectives

The guide describes how to use Cisco equipment to connect trunks from the Public Switched Telephone Network (PSTN) to the Cisco Media Gateway and how the Cisco Media Gateway Controller software controls those connections. This guide also gives general guidelines for and configuring media gateways for Cisco SS7 Interconnect for Access Servers Solution and Cisco SS7 Interconnect for Voice Gateways Solutions.

## Who Should Read This Guide

This publication is designed for people who have some experience installing networking equipment, such as routers, hubs, servers, and switches. The person configuring this equipment should be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician.

This guide is intended as part of a suite of documents for the following users:

- Component installers—Who have experience installing telecommunications equipment and cables, as well as experience installing data communications equipment and cabling.
- Network operators and administrators—Who have experience in telecommunications networks, protocols, and equipment, as well as a familiarity with data communications networks, protocols, and equipment.
- Network designers—Who have experience with telecommunications networks, protocols, and equipment, as well as experience with data communications networks, protocols, and equipment.

# Organization

The major sections of this guide are as follows:

Chapter	Title	Description
Chapter 1	<a href="#">Introduction to Media Gateways</a>	Provides an overview of the <i>Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide</i> , including architecture and component description.
Chapter 2	<a href="#">Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution</a>	Discusses the process of configuring media gateways for Voice-over-IP.
Chapter 3	<a href="#">Configuring Media Gateways for the SS7 Interconnect for Access Servers Solution</a>	Discusses the process of configuring media gateways to function as SS7 dial access servers.
Chapter 4	<a href="#">Upgrading Cisco Media Gateway Software</a>	Lists instructions for loading new Cisco IOS images on media gateways.
Appendix A	<a href="#">Cisco Media Gateway Cable Specifications</a>	Provides a description of the cabling used in the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions.
Appendix B	<a href="#">Managing Cisco Media Gateway Software</a>	Provides information about maintaining the software library.

## Document Conventions

**Table 1** *Media Gateway Guide Conventions*

Convention	Description
<b>boldface font</b>	Commands and keywords.
<i>italic font</i>	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x   y   z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
screen font	Examples of information displayed on the screen.
<b>boldface screen font</b>	Examples of information you must enter.



**Table 1** *Media Gateway Guide Conventions (continued)*

Convention	Description
< >	Nonprinting characters, for example passwords, appear in angle brackets in contexts where italics are not available.
[ ]	Default responses to system prompts appear in square brackets.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this publication.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

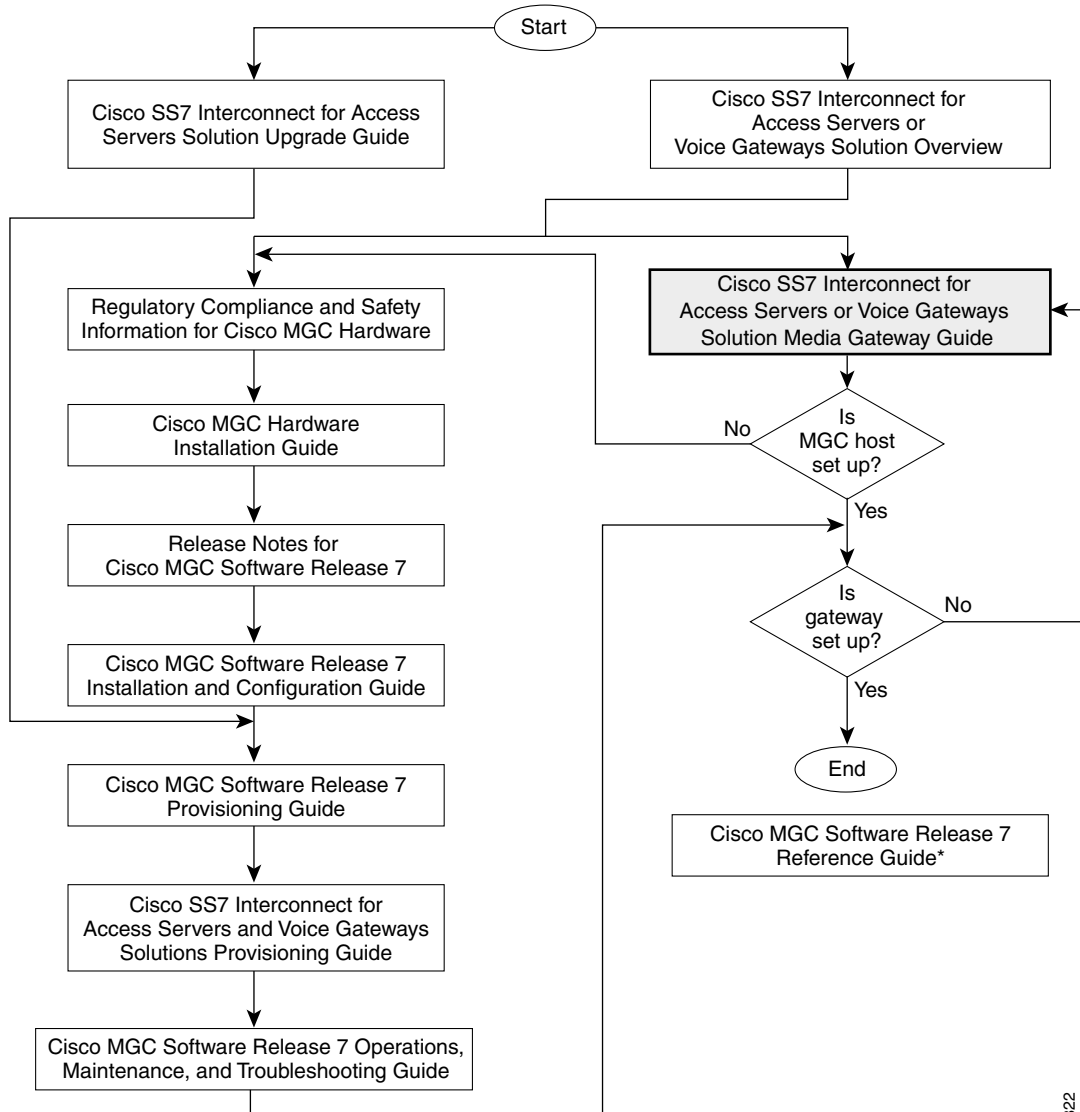
## Cisco Media Gateway Documentation Suite

Refer to the following documents for information about Cisco Media Gateway Controller Release 7:

- *Cisco Media Gateway Controller Hardware Installation Guide*
- *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*
- *Cisco Media Gateway Controller Software Release 7 Reference Guide*
- *Cisco SS7 Interconnect for Access Servers Solution Upgrade Guide*
- *Regulatory Compliance and Safety Information for Cisco Media Gateway Controller Hardware*
- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Release Notes for Cisco Media Gateway Controller Software Release 7*
- *Cisco Media Gateway Controller Online Documentation Notice*

# Documentation Road Map

Here is the road map for the Cisco Media Gateway Controller Release 7 Documentation Suite. Note that the grayed-out box indicates the document you are currently reading.



\* This guide provides useful information that is not required during installation.

30822

Refer to the following documents for detailed Cisco IOS documentation about the Cisco SS7 Interconnect for Access Servers Solutions and Cisco SS7 Interconnect for Voice Gateways Solutions:

- *Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2(B)*
- *Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3*
- *Release Notes for Cisco Media Gateway Controller Software Release 7*

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

### Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

### Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

### Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.





## Introduction to Media Gateways

---

Cisco Media Gateway Controller (MGC) software operates on a UNIX platform and controls call routing between a traditional time-division multiplexing (TDM) network and a packet data network. Calls are routed through a variety of media gateways (MGW), which are separate devices that perform the conversion between the TDM and data network formats. The Cisco MGC software uses a dial plan to determine how to map dialed numbers to other destination numbers, and it uses trunk routing information to determine routes and alternate routes for calls that pass through the MGW.

The Cisco Media Gateway Controller Software Release 7 is part of the following solutions:

- Cisco SS7 Interconnect for Access Servers Solution—Provides a gateway that allows dial-in users on a TDM network to access traditional data services on an IP network. Because this solution supports SS7 signaling, it can be combined with other telephony services such as 800 numbers or caller ID.
- Cisco SS7 Interconnect for Voice Gateways Solution—Provides a gateway for voice calls between a traditional TDM network and a voice-over-IP (VoIP) network. The solution also hosts voice calls between two TDM networks, but it uses two types of call routing: gatekeeper call routing and signaling controller (SC) call routing.

The Cisco SS7 Interconnect for Access Servers Solution supports the following platforms:

- Cisco AS5200 universal access server
- Cisco AS5300 universal access server
- Cisco AS5350 universal gateway
- Cisco AS5400 universal gateway
- Cisco AS5800 universal access server



---

**Note** The Cisco AS5200 can no longer be ordered. Cisco supports the existing installation base only.

---

The Cisco SS7 Interconnect for Voice Gateways Solution supports the following platforms:

- Cisco AS5300 universal access server
- Cisco AS5350 universal gateway
- Cisco AS5400 universal gateway
- Cisco AS5800 universal access server
- Cisco AS5850 universal gateway

# Media Gateway Architecture

The system consists of the following required components that are described in more detail in the “Cisco SS7 Interconnect for Voice Gateways Solution Architecture” section on page 1-3:

Cisco Media Gateway Controller (Cisco MGC)	Performs telephony call processing, routing, signaling, and feature invocations for calls traveling into and out of the packet-switched network.
Cisco Signaling Link Terminal (Cisco SLT)	Used for physical SS7 link termination.
Media gateway (MGW)	Used for bearer channel termination.

Together these components create a system on an IP packet network that connects to a circuit-based TDM network.

Figure 1-1 provides a graphical representation of the Cisco SS7 Interconnect for Access Servers Solution configuration and Figure 1-2 provides a graphical representation of the Cisco SS7 Interconnect for Voice Gateways Solution configuration.

**Figure 1-1 Cisco SS7 Interconnect for Access Servers Solution Architecture**

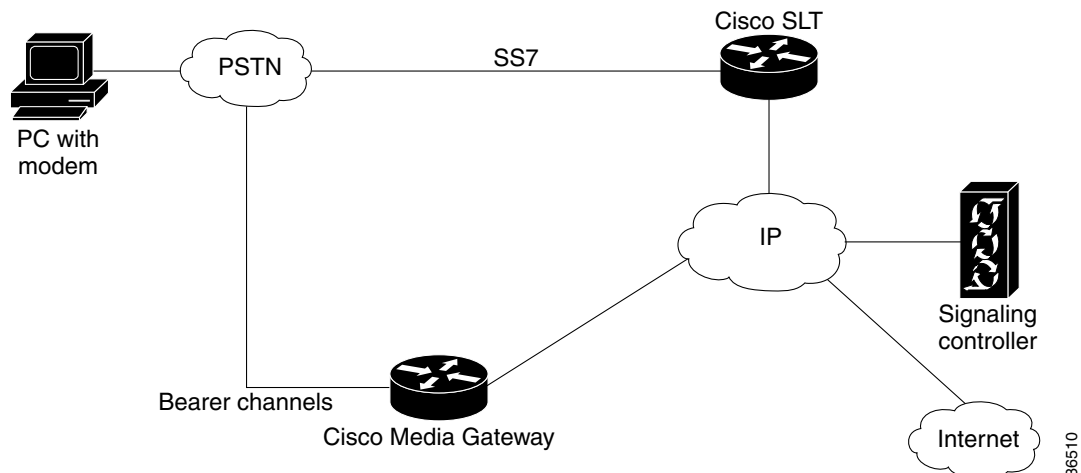
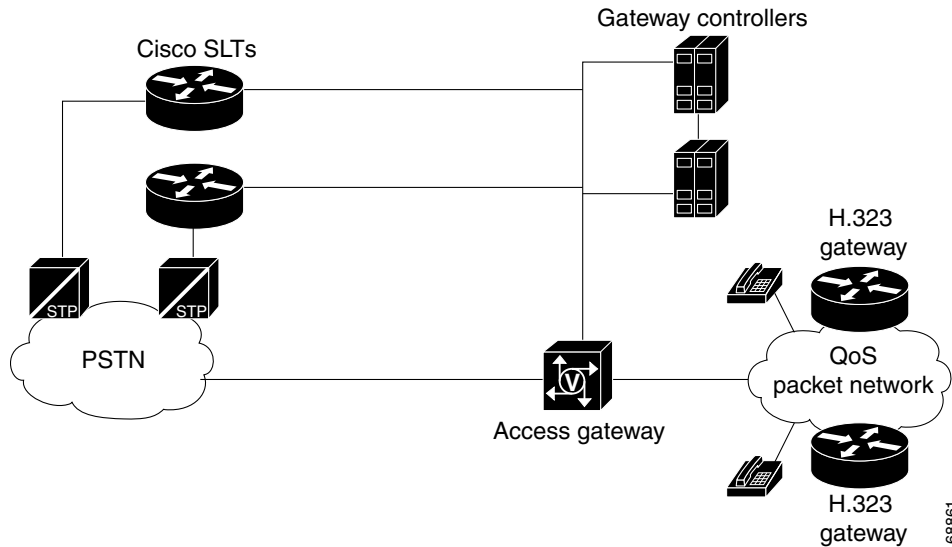




Figure 1-2 Cisco SS7 Interconnect for Voice Gateways Solution Architecture



## Media Gateway Components

This guide contains descriptions of the media gateway and supported solutions. [Table 1-1](#) provides a brief description of the required components.

**Table 1-1** Media Gateway Components

Component	Description
Signaling controller hosts (Cisco SC2200)	In addition to SS7 protocol interworking functions, the Cisco Media Gateway Controller provides system resource management (including the tracking of circuit IDs for ports on the media gateways when calls are assigned), call control (including originating and terminating call processing and signaling), usage measurements for accounting and management purposes, and alarms.  For more information about installing and configuring the Cisco SC2200, refer to <a href="#">Cisco MGC Software Release 7 Installation and Configuration Guide</a> .
Cisco Signaling Link Terminals (Cisco SLTs)	The Cisco SLT handles the incoming and outgoing SS7 messages (MTP layer 1 and 2) from the Signal Transfer Points (STPs). All Cisco SLTs are active and carry traffic. Each Cisco SLT supports one or two SS7 links (one per port). The linksets are distributed across the Cisco SLTs to ensure availability and dependability. Each SLT in a pair can handle the entire signaling load in case of failure, with no impact to call processing.  For more information about installing and configuring the Cisco SLT, refer to <a href="#">Cisco Media Gateway Controller Hardware Installation Guide</a> .

**Table 1-1 Media Gateway Components (continued)**

Component	Description
Cisco Media Gateway Controller Node Manager (CMNM)	<p>CMNM provides the element-specific management features for the SC node. It blends the management framework features of the Cisco Element Management Framework (CEMF) with the individual interfaces and object structures of each managed element to produce an integrated management application.</p> <p>For more information about installing and configuring CMNM, refer to the <i>Cisco Media Gateway Controller Node Manager Users Guide</i>.</p>
Media gateway and supported solutions	The media gateway terminates the PSTN trunks, also referred to as bearer channels that carry the call traffic. The PSTN trunks are T1, E1, or T3 PRI interfaces.

## Media Gateways and Supported Solutions

Table 1-2 lists the media gateways supported by the Cisco SS7 Interconnect for Access Servers Solution and the Cisco SS7 Interconnect for Voice Gateways Solution.

**Table 1-2 Solution Media Gateways**

Media Gateway	Cisco SS7 Interconnect for Access Servers Solution	Cisco SS7 Interconnect for Voice Gateways Solution
Cisco AS5200 <sup>1</sup>	Supported	—
Cisco AS5300	Supported	Supported
Cisco AS5350	Supported	Supported
Cisco AS5400	Supported	Supported
Cisco AS5800	Supported	Supported
Cisco AS5850	—	Supported

1. The Cisco AS5200 can no longer be ordered. Cisco supports the existing installation base only.

### Cisco AS5300 Universal Access Server

For detailed specifications and instructions on installing a Cisco AS5300 and connecting it to a network, see the following documents:

- *Cisco AS5300 Quick Start Guide (with Fast Step)*
- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Software Configuration Guide*

The entire documentation set for the Cisco AS5300 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm)

## Cisco AS5350 Universal Gateway

For detailed specifications and instructions on installing a Cisco AS5350 and connecting it to a network, see the following documents:

- *Cisco AS5350 Universal Gateway Chassis Installation Guide*
- *Cisco AS5350 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5350 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm)

## Cisco AS5400 Universal Gateway

For detailed specifications and instructions on installing a Cisco AS5400 and connecting it to a network, see the following documents:

- *Cisco AS5400 Universal Access Gateway Read Me First*
- *Cisco AS5400 Chassis Installation Guide*
- *Cisco AS5400 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5400 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm)

## Cisco AS5800 Universal Access Server

For detailed specifications and instructions on installing a Cisco AS5800 and connecting it to a network, see the following documents:

- *Read Me First—Cisco AS5800 Universal Access Server*
- *Cisco AS5800 OAM&P Guide*
- *Cisco AS5800 Universal Access Server Hardware Installation Guide*
- *Cisco AS5800 Universal Access Server Dial Shelf Guide*

The entire documentation set for the Cisco AS5800 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm)

## Cisco AS5850 Universal Gateway

For detailed specifications and instructions on installing a Cisco AS5850 and connecting it to a network, see the following documents:

- *Cisco AS5850 Hardware Installation Guide*
- *Cisco AS5850 Universal Gateway Guide*

- *Cisco AS5850 Universal Gateway Commissioning Guidelines*
- *Cisco AS5850 Universal Gateway Operations, Administration, Maintenance, and Provisioning Guide*

The entire documentation set for the Cisco AS5860 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5850/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/index.htm)



# Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution

---

This chapter describes how to configure the access servers used by the Cisco SS7 Interconnect for Voice Gateways Solution. It includes the following sections:

- [Determining Software and Hardware Requirements, page 2-1](#)
- [Installing Media Gateways, page 2-1](#)
- [Configuring Media Gateways, page 2-3](#)
- [Sample Output for the Cisco SS7 Interconnect for Voice Gateways Solution, page 2-22](#)

## Determining Software and Hardware Requirements

Software and hardware requirements vary depending on the version of the Cisco SS7 Interconnect for Voice Gateways Solution installed in your network. To view the latest requirements for your solution, see the following online documentation:

- [Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/voip_rn.htm)  
[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/voip\\_rn.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/voip_rn.htm)

## Installing Media Gateways

This document assumes that all required hardware, voice feature cards, and network modules have been installed, and that each access server or router has been connected to a working IP network. If necessary, refer to the following sections:

- [Installing the Cisco AS5300 Universal Access Server, page 2-2](#)
- [Installing the Cisco AS5350 Universal Gateway, page 2-2](#)
- [Installing the Cisco AS5400 Universal Gateway, page 2-2](#)
- [Installing the Cisco AS5800 Universal Access Server, page 2-2](#)
- [Installing the Cisco AS5850 Universal Gateway, page 2-3](#)

## Installing the Cisco AS5300 Universal Access Server

For instructions on installing a Cisco AS5300 and connecting it to a network, see the following documents:

- *Cisco AS5300 Quick Start Guide (with Fast Step)*
- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Software Configuration Guide*

The entire documentation set for the Cisco AS5300 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm)

## Installing the Cisco AS5350 Universal Gateway

For instructions on installing a Cisco AS5350 and connecting it to a network, see the following documents:

- *Cisco AS5350 Universal Gateway Chassis Installation Guide*
- *Cisco AS5350 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5350 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm)

## Installing the Cisco AS5400 Universal Gateway

For instructions on installing a Cisco AS5400 and connecting it to a network, see the following documents:

- *Cisco AS5400 Universal Access Gateway Read Me First*
- *Cisco AS5400 Chassis Installation Guide*
- *Cisco AS5400 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5400 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm)

## Installing the Cisco AS5800 Universal Access Server

For instructions on installing a Cisco AS5800 and connecting it to a network, see the following documents:

- *Read Me First—Cisco AS5800 Universal Access Server*
- *Cisco AS5800 OAM&P Guide*

- *Cisco AS5800 Universal Access Server Hardware Installation Guide*
- *Cisco AS5800 Universal Access Server Dial Shelf Guide*

The entire documentation set for the Cisco AS5800 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm)

## Installing the Cisco AS5850 Universal Gateway

For instructions on installing a Cisco AS5850 and connecting it to a network, see the following documents:

- *Cisco AS5850 Hardware Installation Guide*
- *Cisco AS5850 Universal Gateway Guide*
- *Cisco AS5850 Universal Gateway Commissioning Guidelines*
- *Cisco AS5850 Universal Gateway Operations, Administration, Maintenance, and Provisioning Guide*



### Note

For detailed instructions on configuring your Cisco AS5850 to operate in handover-split mode, refer to *RSC Handover Redundancy* at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb\\_2/handred.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/handred.htm)

The entire documentation set for the Cisco AS5850 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5850/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/index.htm)

## Configuring Media Gateways

The process for configuring voice gateways includes the following major steps:

- [Setting the ISDN Switch Type, page 2-4](#)
- [Configuring the Cisco AS5300 and Cisco AS5850 for B-Channel Negotiation, page 2-4](#)
- [Configuring Redundant Link Manager, page 2-4](#)
- [Completing VoIP Configuration, page 2-12](#)
- [Configuring Number Translation, page 2-14](#)
- [Configuring the Digit Strip, page 2-14](#)
- [Configuring Dial Peer Call Legs Using Digit Translation Rules, page 2-15](#)

## Setting the ISDN Switch Type

To communicate with the Cisco SC2200, you must set the appropriate ISDN switch type on the media gateway. To set the ISDN switch type, perform the following steps:

---

**Step 1** Enter global configuration mode:

```
Router# configure terminal
Router(config)#
```

**Step 2** Set the ISDN switch type to **primary-ni**:

```
Router# isdn switch-type primary-ni
```

For more information about setting ISDN switch types, refer to *National ISDN Switch Types for Basic Rate and Primary Rate Interfaces* at the following location;

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t\\_3/natisdn.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/natisdn.htm)

---

## Configuring the Cisco AS5300 and Cisco AS5850 for B-Channel Negotiation

To improve call success rates, the Cisco AS5300 and Cisco AS5850 must be configured to negotiate ISDN B-channels with the Cisco Media Gateway Controller (MGC). This negotiation enables the MGC to setup the call on a different channel if the channel requested by the media gateway is unavailable.

To enable ISDN B-channel negotiation, perform the following steps:

---

**Step 1** Enter global configuration mode:

```
Router# configure terminal
Router(config)#
```

**Step 2** To configure the appropriate interface, enter the following command:

```
Router(config)# interface {s0:23 | s0:15}
```




---

**Note** Use **interface s0:23** in T1 networks; use **interface s0:15** in E1 networks.

---

**Step 3** Enter the commands to enable B-channel negotiation:

```
Router(config-if)# isdn negotiate-b
Router(config-if)# isdn negotiate-bchan
```

---

## Configuring Redundant Link Manager

Redundant Link Manager (RLM) provides virtual link management over multiple IP networks so that the Q.931 signaling protocol and other proprietary protocols can be transported on top of redundant links between the Cisco SC2200 and the media gateways. RLM opens, maintains, and closes multiple links, manages buffers of queued signaling messages, and monitors for both link failover and failover of the Cisco SC2200. Additionally, RLM allows these multiple, redundant paths to be treated as one path by upper layers.



**Note**

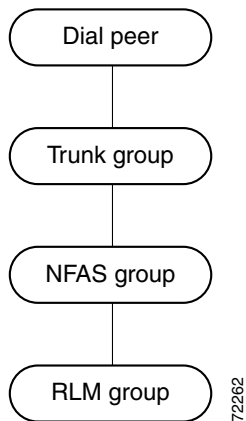
Because the Cisco SC2200 can support only two RLM links to a NFAS group, you can assign only one interface to each route-switch-controller (RSC) card in a Cisco AS5850 operating in handover-split mode. This prevents link redundancy between the individual RSCs and the Cisco SC2200.

Q.921 is used to encapsulate the Q.931 messages, which guarantees the in-sequence transmission of Extended Q.931 messages and provides for retransmission when necessary. UDP provides for the connectionless transfer of signaling messages across the subnetworks (LAN or WAN) that connect the media gateways to the Cisco SC2200.

Because RLM handles all signaling between the Cisco SC2200 and the media gateway, D channels can be used to carry bearer traffic. This is accomplished through the use of Non-Facility Associated Signaling (NFAS). NFAS allows a single D channel to control multiple PRI interfaces. That single D channel is then mapped to the RLM group.

Figure 2-1 shows the mapping that occurs between a VoIP or POTS dial peer and the RLM group.

**Figure 2-1 Call Flow from Dial Peer to RLM Group**

**Note**

This section includes basic instructions for configuring Redundant Link Manager in a Cisco SS7 Interconnect for Voice Gateways Solution. For detailed instructions on planning for RLM implementation, refer to the following online documentation:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/rlm\\_123.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/rlm_123.htm)

**Note**

To configure RLM on a handover-split-mode Cisco AS5850, see the “Configuring RLM on a Handover-Split Mode Cisco AS5850” section on page 2-7.

## Configuring RLM on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Classic-Split Mode Cisco AS5850

To configure RLM on media gateways other than a Cisco AS5850 in handover-split mode, perform the following steps:

**Step 1** To enter enable mode, enter the following commands:

```
Router> enable
Password: password
Router#
```

**Step 2** To enter global configuration mode, enter the following command:

```
Router# configure terminal
Router(config)#
```

**Step 3** To specify the interface, enter the following command:

```
Router(config)# interface FastEthernet0
```

**Step 4** To specify the RLM group that you want to configure, enter the following command:

```
Router(config-if)# rlm group 0
Router(config-rlm-group)#
```

**Step 5** To specify the device name of the Cisco SC2200, enter the following command:

```
Router(config-rlm-group)# server mgc1
```

**Step 6** To specify the link addresses and their weighting preferences, enter the following commands:

```
Router(config-rlm-group-sc)# link address 10.1.4.1 source FastEthernet0 weight1
Router(config-rlm-group-sc)# link address 10.1.4.2 source FastEthernet0 weight2
```



**Note** Links with higher weighting numbers are given higher priority to become active links. If all entries have the same weighting, all links will be treated equally.

**Step 7** Repeat [Step 5](#) and [Step 6](#) for the second Cisco SC2200:

```
Router(config-rlm-group-sc)# server mgc2
Router(config-rlm-group-sc)# link address 10.1.5.1 source FastEthernet0 weight1
Router(config-rlm-group-sc)# link address 10.1.5.2 source FastEthernet0 weight2
```

**Step 8** To enable EIGRP, enter the following command:

```
Router(config-rlm-group-sc)# router eigrp 100
Router(config-router)#
```

**Step 9** Assign controller interfaces to **nfas\_group 0**.

```
Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 0
Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 0
Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 27 nfas_group 0
```



**Note** For detailed instructions on configuring NFAS groups, refer to the following online documentation:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t\\_3/nfas.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/nfas.htm)

## Configuring RLM on a Handover-Split Mode Cisco AS5850

A Cisco AS5850 configured for handover-split mode provides greater redundancy and system availability by enabling each RSC to automatically take control of call processing if the other RSC fails. In normal operation, the RSC in slot 6 controls slots 0 through 5, and the RSC in slot 7 controls slots 8 through 13. When an RSC failure occurs in handover-split mode, the remaining RSC takes over control of all slots, cards, and call processing. The failed RSC will remain in a standby state until the active RSC is instructed to relinquish control of the slots usually controlled by the standby RSC.

Because of the different architecture used by the Cisco AS5850, RLM requires a different configuration to take advantage of handover-split mode. For each RSC, you must configure two RLM groups: an active RLM group to handle calls on the slots controlled by that RSC, and a standby RLM group to handle calls on the other slots if the other RSC fails. [Table 2-1](#) shows the status of these four RLM groups during normal operation and when an RSC goes out of service.

**Table 2-1 RLM Status Under Normal and Failure Conditions**

Condition	RLM Group 0 RSC 0, Slot 0 to 5	RLM Group 1 RSC 0, Slot 8 to 13	RLM Group 2 RSC 1, Slot 8 to 13	RLM Group 3 RSC 1, Slot 0 to 5
Normal operation	Active	Standby	Active	Standby
RSC 0 fails	Standby	Standby	Active	Active
RSC 1 fails	Active	Active	Standby	Standby

### Handover-Split Mode Limitations

Cisco AS5850s configured for handover-split mode operate under the following limitations:

- Each Cisco AS5850 can support 2 CT3 trunks. Cisco AS5850s configured for classic-split mode can support up to 4 CT3 trunks each.
- After an RSC fails, it takes up to 2 minutes for the active RSC to take over for the failed RSC. During this time, calls handled by the failed RSC are dropped, and new calls are not accepted. Calls handled by the active RSC are not affected by a switchover.

For detailed information on classic-split and handover-split modes, refer to the following online documentation:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb\\_2/handred.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/handred.htm)

## Configuring RLM Groups Associated with RSC 0

To configure RLM groups for RSC 0 on a handover-split mode Cisco AS5850, perform the following steps:

**Step 1** Enter enable mode.

```
Router> enable
Password: password
Router#
```

**Step 2** Enter global configuration mode.

```
Router# configure terminal
Router(config)#
```

**Step 3** Specify the interface to be used by RSC 0.

```
Router(config)# interface GigabitEthernet 6/0
```

**Step 4** Specify the RLM group that you want to configure.

```
Router(config-if)# rlm group 0
Router(config-rlm-group)#
```

**Step 5** Specify the device name, link addresses, and weighting preferences for both Cisco SC2200s.

```
Router(config-rlm-group)# server mgc1
Router(config-rlm-group-sc)# link address 10.1.4.1 source GigabitEthernet0 weight1
Router(config-rlm-group-sc)# server mgc2
Router(config-rlm-group-sc)# link address 10.1.5.1 source GigabitEthernet0 weight2
```



**Note** Links with higher weighting numbers are given higher priority to become active links. If all entries have the same weighting, all links will be treated equally.

**Step 6** Repeat [Step 4](#) and [Step 5](#) for RLM group 1.

**Step 7** Assign controller interfaces to **nfas\_group 0** and **nfas\_group 1**. Controller interfaces assigned to slots 0 through 5 must be in one NFAS group. Controller interfaces assigned to slots 8 through 13 must be in the other NFAS group.

```
controller T1 2/0:1
 framing esf
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
!
controller T1 2/0:2
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 0
!
controller T1 2/0:3
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 0
!
controller T1 2/0:28
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 27 nfas_group 0
!
controller T1 10/0:1
 framing esf
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
!
```

```

controller T1 10/0:2
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 1
!
controller T1 10/0:3
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 1
!
controller T1 10/0:28
 framing esf
 pri-group timeslots 1-24 nfas_d none nfas_int 27 nfas_group 1

```

**Step 8** Assign signaling interfaces to RLM groups 0 and 1.

```

interface Serial2/0:1:23
 isdn switch-type primary-ni
 isdn incoming-voice modem
 isdn rlm-group 0

interface Serial10/0:1:23
 isdn switch-type primary-ni
 isdn incoming-voice modem
 isdn rlm-group 1

```

**Step 9** Assign UDP port 3002 to RLM group 1.

```

rlm group 1
 protocol rlm 3002

```




---

**Note** RLM group 0 uses 3000 as the default UDP port.

---

**Step 10** Shutdown RLM group 1, which is assigned to the cards controlled by the other RSC.

```

rlm group 1
 shutdown
 protocol rlm port 3002
 server mgc1
 link address 10.1.4.1 source GigabitEthernet6/0 weight 1

server mgc2
 link address 10.1.5.1 source GigabitEthernet6/0 weight 2

```

---

## Configuring RLM Groups Associated with RSC 1

To configure RLM groups for RSC 1 on a handover-split mode Cisco AS5850, perform the following steps:

**Step 1** Enter enable mode.

```

Router> enable
Password: password
Router#

```

**Step 2** Enter global configuration mode.

```

Router# configure terminal
Router(config)#

```

**Step 3** Specify the interface to be used by RSC 1.

```
Router(config)# interface GigabitEthernet 7/0
```

**Step 4** Specify the RLM group that you want to configure.

```
Router(config-if)# rlm group 2
Router(config-rlm-group)#
```

**Step 5** Specify the device name, link addresses, and weighting preferences for both Cisco SC2200s.

```
Router(config-rlm-group)# server mgc1
Router(config-rlm-group-sc)# link address 10.1.4.1 source GigabitEthernet0 weight1
Router(config-rlm-group-sc)# server mgc2
Router(config-rlm-group-sc)# link address 10.1.5.1 source GigabitEthernet0 weight2
```

**Step 6** Repeat [Step 4](#) and [Step 5](#) for RLM group 3.

**Step 7** Assign controller interfaces to **nfas\_group 3** and **nfas\_group 2**. Controller interfaces assigned to slots 0 through 5 must be in one NFAS group. Controller interfaces assigned to slots 8 through 13 must be in the other NFAS group.

```
controller T1 2/0:1
  framing esf
  pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 3
!
controller T1 2/0:2
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 3
!
controller T1 2/0:3
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 3
!
controller T1 2/0:28
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 27 nfas_group 3
!
controller T1 10/0:1
  framing esf
  pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 2
!
controller T1 10/0:2
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 2
!
controller T1 10/0:3
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 2
!
controller T1 10/0:28
  framing esf
  pri-group timeslots 1-24 nfas_d none nfas_int 27 nfas_group 2
```

**Step 8** Assign signaling interfaces to the RLM groups 3 and 2.

```
interface Serial2/0:1:23
  isdn switch-type primary-ni
  isdn incoming-voice modem
  isdn rlm-group 3

interface Serial10/0:1:23
  isdn switch-type primary-ni
```

```

isdn incoming-voice modem
isdn rlm-group 2

```

**Step 9** Assign UDP port 3002 to RLM group 2.

```

rlm group 2
  protocol rlm port 3002
  no shutdown

```

**Step 10** Assign UDP port 3000 and then shutdown RLM group 3.

```

rlm group 3
  protocol rlm 3000
  shutdown

```

## Verifying RLM Configuration

To verify RLM configuration, perform the following steps:



### Note

The output included in the steps that follow is for reference purposes only. Your media gateways will produce different results as appropriate for your network and configuration.

**Step 1** To verify the RLM configuration, enter the following command and specify the group number:

```
Router# show rlm group 0 status
```

```

RLM Group 0 Status
User/Port: RLM_MGR/3000 ISDN3001
Link State: Up          Last Link Status Reported: Up
Next tx TID: 1         Last rx TID: 0
Server Link Group[mgc1]:
  link [10.1.1.1(Ethernet0), 10.1.4.1] = socket[active]
  link [10.1.1.2(FastEthernet0), 10.1.4.2] = socket[standby]
Server Link Group[mgc2]:
  link [10.1.1.1(Ethernet0), 10.1.5.1] = socket[opening]
  link [10.1.1.2(FastEthernet0), 10.1.5.2] = socket[opening]

```

The link state must be up, and no errors should be reported.

**Step 2** To view layer status information, enter the following command:

```
Router# show isdn status
```

```

Global ISDN Switchtype = primary-ni
ISDN Serial1:23 interface
  dsl 0, interface ISDN Switchtype = primary-ni :Primary D channel of nfas group 0
  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)
  Activated dsl 0 CCBS = 0
ISDN Serial2:23 interface
dsl 1, interface ISDN Switchtype = primary-ni :Group member of nfas group 0
  Layer 1 & 2 Status Not Applicable
  Layer 3 Status:
    0 Active Layer 3 Call(s)
  Activated dsl 1 CCBS = 0

```

Total Allocated ISDN CCBS = 0

For Serial 0:23 (the first half of the message):

- Layer 1 Status should be ACTIVE.
- Layer 2 Status should be MULTIPLE\_FRAME\_ESTABLISHED. (It might take several seconds for Layer 2 status to appear.)
- Layer 3 Status should be 0 Active Layer 3 Calls.

The second half of the message displays information for Serial 1:23.



**Tip**

If the Layer 1 Status is Deactivated, it indicates a problem at the physical layer. Make sure that the cable connection is not loose or disconnected.

A Layer 2 error indicates that the Cisco MGW cannot communicate with the telco; there is a problem at the data link layer. There may be a problem with your telco, or the framing and line code types you entered may not match that of your telco.

## Completing VoIP Configuration

This section lists the steps to configure the voice gateways in your solution to use Voice over IP (VoIP). Perform the following steps to complete this configuration:

- 
- Step 1** Establish a working IP network. For more information about configuring IP, refer to *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1 at the following location:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/ip\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/ip_c/index.htm)
- Step 2** Complete your company's dial plan and establish a working telephony network. For more information, see the appropriate documentation for your gateway:
- *Voice over IP for the Cisco AS5300*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/voip5300/voip53\\_1.htm4934vcip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/voip5300/voip53_1.htm4934vcip.htm)
  - *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/53swcg/index.htm)
- Step 3** Integrate your dial plan and telephony network into your existing IP network topology. Merging your IP and telephony networks depends on your particular IP and telephony network topology. In general, Cisco suggests the following:
- Using canonical numbers wherever possible. (It is important to avoid situations where numbering systems are significantly different on different routers or access servers in your network.)
  - Making routing and dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.
  - Contact your PBX vendor for instructions about how to reconfigure the appropriate PBX interfaces.
- Step 4** Depending on the topology of your network or the resources used in your network, you might need to perform the following additional tasks:
- Distinguishing voice and modem calls on the media gateway



- Optimizing dial peer and network interface configurations
- Configuring IP precedence for dial peers
- Configuring RSVP for dial peers
- Configuring codec and VAD for dial peers
- Configuring Voice over IP for your H.323 clients



**Note** For further information about configuring dial peers, refer to *Dial Peer Enhancements* at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm\\_5/ftdpeer.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftdpeer.htm)

Cisco SS7 Interconnect for Voice Gateways Solution also offers VFC management features that enable you to easily upgrade and manage the system software stored in VFC Flash memory. Depending on your configuration, you might need to perform the following tasks to manage VCWare or DSPWare:

- Downloading VCWare
- Copying Flash files to the VFC
- Downloading VCWare to the VFC from the media gateway motherboard
- Downloading VCWare to the VFC from a TFTP server
- Unbundling VCWare
- Adding files to the default file list
- Adding codecs to the capability list
- Deleting files from VFC Flash memory
- Erasing the VFC Flash memory

## Configuring Number Translation

Number translation is used in dial-peer configuration mode to match on a number type for a dial peer call leg.

To configure number translation using the numbering-type command in dial-peer configuration mode, enter the following commands in global configuration mode:

Command	Purpose	Example
<b>dial-peer voice</b> <i>tag</i> [ <b>voip</b>   <b>pots</b> ]	Enters the dial-peer configuration mode to configure a VoIP or POTS peer.	Media-Gateway (config) # <b>dial-peer voice 100 pots</b>
<b>numbering-type</b> <i>type of number</i>	Specifies number type. Number types are: <ul style="list-style-type: none"> <li>• International</li> <li>• Abbreviated</li> <li>• National</li> <li>• Network</li> <li>• Reserved</li> <li>• Subscriber</li> <li>• Unknown</li> </ul>	Media-Gateway (config-dial-peer) # <b>numbering-type international</b>

## Configuring the Digit Strip

When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface. The Cisco SS7 Interconnect for Voice Gateways Solution implements a new command called the digit strip option to make this default behavior an option. The digit strip option is enabled by default.

To disable digit strip for a dial peer, enter the following commands in global configuration mode:

Command	Purpose	Example
<code>dial-peer voice tag [pots]</code>	Enters the dial-peer configuration mode to configure a POTS peer.	<p><b>Note</b> In this example, the dialed number is 525-1234 and the dial string matches dial-peer tag 100. The destination-pattern is 525..., strip match yields 1234, prefix 521 yields 521-1234.</p> <pre>Media-Gateway (config) #dial-peer voice 100 pots Media-Gateway (config-dial-peer) #destination-pattern 525... Media-Gateway (config-dial-peer) #direct-inward dial Media-Gateway (config-dial-peer) #no digit strip Media-Gateway (config-dial-peer) #port0:D</pre>
<code>no digit strip</code>	Disables digit strip.	

## Configuring Dial Peer Call Legs Using Digit Translation Rules

A dial peer defines the characteristics associated with a call leg. Dial peers are used to apply attributes to call legs and to identify call origin and destination. Attributes applied to a call leg include QoS, codec, VAD, and fax rate. A call leg is a discrete segment of a call connection that lies between two points in the connection. All of the call legs for a particular connection have the same connection ID.

There are two different kinds of dial peers:

- **POTS**—POTS dial peers describe the line characteristics usually associated with a traditional telephony network. POTS dial peers point to a particular voice port on a network device. On the media gateway, POTS dial peers point to a specific voice port on the media gateway through which voice traffic will travel to the rest of the voice network.
- **VoIP**—VoIP dial peers describe the line characteristics usually associated with a packet network connection (in the case of VoIP, this is an IP network). VoIP peers define the line characteristics between VoIP devices—the routers and access servers carrying voice traffic in this voice network.

A POTS dial peer points to a voice-port on the router, while the destination of a VoIP dial peer points to the destination IP address of the voice-router that terminates the call.

Complete the following procedures to configure call legs using the **translation-rule** command:



**Tip**

You should configure your translation rules before you apply rules to your dial-peer call legs.

- Step 1** To enter the translation-rule configuration mode and specify a rule, enter the following commands in global configuration mode:

Command	Purpose	Example
<b>translation-rule translation-tag</b>	Defines a translation-rule tag number and enter translation-rule configuration mode. All subsequent commands that you enter in this mode before you exit will apply to this translation-rule tag.	Media-Gateway (config) # <b>translation-rule 5</b>
<b>rule precedence input-searched-pattern substituted-pattern match-type substituted-type</b>	Specifies translation rules. This command can be entered <i>n</i> times and is applied to translation-rule defined in Step 1.	Media-Gateway (config-translate) # <b>rule 1 213% 510 national international</b>



**Note** Applying translation rules to more than one dial-peer call leg in your end-to-end call is not recommended.

- Step 2** To apply a rule to an inbound POTS call leg, enter the following commands in global configuration mode:

Command	Purpose	Example
<b>voice-port port</b>	Specifies the voice port.	Media-Gateway (config) # <b>voice-port 0:1</b>
<b>translate [called   calling] translation-tag</b>	Specifies the translation tag for inbound called or calling number.	Media-Gateway (config-voiceport) # <b>translate called 5</b>

- Step 3** To apply a rule to an outbound VoIP call leg, enter the following commands in global configuration mode:

Command	Purpose	Example
<b>dial-peer voice tag voip</b>	Enters the dial-peer configuration mode to configure a VoIP peer.	Media-Gateway (config) # <b>dial-peer voice 100 voip</b>
<b>session target {ipv4:destination-address   dns:host-name}</b>	Specifies a destination IP address for this dial peer.	Media-Gateway (config-dial-peer) # <b>session target ipv4:10.1.1.2.2</b>
<b>translate-outgoing calling translation-tag</b>	Translates outbound calling number.	Media-Gateway (config-voiceport) # <b>translate-outgoing calling 5</b>

- Step 4** To apply a rule to a VoIP call that originates from an H.323 node, enter the following global command:

Command	Purpose	Example
<b>voip-incoming translation-rule called translation-tag</b>	Specifies the translation tag for the VoIP inbound call leg.	Media-Gateway (config) # <b>voip-incoming translation-rule called 5</b>

- Step 5** To apply a translation rule to an outbound POTs call leg, enter the following commands in global configuration mode:

Command	Purpose	Example
<b>dial-peer voice</b> <i>tag pots</i>	Enters the dial-peer configuration mode to configure a POTs dial peer.	Media-Gateway (config) <b>#dial-peer voice 100 pots</b>
<b>port</b> <i>port</i>	Specifies the voice port.	Media-Gateway (config-dial-peer) <b>#port 0:1</b>
<b>translate-outgoing</b> [ <b>called</b>   <b>calling</b> ] <i>translation-tag</i>	Specifies the translation tag for inbound called or calling number.	Media-Gateway (config-dial-peer) <b>#translate-outgoing called 5</b>

## Sample Configuration and Output for Voice-over-IP

Following is a sample output from a Cisco AS5300 set up for bearer channels for VoIP:

- Step 1** Enter your host name:

```
hostname XXXXXX
!
no logging buffered
no logging console
aaa new-model
```

- Step 2** Enter your password:

```
!
username voice password
username lab password
!
!
resource-pool disable
!
!
!
ip subnet-zero
no ip domain-lookup
ip host carteret 10.15.12.134 10.15.12.150
ip host YauPon 10.15.12.135 10.15.12.151
!
mgcp package-capability trunk-package
mgcp default-package trunk-package
```

- Step 3** Enter **isdn switch-type primary-ni** (This is the first command you will enter once the router is up and running.)

```
isdn voice-call-failure 0
cns event-service server
mta receive maximum-recipients 0
!
dial-control-mib max-size 1200
!
```

- Step 4** Enter **controller T1 0**: (This is the controller configuration command.)

```

framing esf
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
```

**Step 5** Enter **controller T1 1**:

```

framing esf
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
```

**Step 6** Enter **controller T1 2**:

```

framing esf
clock source line secondary 1
linecode b8zs
cablelength short 133
```

**Step 7** Enter **pri-group timeslots 1-24 nfas\_d primary nfas\_int 2 nfas\_group 0**:

This command links the PRI bearer channels on the media gateway to the RLM group for D-channel communication to the signaling controller over IP. The `nfas_group` number represents one or more PRIs that are controlled by the same D-channel. The `int` number should be configured to match the T-1 controller number.

Some tips to remember when configuring are as follows:

- Multiple T1/E1s can be part of the same `nfas_group`.
- Multiple NFAS groups within the same RLM group on the media gateway are not supported at this time.
- The `nfas_int` number should be unique and defines the D-channel.
- All PRIs have to be part of the one RLM group.

**Step 8** Enter **controller T1 3**:

```

framing esf
clock source line primary
linecode b8zs
cablelength short 133
```

**Step 9** Enter **pri-group timeslots 1-24 nfas\_d none nfas\_int 3 nfas\_group 0**.

The voice ports will be automatically configured as shown below. The voice-port is created as a result of **pri group nfas** command. Voice ports 2:D and 3:D will be used in `nfas-group 0`.

```

!
!
voice-port 0:D
!
voice-port 1:D
!
voice-port 2:D
!
voice-port 3:D
```

The dial peers shown below are classic examples of Cisco H.323 provisioning to reach call destination.

**Step 10** Enter **dial-peer voice 471 pots**:

```

destination-pattern 471.....
direct-inward-dial
  port 2:D
  prefix 471
!
```

**Step 11** Enter **dial-peer voice 4514101 pots:**

```

destination-pattern 4514101...
direct-inward-dial
  port 0:D
  prefix 4514101
!
```

**Step 12** Enter **dial-peer voice 4514102 pots:**

```

destination-pattern 4514102...
direct-inward-dial
  port 1:D
  prefix 4514102
!
```

**Step 13** Enter **dial-peer voice 4101 pots:**

```

destination-pattern 4101...
direct-inward-dial
  port 0:D
  prefix 4101
!
```

**Step 14** Enter **dial-peer voice 4102 pots:**

```

destination-pattern 4102...
direct-inward-dial
  port 1:D
  prefix 4102
!
```

**Step 15** Enter **dial-peer voice 271 voip:**

```

destination-pattern 271.....
session target ipv4:172.18.193.110
tech-prefix 271#
!
num-exp 451#.....
num-exp 451#.....
num-exp 471#.....
!
gateway
!
```

**Step 16** Enter **interface Loopback0:**

```

ip address 10.15.14.233 255.255.255.252
no ip directed-broadcast
h323-gateway voip interface
h323-gateway voip id z3-gk1 ipaddr 10.15.14.197 1719
h323-gateway voip h323-id z3-5300-1
h323-gateway voip tech-prefix 451#
h323-gateway voip tech-prefix 471#
!
```

**Step 17** Enter **interface Ethernet0:**

```

ip address 10.15.12.2 255.255.255.240
no ip directed-broadcast
```

!

**Step 18** Enter **interface Serial1:23**.

**Step 19** Enter **isdn rlm-group 0**.

This command is created as a result of the RLM global configuration command that resides at the bottom of the configuration.

**Step 20** Enter **rlm group 0**.

This command allows the SC to communicate with the Cisco Media Gateway for call signaling and bearer channel control over UDP ports 3000 for Q.921 keepalives and 3001 for Q931 call setup.

```
server name x
  link address 10.15.12.134 source Ethernet0 weight 5
  link address 10.15.12.150 source FastEthernet0 weight 2
server name y
  link address 10.15.12.135 source Ethernet0 weight 5
  link address 10.15.12.151 source FastEthernet0 weight 2
radius-server host 10.15.12.6 auth-port 1645 acct-port 1646
radius-server key tvtest
```

Radius configuration is used for authentication and accounting records.

**Step 21** Enter **ntp server 10.10.10.25**.

Network Time Protocol (NTP) is recommended to synchronize all the components of the solution to the same time reference. This can be achieved with the router or another NTP device such as the master source.

## Verifying the Configuration

To verify the configuration perform the following steps:

**Step 1** Enter **sh isdn nfas gr 0**.

```
ISDN NFAS GROUP 0 ENTRIES:
```

```
The primary D is Serial2:23.
The NFAS member is Serial3:23.
```

The example shown above indicates the primary D-channel interface and its associated members in the group. There are two total NFAS members. There are 48 total available B channels.

The primary D-channel is DSL 2 in the IN SERVICE state.

There is currently no backup D-channel configured.

The current active layer 2 DSL is 2.

**Step 2** Enter **sh isdn stat** to show the status:

```
ISDN Serial2:23 interface          rlm-group = 0
      dsl 2, interface ISDN Switchtype = primary-ni : Primary D channel of nfas group 0
Layer 1 Status:
```



```

ACTIVE
Layer 2 Status:
  TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
  I_Queue_Len 0, UI_Queue_Len 0
Layer 3 Status:
  0 Active Layer 3 Call(s)
Activated dsl 2 CCBS = 0
The Free Channel Mask: 0x80FFFFFF
ISDN Serial3:23 interface
  dsl 3, interface ISDN Switchtype = primary-ni : Group member of nfas group 0
Layer 1 Status:
ACTIVE
Layer 2 Status: Not Applicable
Layer 3 Status:
  0 Active Layer 3 Call(s)
Activated dsl 3 CCBS = 0

```

**Step 3** Enter `sh rlm gro 0`.

The presence of two signaling controllers shown below, indicates redundancy in the case of failover. This step is optional.

```

RLM Group 0 Status
User/Port: RLM_MGR/3000 ISDN/3001
RLM Version : 2
Link State: Up          Last Link Status Reported: Up
Next tx TID: 1          Last rx TID: 0
Server Link Group[carteret]: Last Reported Priority: HIGH
  link [10.15.12.2(Ethernet0), 10.15.12.134] = socket[standby]
  link [10.15.12.34(FastEthernet0), 10.15.12.150] = socket[standby]
Server Link Group[yaupon]: Last Reported Priority: HIGH
  link [10.15.12.2(Ethernet0), 10.15.12.135] = socket[active]
  link [10.15.12.34(FastEthernet0), 10.15.12.151] = socket[standby]

```

This is the interface that call signaling will traverse.

```

RLM Group 0 Timer Values
open_wait   = 3s          force-down   = 30s
recovery    = 12s         switch-link  = 5s
minimum-up  = 60s         retransmit   = 1s
keepalive   = 1s

```

```

RLM Group 0 Statistics
Link_up:
  last time occurred at Nov 18 10:57:43.992, total transition=59
  avg=06:36:36.298, max=2d22h, min=00:00:00.000, latest=00:00:04.844
Link_down:
  last time occurred at Nov 18 10:57:10.992, total transition=28
  avg=00:56:54.621, max=1d00h, min=00:00:00.000, latest=00:00:33.000
Link_recovered:
  last time occurred at Nov 18 10:56:58.992, success=25(49%), failure=26
  avg=0.038s, max=0.224s, min=0.000s, latest=0.000s
Link_switched:
  last time occurred at Nov 11 12:25:52.324, success=6(100%), failure=0
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
Server_changed:
  last time occurred at Nov 18 10:56:54.148 for totally 29 times
Server Link Group[carteret]:
Open the link [10.15.12.2(Ethernet0), 10.15.12.134]:
  last time occurred at Nov 18 10:57:40.992, success=33(6%), failure=509-0
  avg=43.634s, max=177.004s, min=0.000s, latest=0.000s
Echo over link [10.15.12.2(Ethernet0), 10.15.12.134]:
  last time occurred at Nov 18 11:12:40.979, success=1355251(97%), failure=33527-0
  avg=0.000s, max=0.964s, min=0.000s, latest=0.000s

```

```

Open the link [10.15.12.34(FastEthernet0), 10.15.12.150]:
  last time occurred at Nov 18 10:57:40.992, success=33(6%), failure=509-0
  avg=43.549s, max=177.004s, min=0.000s, latest=0.000s
Echo over link [10.15.12.34(FastEthernet0), 10.15.12.150]:
  last time occurred at Nov 18 11:12:40.979, success=1378593(97%), failure=32887-0
  avg=0.000s, max=0.960s, min=0.000s, latest=0.000s
Server Link Group[yaupon]:
Open the link [10.15.12.2(Ethernet0), 10.15.12.135]:
  last time occurred at Nov 18 10:57:40.992, success=35(1%), failure=2247-0
  avg=61.347s, max=177.000s, min=0.000s, latest=0.004s
Echo over link [10.15.12.2(Ethernet0), 10.15.12.135]:
  last time occurred at Nov 18 11:12:41.983, success=998740(87%), failure=139142-0
  avg=0.000s, max=2.688s, min=0.000s, latest=0.004s
Open the link [10.15.12.34(FastEthernet0), 10.15.12.151]:
  last time occurred at Nov 18 10:57:40.992, success=35(1%), failure=2247-0
  avg=61.270s, max=177.000s, min=0.000s, latest=0.032s
Echo over link [10.15.12.34(FastEthernet0), 10.15.12.151]:
  last time occurred at Nov 18 11:12:42.019, success=1059514(88%), failure=138872-0
  avg=0.000s, max=2.688s, min=0.000s, latest=0.016s

```

---

## Sample Output for the Cisco SS7 Interconnect for Voice Gateways Solution

The following sections contain sample output for a voice gateway that has been configured for the Cisco SS7 Interconnect for Voice Gateways Solution.

```

!
version 12.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log uptime
no service password-encryption
service internal
!
hostname
!
no logging console
enable password
!
username all
spe 1/0 2/9
firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
!
!
!
!
modem recovery action none
ip subnet-zero
no ip domain-lookup
ip host holden 10.15.0.1
!
isdn switch-type primary-ni
mta receive maximum-recipients 0
!
!

```

```
controller E1 0
framing NO-CRC4
clock source line primary
pri-group timeslots 1-31 nfas_d primary nfas_int 0 nfas_group 0
!
controller E1 1
framing NO-CRC4
pri-group timeslots 1-31 nfas_d none nfas_int 1 nfas_group 0
!
controller E1 2
shutdown
framing NO-CRC4
clock source line secondary 1
pri-group timeslots 1-31 nfas_d none nfas_int 2 nfas_group 0
!
controller E1 3
shutdown
framing NO-CRC4
pri-group timeslots 1-31 nfas_d none nfas_int 3 nfas_group 0
!
!
!
!
interface Ethernet0
ip address 209.165.200.224 255.255.255.224
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Serial0:15
no ip address
ip helper-address 209.165.200.224
no ip directed-broadcast
no ip route-cache
isdn switch-type primary-ni
isdn incoming-voice modem
isdn rlm-group 1
no fair-queue
no cdp enable
!
interface FastEthernet0
ip address 209.165.200.224 255.255.255.224
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
duplex full
!
interface Group-Async1
description "Async Incoming Call"
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
async dynamic address
async mode interactive
no snmp trap link-status
no peer default ip address
no fair-queue
group-range 1 120
!
interface Dialer0
no ip address
no ip directed-broadcast
no cdp enable
```

```
!
router rip
redistribute connected
network 10.0.0.0
!
no ip classless
no ip http server
!
logging 10.15.0.130
!
dialer dnis group dnis1
number 9157181
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
snmp-server engineID local 00000009020000D00604FB36
snmp-server community public RO
snmp-server community RW
snmp-server trap-source FastEthernet0
snmp-server system-shutdown
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps voice poor-qov
snmp-server host 10.15.0.130 public
!
rlm version 2
!
rlm group 1
server xxxx
link hostname xxx source Ethernet0 weight 1
!
line con 0
exec-timeout 0 0
transport input none
line 1 120
logging synchronous level 7
modem InOut
transport preferred lat pad telnet rlogin udptn v120
transport input all
transport output pad telnet rlogin udptn v120
line aux 0
line vty 0 4
exec-timeout 0 0
password
login
!
ntp clock-period 17179771
ntp update-calendar
ntp server 10.15.0.1 source FastEthernet0
end
```



## Configuring Media Gateways for the SS7 Interconnect for Access Servers Solution

---

This chapter describes how to configure the access servers used by the Cisco SS7 Interconnect for Access Servers Solution. It includes the following sections:

- [Determining Software and Hardware Requirements, page 3-1](#)
- [Installing Media Gateways, page 3-1](#)
- [Configuring Media Gateways, page 3-3](#)
- [Sample Output for the Cisco SS7 Interconnect for Access Servers Solution, page 3-13](#)
- [Configuring Call Hairpinning on the Cisco AS5800, page 3-17](#)

### Determining Software and Hardware Requirements

Software and hardware requirements vary depending on the version of the Cisco SS7 Interconnect for Access Servers Solution installed in your network. To view the latest requirements for your solution, see the following online documentation:

- [Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2\(B\)](#)  
[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/das\\_rn.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/das_rn.htm)

### Installing Media Gateways

This document assumes that all required hardware has been installed, and that each access server has been configured for channelized T1 or E1 signaling and connected to a working IP network. If necessary, refer to the following sections:

- [Installing the Cisco AS5300 Universal Access Server, page 3-2](#)
- [Installing the Cisco AS5350 Universal Gateway, page 3-2](#)
- [Installing the Cisco AS5400 Universal Gateway, page 3-2](#)
- [Installing the Cisco AS5800 Universal Access Server, page 3-2](#)

## Installing the Cisco AS5300 Universal Access Server

For instructions on installing a Cisco AS5300 and connecting it to a network, see the following documents:

- *Cisco AS5300 Quick Start Guide (with Fast Step)*
- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*
- *Cisco AS5300 Software Configuration Guide*

The entire documentation set for the Cisco AS5300 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm)

## Installing the Cisco AS5350 Universal Gateway

For instructions on installing a Cisco AS5350 and connecting it to a network, see the following documents:

- *Cisco AS5350 Universal Gateway Chassis Installation Guide*
- *Cisco AS5350 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5350 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm)

## Installing the Cisco AS5400 Universal Gateway

For instructions on installing a Cisco AS5400 and connecting it to a network, see the following documents:

- *Cisco AS5400 Universal Access Gateway Read Me First*
- *Cisco AS5400 Chassis Installation Guide*
- *Cisco AS5400 Universal Gateway Card Installation Guide*
- *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*

The entire documentation set for the Cisco AS5400 universal gateway is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5400/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm)

## Installing the Cisco AS5800 Universal Access Server

For instructions on installing a Cisco AS5800 and connecting it to a network, see the following documents:

- *Read Me First—Cisco AS5800 Universal Access Server*
- *Cisco AS5800 OAM&P Guide*

- *Cisco AS5800 Universal Access Server Hardware Installation Guide*
- *Cisco AS5800 Universal Access Server Dial Shelf Guide*

The entire documentation set for the Cisco AS5800 universal access server is available at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm)

## Configuring Media Gateways

The process for configuring access servers includes the following major steps:

- [Preparing the Media Gateway for Configuration, page 3-3](#)
- [Setting the ISDN Switch Type, page 3-3](#)
- [Configuring Redundant Link Manager, page 3-4](#)
- [Configuring Resource Pool Manager \(RPM\), page 3-6](#)

## Preparing the Media Gateway for Configuration

Complete basic configuration for the media gateway. This includes, as a minimum, the following tasks:

- Configuring a host name and password for the media gateway
- Configuring the Ethernet 10BASE-T/100BASE-T interface of your media gateway so that it can be recognized as a device on the Ethernet LAN
- Configuring the media gateway interfaces for ISDN PRI lines

## Setting the ISDN Switch Type

To communicate with the Cisco SC2200, you must set the appropriate ISDN switch type on the media gateway. To set the ISDN switch type, perform the following steps:

---

**Step 1** Enter global configuration mode:

```
Router# configure terminal  
Router(config)#
```

**Step 2** Set the ISDN switch type to **primary-ni**:

```
Router# isdn switch-type primary-ni
```

For more information about setting ISDN switch types, refer to *National ISDN Switch Types for Basic Rate and Primary Rate Interfaces* at the following location;

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t\\_3/natisdn.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/natisdn.htm)

---

## Configuring Redundant Link Manager

The Cisco Redundant Link Manager (RLM) provides link management over multiple IP networks so that your Cisco SS7 solution can tolerate failure of a signaling controller or one of its components. A feature enhancement to RLM for the Cisco SS7 Interconnect for Access Servers Solution is redundancy at the link and signaling controller level (Version 2 below). When each RLM group has multiple signaling controllers associated with a Cisco MGW, a signaling controller priority and link priority are examined by the RLM client (RLM software on the Cisco MGW) during failover, ensuring improved control handling.

The RLM client supports both versions of RLM functionality:

- Multiple redundant links between a single signaling controller and the MGWs (Version 1)
- Multiple redundant links between multiple signaling controllers and the MGWs (Version 2)

Upon installation, the RLM version defaults to the latest version (Version 2). To configure a different RLM version, use the following global configuration command:

```
MGW# rlm version version id #
```



### Note

The RLM feature is backward compatible on the signaling controller, but only one version of the RLM client can run on a given Cisco MGW. Cisco recommends using Version 2.

For more detailed information, refer to *Redundant Link Manager* at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/rlm\\_123.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/rlm_123.htm)

To configure the RLM on the media gateway, perform the following steps:

**Step 1** To enter enable mode, enter the following commands:

```
Router> enable
Password: password
Router#
```

**Step 2** To enter global configuration mode, enter the following command:

```
Router# configure terminal
Router(config)#
```

**Step 3** To specify the IP address of the first interface, enter the following commands:

```
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.255.255.255
```



### Note

The IP addresses used in this book are for illustrative purposes only. Be sure to use IP addresses appropriate for your network.

**Step 4** To specify the IP address of the second interface, enter the following commands:

```
Router(config-if)# interface ethernet0
Router(config-if)# ip address 10.1.1.2 255.255.255.255
```



**Step 5** To specify the RLM group (MGW) that you want to configure, enter the following command:

```
Router(config-if)# rlm group 1
Router(config-rlm-group)#
```



**Note** The RLM group number must match the non-facility associated signaling (NFAS) group number.

**Step 6** To specify the device name, enter the following command:

```
Router(config-rlm-group)# server r1-server
```

**Step 7** To specify the link addresses and their weighting preference, enter the following commands:

```
Router(config-rlm-group-sc)# link address 10.1.4.1 source ethernet0 weight1
Router(config-rlm-group-sc)# link address 10.1.4.2 source ethernet0 weight2
```

**Step 8** Repeat [Step 6](#) and [Step 7](#) for the second device:

```
Router(config-rlm-group-sc)# server r2-server
Router(config-rlm-group-sc)# link address 10.1.5.1 source ethernet0 weight1
Router(config-rlm-group-sc)# link address 10.1.5.2 source ethernet0 weight2
```

**Step 9** To configure the enhanced interior gateway routing protocol (EIGRP), enter the following command:

```
Router(config-rlm-group-sc)# router eigrp 100
Router(config-router)#
```

**Step 10** To configure NFAS and specify the channels to be controlled by the primary NFAS D channel, enter **pri-group timeslots 1-24 nfas\_d primary nfas\_int 2 nfas\_group 0**

This command links the PRI bearer channels on the media gateway to the RLM group for D-channel communication to the signaling controller over IP. The `nfas_group` number represents one or more PRIs that are controlled by the same D-channel. The `int` number should be configured to match the T-1 controller number.

Some tips to remember when configuring NFAS are as follows:

- Multiple T1/E1s can be part of the same `nfas` group.
- Multiple NFAS groups within the same RLM group on the media gateway are not supported at this time.
- The `nfas_int` number should be unique and defines the D-channel.
- All PRIs have to be part of the one RLM group.

For more detailed information about configuring NFAS, refer to *NFAS with D Channel Back Up* at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t\\_3/nfas.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/nfas.htm)

## Verifying RLM Configuration

**Step 1** To verify the RLM configuration, enter the following command and specify the group number:

```
Router# show rlm group 0 status

RLM Group 0 Status
User/Port: RLM_MGR/3000 ISDN3001
```

```

Link State: Up          Last Link Status Reported: Up
Next tx TID: 1         Last rx TID: 0
Server Link Group[r1-server]:
  link [10.1.1.1(Ethernet0), 10.1.4.1] = socket[active]
  link [10.1.1.2(FastEthernet0), 10.1.4.2] = socket[standby]
Server Link Group[r2-server]:
  link [10.1.1.1(Ethernet0), 10.1.5.1] = socket[opening]
  link [10.1.1.2(FastEthernet0), 10.1.5.2] = socket[opening]

```

The link state must be up, and no errors should be reported.

**Step 2** To view layer status information, enter the following command:

```

Router# show isdn status

Global ISDN Switchtype = primary-ni
ISDN Serial1:23 interface
  dsl 0, interface ISDN Switchtype = primary-ni :Primary D channel of nfas group 0
  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)
    Activated dsl 0 CCBS = 0
ISDN Serial2:23 interface
  dsl 1, interface ISDN Switchtype = primary-ni :Group member of nfas group 0
  Layer 1 & 2 Status Not Applicable
  Layer 3 Status:
    0 Active Layer 3 Call(s)
    Activated dsl 1 CCBS = 0
    Total Allocated ISDN CCBS = 0

```

For Serial 0:23 (the first half of the message):

- Layer 1 Status should be ACTIVE.
- Layer 2 Status should be MULTIPLE\_FRAME\_ESTABLISHED. (It might take several seconds for Layer 2 status to appear.)
- Layer 3 Status should be 0 Active Layer 3 Calls.

The second half of the message displays information for Serial 1:23.



**Tip**

If the Layer 1 Status is Deactivated, it indicates a problem at the physical layer. Make sure that the cable connection is not loose or disconnected.

A Layer 2 error indicates that the Cisco MGW cannot communicate with the telco; there is a problem at the data link layer. There may be a problem with your telco, or the framing and line code types you entered may not match that of your telco.

## Configuring Resource Pool Manager (RPM)

Resource pool management allows service providers to provide wholesale (VPDN) dial service to corporate customers and retail dial service to end users from a single Cisco MGW or across multiple Cisco MGW stacks using one or more external Cisco Resource Pool Manager Servers (RPMS).

Cisco RPMS provides the following:

- Customer shared resource management.
- Advanced VPDN services for enterprise accounts and ISPs.
- Efficient use of resources to offer different oversubscription ratios and dial service agreements.
- Combination of retail and wholesale services on the same Cisco MGW.

Cisco RPMS offers three major functions:

- Resource management uses the call type and dialed number information service (DNIS) number to accept or reject the call based on the customer profile session limits associated with the DNIS number. If the call is accepted, the call is assigned to a media gateway resource.
- Dial services determines how the call is handled after it is answered. The call can be authenticated locally or sent to a home gateway through a VPDN tunnel (using the DNIS number or a domain name).
- Call discrimination prevents unapproved call types from accessing Cisco MGW resources. When a call is placed, the Cisco MGW sends the call type and (DNIS) to the Cisco RPMS. The Cisco RPMS compares this combination to the call discrimination table. If the call type/DNIS number combination appears in the table, it is rejected.

For detailed configuration, troubleshooting, and command reference information, see *Resource Pool Management* at the following location:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/rpm1205t.htm>

To configure RPM on your Cisco Media Gateway, perform the following steps:

---

**Step 1** To enable RPM, enter the following commands in configuration mode:

```
Router(config) # resource-pool {enable | disable}
Router(config) # resource-pool call treatment profile {busy | no-answer}
Router(config) # resource-pool call treatment resource {busy | channel-not-available}
Router(config) # resource-pool aaa protocol local
```




---

**Note** With RPM disabled, the resource groups still take effect (that is, modem pooling is still not possible). Also, local AAA is authorization and accounting for RPM.

---

**Step 2** To configure resource groups, enter the following commands:

```
Router(config) # resource-pool group resource WORD
Router(config) # range port s/s/p s/s/p
Router(config) # range limit limit
```

Note the following rules:

- Resource groups can apply to multiple customer profiles.
- You can separate the physical resources into groups.
- Do not mix MICA and Microcom modems.




---

**Note** For external Cisco RPMS environments, configure resource groups on the Cisco MGW before defining them on external RPMS servers. For standalone environments, configure resource groups before using them in customer profiles.

---

**Tip**

If you have an RPMS, you do not need to define VPDN groups/profiles, customer profiles, or DNIS groups on the media gateway—you need to define only resource groups. Configure the remaining items by using the RPMS system.

**Step 3** To configure DNIS groups, enter the following commands:

```
Router(config) # dialer dnis group {dnis-group-name}
Router(config) # call-type cas {digital | speech}
Router(config) # number number
```

Note the following:

- For default DNIS service, DNIS group configuration is not required.
- Each DNIS group or call type combination applies to one customer profile.
- Default DNIS groups can be used four times, one for each call type.
- You must statically configure CAS call types.
- You can use x, X, or . as a wildcard within each number.

**Step 4** To configure discriminator profiles, which enable you to process calls differently based on call type and DNIS combination, enter the following commands:

```
Router(config) # resource-pool profile discriminator WORD
Router(config) # call-type {all | digital | speech | v110 | v120}
Router(config) # dnis group {dnis-group-name | default}
```



**Note** You must specify both profiles.

**Step 5** To configure service profiles, enter the following commands:

```
Router(config) # resource-pool profile service WORD
Router(config) # modem {min-speed {speed | any}} {max-speed {speed | any}} [modulation
{k56flex | v22bis | v32bis | v32terbo | v34 | v90 | any}] [error-correction {mnp4 | lapm |
any | none}] [compression {mnp5 | v42bis | any | none}]
```

Note the following:

- Services apply only to MICA modems (speech or V.110).
- Error-correction and compression are hidden options.

**Step 6** To configure customer profiles, enter the following commands:

```
Router(config) # resource-pool profile customer WORD
Router(config) # dnis group {dnis-group-name | default}
Router(config) # limit base-size {number | all}
Router(config) # limit overflow-size {number | all}
Router(config) # resource WORD {digital | speech | v110 | v120} [service WORD]
```

Note the following:

- Multiple resources of the same call type are used sequentially.
- The limits imposed are per customer (DNIS)—not per resource.
- A digital resource with a call type of “speech” allows for Data over Speech Bearer Service (DOSBS).

**Step 7** To configure VPDN profiles, enter the following commands:

```
Router(config) # resource-pool profile customer WORD
```

```
Router(config) # vpdn profile profile-name
Router(config) # resource-pool profile vpdn profile-name
Router(config) # limit base-size {number | all}
Router(config) # limit overflow-size {number | all}
Router(config) # vpdn group group-name
```



**Note** A VPDN profile is required only if you want to impose limits on the VPDN tunnel that are separate from customer limits.

**Step 8** To configure VPDN groups, enter the following commands:

```
Router(config) # vpdn-group group-name
Router(config) # request dialin {12f | 12tp} ip A.B.C.D {dnis dnis-group-name | domain
Word}
Router(config) # multilink {link | bundle} number
Router(config) # loadsharing ip A.B.C.D [limit number]
Router(config) # backup ip A.B.C.D [limit number] [priority number]
```



**Note** The *dnis-group-name* is required to authorize the VPDN-group with the RPM. Also, this data is optional on the AAA server.

## RPM Configuration Examples

This section provides the following configuration examples:

- [Sample Configuration for Resource Pool Management](#)
- [Sample Customer Profile Configuration for Data-over-Voice Bearer Service](#)
- [Sample VPDN Configuration](#)

### Sample Configuration for Resource Pool Management

```
resource-pool enable
resource-pool call treatment resource busy
resource-pool call treatment profile no-answer
!
resource-pool group resource isdn-ports
range limit 46
resource-pool group resource MICA-modems
range port 1/0 2/23
!
resource-pool profile customer ACME
limit base-size 30
limit overflow-size 10
resource isdn-ports digital
resource MICA-modems speech service gold
dnis group ACME_dnis_numbers
```



**Note** Replace **resource isdn-ports digital** above with **resource isdn-ports speech** to set up DOVBS.

```
!
resource-pool profile customer DEFAULT
limit base-size 10
resource MICA-modems speech service silver
dnis group default
```

```

resource-pool profile discriminator deny_DNIS
  call-type digital
  dnis group bye-bye
!
resource-pool profile service gold
  modem min-speed 33200 max-speed 56000 modulation v90
resource-pool profile service silver
  modem min-speed 19200 max-speed 33200 modulation v34
!
resource-pool aaa protocol local
!
dialer dnis group ACME_dnis_numbers
  number 301001
dialer dnis group bye-bye
  number 301005

```

- Digital calls to 301001 are associated with the customer ACME by using the resource group isdn-ports.
- Speech calls to 301001 are associated with the customer ACME by using the resource group mica-modems and allow for V.90 connections (anything less than V.90 are also allowed).
- Digital calls to 301005 are denied.
- All other speech calls to any other DNIS number are associated with the customer profile DEFAULT. Using the resource group mica-modems allows for V.34 connections (anything more than V.34 is not allowed; anything less than V.34 is allowed).
- All other digital calls to any other DNIS number are not associated with a customer profile and are, therefore, not allowed.
- In this case, the customer profile named DEFAULT serves as the default customer profile for speech calls only. If the solution uses an external RPMS server, this same configuration can be used for backup resource pooling if communication is lost between the Cisco MGW and the RPMS.

### Sample Customer Profile Configuration for Data-over-Voice Bearer Service

To allow ISDN calls with a speech bearer capability to be directed to digital resources, make only the following change (highlighted in bold) to the configuration shown in the [“Sample Configuration for Resource Pool Management”](#) section on page 3-9:

```

resource-pool profile customer ACME
  limit base-size 30
  limit overflow-size 10
  resource isdn-ports speech
  dnis group ACME_dnis_numbers

```



#### Note

This change causes ISDN speech calls (in addition to ISDN digital calls) to be directed to the resource isdn-ports, thus providing DOVBS.

### Sample VPDN Configuration

The following command allows you to use VPDN by setting up a VPDN profile and a VPDN group:

```

resource-pool profile vpdn ACME_VPDN
  limit base-size 6
  limit overflow-size 0
  vpdn group outgoing-2
!
resource-pool profile customer ACME

```

```

limit base-size 30
limit overflow-size 10
resource isdn-ports digital
resource MICA-modems speech service gold
dnis group ACME_dnis_numbers
vpdn profile ACME_VPDN

vpdn enable
!
vpdn-group outgoing-2
 request dialin 12f ip 172.16.1.9 dnis ACME_dnis_numbers
 local name HQ-NAS
 multilink bundle 1
 multilink link 2
 dnis ACME_dnis_numbers
!
dialer dnis group ACME_dnis_numbers
 number 301001

```

**Note**

If the limits imposed by the VPDN profile are not required, do not configure the VPDN profile. Replace the command **vpdn profile ACME\_VPDN** under the customer profile ACME with the command **vpdn group outgoing-2**.

## Verifying the Configuration

To verify the configuration perform the following steps:

### Step 1 Enter **sh isdn nfas gr 0**.

```
ISDN NFAS GROUP 0 ENTRIES:
```

```

The primary D is Serial2:23.
The NFAS member is Serial3:23.

```

The example shown above indicates the primary D-channel interface and its associated members in the group. There are two total NFAS members. There are 48 total available B channels.

The primary D-channel is DSL 2 in the IN SERVICE state.

There is currently no backup D-channel configured.

The current active layer 2 DSL is 2.

### Step 2 Enter **sh isdn stat** to show the status:

```

ISDN Serial2:23 interface          rlm-group = 0
    dsl 2, interface ISDN Switchtype = primary-ni : Primary D channel of nfas group 0
Layer 1 Status:
    ACTIVE
Layer 2 Status:
    TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    I_Queue_Len 0, UI_Queue_Len 0
Layer 3 Status:
    0 Active Layer 3 Call(s)
Activated dsl 2 CCBS = 0
The Free Channel Mask: 0x80FFFFFF
ISDN Serial3:23 interface
    dsl 3, interface ISDN Switchtype = primary-ni : Group member of nfas group 0

```

```

Layer 1 Status:
ACTIVE
Layer 2 Status: Not Applicable
Layer 3 Status:
  0 Active Layer 3 Call(s)
  Activated dsl 3 CCBS = 0

```

**Step 3 Enter `sh rlm gro 0`.**

The presence of two signaling controllers shown below, indicates redundancy in the case of failover. This step is optional.

```

RLM Group 0 Status
User/Port: RLM_MGR/3000 ISDN/3001
RLM Version : 2
Link State: Up          Last Link Status Reported: Up
Next tx TID: 1         Last rx TID: 0
Server Link Group[carteret]: Last Reported Priority: HIGH
  link [10.15.12.2(Ethernet0), 10.15.12.134] = socket[standby]
  link [10.15.12.34(FastEthernet0), 10.15.12.150] = socket[standby]
Server Link Group[yaupon]: Last Reported Priority: HIGH
  link [10.15.12.2(Ethernet0), 10.15.12.135] = socket[active]
  link [10.15.12.34(FastEthernet0), 10.15.12.151] = socket[standby]

```

This is the interface that call signaling will traverse.

```

RLM Group 0 Timer Values
open_wait   = 3s           force-down   = 30s
recovery    = 12s          switch-link  = 5s
minimum-up  = 60s          retransmit   = 1s
keepalive   = 1s

```

```

RLM Group 0 Statistics
Link_up:
  last time occurred at Nov 18 10:57:43.992, total transition=59
  avg=06:36:36.298, max=2d22h, min=00:00:00.000, latest=00:00:04.844
Link_down:
  last time occurred at Nov 18 10:57:10.992, total transition=28
  avg=00:56:54.621, max=1d00h, min=00:00:00.000, latest=00:00:33.000
Link_recovered:
  last time occurred at Nov 18 10:56:58.992, success=25(49%), failure=26
  avg=0.038s, max=0.224s, min=0.000s, latest=0.000s
Link_switched:
  last time occurred at Nov 11 12:25:52.324, success=6(100%), failure=0
  avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
Server_changed:
  last time occurred at Nov 18 10:56:54.148 for totally 29 times
Server Link Group[carteret]:
  Open the link [10.15.12.2(Ethernet0), 10.15.12.134]:
    last time occurred at Nov 18 10:57:40.992, success=33(6%), failure=509-0
    avg=43.634s, max=177.004s, min=0.000s, latest=0.000s
  Echo over link [10.15.12.2(Ethernet0), 10.15.12.134]:
    last time occurred at Nov 18 11:12:40.979, success=1355251(97%), failure=33527-0
    avg=0.000s, max=0.964s, min=0.000s, latest=0.000s
  Open the link [10.15.12.34(FastEthernet0), 10.15.12.150]:
    last time occurred at Nov 18 10:57:40.992, success=33(6%), failure=509-0
    avg=43.549s, max=177.004s, min=0.000s, latest=0.000s
  Echo over link [10.15.12.34(FastEthernet0), 10.15.12.150]:
    last time occurred at Nov 18 11:12:40.979, success=1378593(97%), failure=32887-0
    avg=0.000s, max=0.960s, min=0.000s, latest=0.000s
Server Link Group[yaupon]:
  Open the link [10.15.12.2(Ethernet0), 10.15.12.135]:
    last time occurred at Nov 18 10:57:40.992, success=35(1%), failure=2247-0
    avg=61.347s, max=177.000s, min=0.000s, latest=0.004s

```



```

Echo over link [10.15.12.2(Ethernet0), 10.15.12.135]:
  last time occurred at Nov 18 11:12:41.983, success=998740(87%), failure=139142-0
  avg=0.000s, max=2.688s, min=0.000s, latest=0.004s
Open the link [10.15.12.34(FastEthernet0), 10.15.12.151]:
  last time occurred at Nov 18 10:57:40.992, success=35(1%), failure=2247-0
  avg=61.270s, max=177.000s, min=0.000s, latest=0.032s
Echo over link [10.15.12.34(FastEthernet0), 10.15.12.151]:
  last time occurred at Nov 18 11:12:42.019, success=1059514(88%), failure=138872-0
  avg=0.000s, max=2.688s, min=0.000s, latest=0.016s

```

## Sample Output for the Cisco SS7 Interconnect for Access Servers Solution

The following section contains sample output from an media gateway that has been configured for the Cisco SS7 Interconnect for Access Servers Solution

```

version 12.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname pppl-1.os1
!
boot system flash c5300-js-mz.121-5.bin
boot system flash bootflash:
logging console emergencies
!
username admin privilege 15 password 7 <---- Removed ---->
username pppl.os password 7 <---- Removed ---->
spe 1/0 2/9
  firmware location flash:/mica-modem-pw.2.7.1.0.bin
!
!
resource-pool disable
!
!
!
!
!
clock timezone MET 1
clock summer-time MET-DST recurring last Sun Mar 2:00 last Sun Oct 3:00
modem country mica norway
ip subnet-zero
no ip finger
ip domain-list world-online.no
ip name-server 10.2.64.170
ip name-server 10.2.64.171
!
ip cef
!
async-bootp nbns-server 0.0.0.0
vty-async
vty-async virtual-template 1
isdn switch-type primary-ni
isdn voice-call-failure 0
cns event-service server
mta receive maximum-recipients 0
!

```

```

!
controller E1 0
  framing NO-CRC4
  clock source line primary
  pri-group timeslots 1-31 nfas_d primary nfas_int 1 nfas_group 0
!
controller E1 1
  framing NO-CRC4
  clock source line secondary 1
  pri-group timeslots 1-31 nfas_d none nfas_int 2 nfas_group 0
!
controller E1 2
  framing NO-CRC4
  clock source line secondary 2
  pri-group timeslots 1-31 nfas_d none nfas_int 3 nfas_group 0
!
controller E1 3
  framing NO-CRC4
  clock source line secondary 3
  pri-group timeslots 1-31 nfas_d none nfas_int 4 nfas_group 0
!
!
!
!
interface Ethernet0
  ip address 10.0.1.17 255.255.255.192
  no ip mroute-cache
  no cdp enable
!
interface Virtual-Template1
  ip unnumbered FastEthernet0
  ip verify unicast reverse-path
  no logging event link-status
  peer default ip address pool ippool
  compress stac
  ppp authentication pap callin modemaauthen
  ppp accounting modemaccount
  ppp multilink bap
  ppp bap call accept
  ppp bap timeout pending 20
!
interface Serial0
  no ip address
  no ip mroute-cache
  no fair-queue
  clockrate 2015232
  no cdp enable
!
interface Serial1
  no ip address
  no ip mroute-cache
  no fair-queue
  clockrate 2015232
  no cdp enable
!
interface Serial2
  no ip address
  no ip mroute-cache
  no fair-queue
  clockrate 2015232
  no cdp enable
!
interface Serial3
  no ip address

```

```
no ip mroute-cache
no fair-queue
clockrate 2015232
no cdp enable
!
interface Serial0:15
no ip address
encapsulation ppp
no ip route-cache cef
dialer rotary-group 1
autodetect encapsulation ppp v120
isdn switch-type primary-ni
isdn incoming-voice modem
isdn T203 10000
isdn rlm-group 0
no isdn send-status-enquiry
compress stac
no cdp enable
!
interface FastEthernet0
ip address 10.2.67.17 255.255.255.192
ip access-group snmp-filter in
ip access-group ppp-martians-out out
ip route-cache flow
ip summary-address eigrp 900 10.2.73.0 255.255.255.128 5
no ip mroute-cache
duplex full
speed auto
no cdp enable
no mop enabled
!
interface Group-Async1
ip unnumbered FastEthernet0
ip verify unicast reverse-path
encapsulation ppp
no ip mroute-cache
no logging event link-status
dialer in-band
dialer idle-timeout 7200
dialer-group 1
async mode dedicated
peer default ip address pool ippool
compress stac
no cdp enable
ppp max-bad-auth 3
ppp authentication pap callin modemaauthen
ppp accounting modemaccount
group-range 1 120
!
interface Dialer1
ip unnumbered FastEthernet0
ip verify unicast reverse-path
encapsulation ppp
no ip mroute-cache
no logging event link-status
no keepalive
dialer in-band
dialer idle-timeout 7200
dialer-group 1
peer default ip address pool ippool
compress stac
no cdp enable
ppp max-bad-auth 3
ppp authentication pap callin modemaauthen
```

```

ppp accounting modemaccount
ppp multilink bap
ppp timeout retry 1
ppp timeout authentication 1
ppp bap call accept
no ppp bap drop request
no ppp bap timeout pending
no ppp bap monitor load
!
!
ip local pool ippool 10.2.73.1 10.2.73.127
ip classless
ip route 10.0.2.0 255.255.255.192 10.0.1.1
ip route 10.2.66.10 255.255.255.254 10.2.67.1
ip tacacs source-interface FastEthernet0
no ip http server
!
!
dialer-list 1 protocol ip permit
no cdp run
!
tacacs-server host 10.2.64.147
tacacs-server host 10.2.64.146
tacacs-server key <---- Removed ---->
snmp-server engineID local 000000090200003080BD3C8C
snmp-server community <---- Removed ----> RO
snmp-server community <---- Removed ----> RO
!
!
rlm group 0
server sc000
  link address 10.2.66.12 source FastEthernet0 weight 3
  link address 10.0.2.12 source Ethernet0 weight 4
server sc010
  link address 10.2.66.13 source FastEthernet0 weight 1
  link address 10.0.2.13 source Ethernet0 weight 2
alias exec u undeb all
!
line con 0
  exec-timeout 0 0
  login authentication xTY
  transport input none
line 1 120
  no flush-at-activation
  modem InOut
  modem autoconfigure type mica
  autocommand ppp
  transport input all
  transport output pad telnet rlogin udptn v120 lapb-ta
line aux 0
  password 7 <---- Removed ---->
line vty 0 4
  access-class 1 in
  exec-timeout 0 0
  password 7 <---- Removed ---->
  transport input telnet
  escape-character 3
line vty 5 124
  autocommand ppp nego
  transport input v120
!

```

```
ntp clock-period 17180014
ntp update-calendar
ntp server 10.2.64.146
end
```

## Configuring Call Hairpinning on the Cisco AS5800

The hairpinning feature takes an incoming call and forwards the call out from the access server to another device, such as a voice switch or voice terminal. This is done without affecting the calling customer's experience. An incoming call is matched against configured dial peers, and based on the configured called number, the outgoing interface is selected. The call is sent out through a circuit-switched connection through the access server. No Cisco AS5800 modems or DSPs are involved, although a circuit is established through the access server.



---

**Note** Hairpinning is supported only on the Cisco AS5800.

---



---

**Note** Hairpinning requires the MICA plane.

---

## Call Switching Using Dial Peers

Call switching using dial peers enables the Cisco AS5800 to switch both voice and data calls between different interfaces based on the dial peer matching. An incoming call is matched against configured dial peers, and based on the configured called number, the outgoing interface is selected. Any call that arrives from the PSTN is either terminated on the access server or switched back to the PSTN, depending on the configuration.



---

**Note** An incoming call will be hairpinned back to the PSTN only if it matches a dial peer.

---

A dial peer is an addressable call endpoint identified, for example, by a phone number or a port number. Dial peers are defined from the perspective of the access server and are used for both inbound and outbound call legs. An *inbound* call leg originates outside the access server. An *outbound* call leg originates from the access server.

For inbound call legs, a dial peer might be associated with the calling number or the port designation. Outbound call legs always have a dial peer associated with them. The destination pattern (a defined initial part of a phone number) is used to identify the outbound dial peer. The call is associated with the outbound dial peer at setup time.

POTS dial peers associate a telephone number with a particular voice port so that incoming calls for that telephone number can be received and outgoing calls can be placed.

## Using Class of Restrictions

The Class of Restrictions (COR) functionality provides the ability to deny certain call attempts based on the incoming and outgoing class of restrictions provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, to 900 numbers), and applies different restrictions to call attempts from different originators.

COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. The incoming COR list indicates the capability of the dial peer to initiate certain classes of calls. The outgoing COR list indicates the capability required for an incoming dial peer to deliver a call via this outgoing dial peer. If the capabilities of the incoming dial peer are not the same or a superset of the capabilities required by the outgoing dial peer, the call cannot be completed using this outgoing dial peer.



**Note** The use of COR is not required for call hairpinning.


## Call Hairpinning Configuration Tasks

To configure call hairpinning on the Cisco AS5800, refer to the following sections:

- [Configuring Global or Interface Trunk Groups, page 3-18](#)
- [Configuring Dial Peer Classes of Restrictions, page 3-19](#)

### Configuring Global or Interface Trunk Groups




You can create trunk groups globally (using the one-command version of Step 1) or on each interface (using the two-command version of Step 1). To configure trunk groups, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	<pre>Router(config)# trunk group group-number</pre> <p>or</p> <pre>Router(config-if)# interface serial0/0/n</pre> <p>and</p> <pre>Router(config-if)# trunk-group group-number</pre>	<p>Defines the trunk group globally.</p> <p>Specifies the PRI D-channel. For <i>n</i>, the D-channel number, use:</p> <ul style="list-style-type: none"> <li>• <b>0:23</b> on a T1 PRI</li> <li>• <b>0:15</b> on an E1 PRI</li> </ul> <p>Adds the interface to a trunk group. If the trunk group has not been defined globally, it will be created now.</p>
<b>Step 2</b>	<pre>Router(config-if)# max-calls {voice   data   any} number [direction in   out]</pre>	<p>Applies a maximum number of calls restriction to the trunk group.</p> <p>This command can be repeated to apply a maximum number to different types of calls and, optionally, to specify whether the maximum applies to incoming or outgoing calls.</p> <p> <b>Note</b> Repeat <a href="#">Step 1</a> and <a href="#">Step 2</a> to create additional trunk groups and specify their restrictions, as needed for your traffic.</p>

	Command	Purpose
Step 3	Router(config)# <b>dial-peer voice tag pots</b>	Enters dial-peer configuration mode and defines a remote dial peer.
Step 4	Router(config-dial-peer)# <b>trunkgroup group-number</b>	Specifies the trunk group to be used for outgoing calls to the destination phone number.

## Configuring Dial Peer Classes of Restrictions

To configure classes of restrictions for dial peers, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>dial-peer cor custom</b>	Specifies that named classes of restrictions apply to dial peers.
Step 2	Router(config-cor)# <b>name class-name</b>	Provides a name for a custom class of restrictions.   <b>Note</b> Repeat this step for additional class names, as needed. These class names are used in various combinations to define the lists in Step 3 and Step 4.
Step 3	Router(config)# <b>dial-peer cor list list-name</b>	Provides a name for a list of restrictions.
Step 4	Router(config-cor)# <b>member class-name</b>	Adds a COR class to this list of restrictions. The member is a class named in Step 2.   <b>Note</b> Repeat <a href="#">Step 3</a> and <a href="#">Step 4</a> to define another list and its membership, as needed.
Step 5	Router(config)# <b>dial-peer voice tag pots</b>	Enters dial-peer configuration mode and defines a remote dial peer.
Step 6	Router(config-dial-peer)# <b>corlist incoming cor-list-name</b>	Specifies the COR list to be used when this is the incoming dial peer.
Step 7	Router(config-dial-peer)# <b>corlist outgoing cor-list-name</b>	Specifies the COR list to be used when this is the outgoing dial peer.   <b>Note</b> Repeat <a href="#">Step 5</a> through <a href="#">Step 7</a> for additional dial peers, as needed.

## Complete Dial Plan Setup for Hairpinning

This example represents a complete dial-plan configuration for hairpinning on the Cisco AS5800:

```

!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname nas-pop1
!
boot bootldr slot0:c5800-p4-mz.0.3.0
no logging buffered
no logging buffered
logging rate-limit console 10 except errors
enable password letmein
!
username user_T password 0 cisco
username user_B password 0 cisco
username nas-pstn password 0 cisco
username callgen-term password 0 cisco
username nas-pop1 password 0 cisco
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 MST -7
!
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
isdn switch-type primary-ni
isdn voice-call-failure 0
call rsvp-sync
!
!
controller E1 1/0/0
  pri-group timeslots 1-31 nfas_d primary nfas_int 0 nfas_group 1
!
controller E1 1/0/1
  pri-group timeslots 1-31 nfas_d none nfas_int 1 nfas_group 1
!
controller E1 1/0/2
  pri-group timeslots 1-31 nfas_d none nfas_int 2 nfas_group 1
!
controller E1 1/0/3
  pri-group timeslots 1-31 nfas_d none nfas_int 3 nfas_group 1
!
controller E1 1/0/4
  pri-group timeslots 1-31 nfas_d none nfas_int 4 nfas_group 1
!
controller E1 1/0/5
  pri-group timeslots 1-31 nfas_d none nfas_int 5 nfas_group 1
!

```



```
controller E1 1/0/6
  pri-group timeslots 1-31 nfas_d none nfas_int 6 nfas_group 1
!
controller E1 1/0/7
  pri-group timeslots 1-31 nfas_d none nfas_int 7 nfas_group 1
!
controller E1 1/0/8
  pri-group timeslots 1-31
!
controller E1 1/0/9
  pri-group timeslots 1-31
!
controller E1 1/0/10
  pri-group timeslots 1-31
!
controller E1 1/0/11
  pri-group timeslots 1-31
!
controller T1 1/1/0
!
controller T1 1/1/1
!
controller T1 1/1/2
!
controller T1 1/1/3
!
controller T1 1/1/4
!
controller T1 1/1/5
!
controller T1 1/1/6
!
controller T1 1/1/7
!
controller T1 1/1/8
!
controller T1 1/1/9
!
controller T1 1/1/10
!
controller T1 1/1/11
!
!
interface Loopback0
  ip address 192.168.111.1 255.255.255.255
  ip broadcast-address 192.168.111.1
  no ip route-cache
  no ip mroute-cache
!
interface Loopback1
  no ip address
!
interface FastEthernet0/0/0
  ip address 10.10.7.10 255.255.255.0
  ip broadcast-address 10.10.7.255
  no ip route-cache
  no ip mroute-cache
  logging event link-status
  duplex full
!
interface FastEthernet0/1/0
  ip address 10.10.8.10 255.255.255.0
  ip broadcast-address 10.10.8.255
  no ip route-cache
```

```

no ip mroute-cache
duplex full
!
interface Serial1/0/0:15
ip unnumbered Loopback0
encapsulation ppp
ip mroute-cache
no keepalive
dialer hold-queue 1
dialer-group 1
isdn switch-type primary-ni
isdn incoming-voice modem
isdn rlm-group 1
no isdn send-status-enquiry
isdn bchan-number-order ascending
ppp authentication chap
!
interface Serial1/0/8:15
no ip address
isdn switch-type primary-ni
isdn protocol-emulate network
isdn calling-number 5800-ch8
no isdn T309-enable
isdn bchan-number-order ascending
trunk-group 101
no cdp enable
!
interface Serial1/0/9:15
no ip address
isdn switch-type primary-ni
isdn protocol-emulate network
isdn calling-number 5800-ch9
no isdn T309-enable
isdn bchan-number-order ascending
trunk-group 101
no cdp enable
!
interface Serial1/0/10:15
no ip address
isdn switch-type primary-ni
isdn protocol-emulate network
isdn calling-number 5800-ch10
no isdn T309-enable
isdn bchan-number-order ascending
trunk-group 101
no cdp enable
!
interface Serial1/0/11:15
no ip address
isdn switch-type primary-ni
isdn protocol-emulate network
isdn calling-number 5800-ch11
no isdn T309-enable
isdn bchan-number-order ascending
trunk-group 101
no cdp enable
!
interface Group-Async0
ip unnumbered Loopback0
no ip proxy-arp
encapsulation ppp
ip tcp header-compression passive
no ip mroute-cache
logging event link-status

```

```
dialer in-band
dialer-group 1
async default routing
async dynamic address
async mode dedicated
no peer default ip address
ppp authentication chap
group-range 1/2/00 1/3/143
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.8.1
ip route 192.168.65.0 255.255.255.0 10.10.8.5
ip route 192.168.100.0 255.255.255.0 10.10.8.5
no ip http server
!
no logging trap
logging facility local0
logging 10.1.1.5
snmp-server engineID local 000000090200000217C46400
snmp-server community public RO
snmp-server community lab RW
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps calltracker
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps aaa_server
snmp-server enable traps syslog
snmp-server enable traps ipmulticast
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps ipdc
snmp-server enable traps bgp
snmp-server enable traps voice poor-qov
snmp-server host 10.10.8.100 public
!
!
rlm group 1
server sc2200b
link address 10.10.7.20 source FastEthernet0/0/0 weight 100
!
!
trunk group 101
!
voice-port 1/0/0:D
!
voice-port 1/0/8:D
!
voice-port 1/0/9:D
!
voice-port 1/0/10:D
!
voice-port 1/0/11:D
!
dial-peer cor custom
name 800_call
name 900block
```

```

    name 888_call
    !
    !
dial-peer cor list list1
    member 800_call
    !
dial-peer cor list list2
    member 888_call
    !
    !
dial-peer voice 1 pots
    corlist incoming list1
    trunkgroup 101
    destination-pattern 1800.....
    no digit-strip
    direct-inward-dial
    prefix 1800
    !
dial-peer voice 2 pots
    corlist incoming list2
    trunkgroup 101
    destination-pattern 1888.....
    no digit-strip
    direct-inward-dial
    prefix 1888
    !
    !
line con 0
    session-timeout 5
    transport input none
line aux 0
line vty 0 4
    exec-timeout 0 0
    password letmein
    login
line vty 5 9
    password letmein
    login
line 1/2/00 1/2/143
    activation-character 0
    disconnect-character 0
    modem InOut
    no modem log rs232
    escape-character soft 0
    escape-character 0
    autohangup
    hold-character 0
line 1/3/00 1/3/143
    activation-character 0
    disconnect-character 0
    modem InOut
    no modem log rs232
    escape-character soft 0
    escape-character 0
    autohangup
    hold-character 0
    !
ntp update-calendar
ntp peer 172.20.144.245

```



## Upgrading Cisco Media Gateway Software

---

This chapter describes procedures for upgrading software on Cisco network access servers (NAS). It contains the following sections:

- [Determining Your Cisco IOS Version, page 4-1](#)
- [Determining Memory Requirements, page 4-1](#)
- [Upgrading the Cisco AS5300 Universal Access Server, page 4-2](#)
- [Upgrading the Cisco AS5350 or Cisco AS5400 Universal Gateway, page 4-4](#)
- [Upgrading the Cisco AS5800 Universal Access Server, page 4-6](#)

For detailed information about obtaining and managing Cisco IOS images, refer to [Appendix B, “Managing Cisco Media Gateway Software.”](#)

### Determining Your Cisco IOS Version

To determine the version of Cisco IOS software running on your NAS, log in to the Cisco AS5X00 and enter the **show version EXEC** command:

```
AS5300> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software c5300-i-mz, Version 12.1(2), RELEASE SOFTWARE
```

### Determining Memory Requirements

The amount of memory required by a Cisco IOS image depends on the platform and the SS7 Interconnect Solution that the platform supports. To determine the latest memory requirements, refer to the following online documents:

- [Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2\(B\)](#)
- [Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3](#)

# Upgrading the Cisco AS5300 Universal Access Server

The Cisco AS5300 Universal Access Server will not allow the Flash to be overwritten during normal operation. You need to configure your router to boot up from boot Flash (or ROM) so you can copy the upgraded version of Cisco IOS Software into the regular system Flash.

## Blocking Voice Gateway Circuits

Cisco AS5300s that use H.225 Resource Availability Indicator (RAI) to load-share VoIP traffic with other voice gateways require special preparation before you can place them out of service. You must block the appropriate circuits on the Cisco SC2200 and wait for in-progress calls to disconnect on the affected Cisco AS5300. Doing so will cause the NAS to send a “resource unavailable” message to the local H.323 gatekeeper, which will then route calls only to the remaining Cisco AS5300s.



### Note

This procedure is required only for the Cisco SS7 Interconnect for Voice Gateways Solution in environments where H.225 RAI is used to share egress traffic among multiple Cisco AS5300s.

Complete the following steps before placing the Cisco AS5300 out of service:

- Step 1** On the Cisco SC2200, block the circuits that terminate on the NAS.

```
SC2200 mml> blk-cic:point code:CIC=circuit identification code,RNG=CIC+range
```



### Note

For more information on MML commands, refer to *MML Command Reference* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/sw\\_ref/elmmmlref.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/sw_ref/elmmmlref.htm)

- Step 2** When all in-progress calls have disconnected, disable the loopback interface on the NAS. H.323-id and gatekeeper information is contained in the loopback interface, and disabling this interface will cause the NAS to unregister with the local gatekeeper.

```
AS5300(config)# interface loopback 0
AS5300(config)# shutdown
```

- Step 3** Save the configuration of the NAS. This command will prevent the NAS from re-registering with the gatekeeper until Redundant Link Manager (RLM) and all ISDN channels have initialized. The NAS is now ready to be shut down.



```
AS5300# write memory
```

## Loading a Cisco IOS Upgrade on the Cisco AS5300

Complete the following steps to upgrade the Cisco IOS Software on a Cisco AS5300:

- Step 1** Back up the boot Flash memory.

```
AS5300# copy bootflash tftp
```

- Step 2** Back up the Flash memory.
- ```
AS5300# copy flash tftp
```
- Step 3** Back up your configuration. Be sure to use a distinct name for the startup configuration for each of your Cisco AS5300s.
- ```
AS5300# copy startup-config tftp
```
- Step 4** Change the configuration register from its current setting to 0x2101 so that the Cisco AS5300 boots from boot Flash memory. Be sure to enter the **show version** command and take note of the current configuration register settings.
- ```
AS5300# show version
AS5300# configure terminal
AS5300(config)# config-reg 0x2101
AS5300(config)# exit
AS5300#
```
- Step 5** Reload the Cisco AS5300.
- ```
AS5300# reload
```
- Step 6** Copy the Cisco IOS software to Flash memory.
- ```
AS5300(boot)# copy tftp flash
```
- Step 7** Change the configuration register back to its original setting so that the Cisco AS5300 boots from Flash. In this example, the original setting was 0x2102.
- ```
AS5300(boot)# configure terminal
AS5300(config)# config-reg 0x2102
AS5300(config)# exit
AS5300(boot)#
```
- Step 8** Reload the Cisco AS5300.
- ```
AS5300(boot)# reload
```
-  **Note** Do not save the configuration at this time.
- 
- Step 9** Confirm the software upgrade.
- ```
AS5300# show version
```
-  **Note** Complete [Step 10](#) through [Step 13](#) only if your network uses H.225 RAI to load-share VoIP traffic among multiple Cisco AS5300s.
- 
- Step 10** Verify that the Redundant Link Manager (RLM) is operational.
- ```
AS5300# show rlm group 1 status
```
- Step 11** Verify that all ISDN channels on the NAS show “maintenance pending.”
- ```
AS5300# show isdn service
```
- Step 12** On the Cisco SC2200, unblock the circuits that terminate on the NAS.
- ```
SC2200 mm1> unblk-cic:point code:CIC=circuit identification code,RNG=CIC+range
```
- Step 13** Enable the loopback interface on the NAS. The NAS will re-register with the gatekeeper and begin processing calls.

```
AS5300(config)# interface loopback 0
AS5300(config)# no shut
```

## Upgrading Cisco VCWare

Cisco VCware is a software image that runs only on voice cards used in the Cisco AS5300. Because Cisco VCWare is a separate image from Cisco IOS Software, it must be loaded and upgraded separately from Cisco IOS Software. For all other Cisco voice gateways using C54x series DSPs, the DSPware is embedded in the Cisco IOS Software image, so in those systems, Cisco VCware is not used. For instructions on upgrading Cisco VCWare, refer to *Release Notes for Cisco VCWare on Cisco AS5300 Universal Access Servers* at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/sw\\_conf/vcw\\_rn/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/vcw_rn/index.htm)

## Upgrading the Cisco AS5350 or Cisco AS5400 Universal Gateway

Complete the following steps to upgrade the Cisco IOS software on a Cisco AS5350 or Cisco AS5400 universal access gateway:

### Step 1 Display the contents of Flash memory:

```
Router# cd flash:
Router# dir
Directory of flash:/

 1  -rw-      9950528   Jan 01 2000 00:48:59  c5350-js-mz.121-1.XD1.bin

32768000 bytes total (13041600 bytes free)
```

### Step 2 Copy the new image from the remote TFTP server into Flash memory. Make sure that you specify your own TFTP server's IP address and Cisco IOS filename. If you encounter issues with upgrading the image, be sure that you can ping the TFTP server and that appropriate directory permissions are configured on the TFTP server. To see the bangs (!) during the download operation, enable line wrap in your terminal emulation software.



**Note** If you have available space for two images, leave both images in Flash memory. If necessary, you can easily revert back to the previous image. Enter the **boot system flash newiosname.bin** command to point to the new image filename. By default, the first image in Flash memory is loaded.

If you do not have available space, during the copy operation the system displays a message telling you to delete the current file and squeeze the flash to make room for the new image. Enter the **delete flash:version** command, followed by the **squeeze flash** command, to perform this delete-and-squeeze operation. Then proceed with the copy operation.

```
Router# copy tftp flash
Address or name of remote host [172.22.191.135]? 172.22.191.135
Source filename [c5350-js-mz.121-1.XD1.bin]? c5350-js-mz.121-3.T.bin
Destination filename [c5350-js-mz.121-3.T.bin]?
```



```

Accessing tftp://172.22.191.135/c5350-js-mz.121-3.T.bin...
Loading c5350-js-mz.121-3.T.bin from 172.22.191.135 (via FastEthernet0/0): !!!!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
[OK - 9775616/19551232 bytes]

9775616 bytes copied in 66.424 secs (148115 bytes/sec)

```

**Caution**

Occasionally TFTP errors occur. Make sure that the verifying checksum reports “OK.” Do *not* reload the gateway if the checksum reports errors.

**Step 3**

Verify that the new image was downloaded. In this example, notice that the Cisco IOS Release 12.1(1)XD image is the first in Flash memory, so it is loaded during the boot sequence. To boot using the new image, you must either delete the unwanted image or use the **boot system** command to specify the alternate image to use during the boot sequence.

```

Router# dir flash:
Directory of flash:/

 1  -rw-      9950528   Jan 01 2000 00:48:59  c5350-js-mz.121-1.XD1.bin
 2  -rw-      9775616   Jan 01 2000 00:59:10  c5350-js-mz.121-3.T.bin

32768000 bytes total (13041600 bytes free)

```

For more information on deleting the image, refer to the document *Cisco IOS File System*, available online at

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa\\_2/allplats/ifs.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_2/allplats/ifs.htm)

**Note**

The Cisco AS5350 and Cisco AS5400, unlike the Cisco AS5200 and Cisco AS5300, use a Class A Flash File System.

**Step 4**

To specify the alternate image that is to be used during the boot sequence use the **boot system flash newiosname.bin** command to specify the location (device) and name of the image to be used:

```

Router(config)# boot system flash c5350-js-mz.121-3.T.bin
Router(config)# ^Z
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

To verify that this command is in effect, use the **show running-configuration** command. Save your running configuration before the reload so that the gateway loads the correct image.

**Step 5**

Reload the Cisco AS5350 or Cisco AS5400 to run the new image. If you erased the old Cisco IOS image, make sure that the **boot system flash oldiosname.bin** command is not enabled and pointing to the old image file name; otherwise, the gateway gets stuck trying to reload the old image over and over again.

```

Router# reload
Proceed with reload? [confirm]

System Bootstrap, Version 12.0(20000106:234457) [tombnyg-rommon_1_6 106],
SOFTWARE REV 1.6
Copyright (c) 1994-2000 by cisco Systems, Inc.
AS5400 platform with 131072 Kbytes of main memory

```

```

Self decompressing the image : #####
##### [OK]
Self decompressing the image : #####
#####
#####
#####
#####
##### [OK]
Press RETURN to get started!

```



**Note** Most sections of the boot sequence have been omitted from the example.



**Tips**

On system reload, if the console session freezes or displays unusual characters on the screen, you may have a console session mismatch between the Cisco IOS console line speed and the terminal server speed. This mismatch may occur because of the program settings of your console or your terminal server speed.

## Upgrading the Cisco AS5800 Universal Access Server

### Backing Up Your AS5800 Configuration

Cisco recommends backing up all existing IOS images and configurations from privileged exec mode.



**Note**

Backup current IOS images (boot, router-shelf, dial-shelf), and configurations, to a TFTP server prior to upgrading. By default, files are copied to and from the Cisco TFTP root directory.

- Step 1** Backup your existing startup configuration. Use a distinct file name for the startup configuration. This makes it easy to distinguish from other startup configurations previously saved on your TFTP Server.

```

AS5800# copy startup-config tftp
Address or name of remote host []? 171.71.219.167
Destination filename [startup-config]? AS5800-startup
!!
3449 bytes copied in 0.136 secs

```

- Step 2** Backup your existing running configuration. Use a distinct file name for the running configuration. This makes it easy to distinguish from other running configurations previously saved on your TFTP Server.

```

AS5800# copy running-config tftp
Address or name of remote host []? 171.71.219.167
Destination filename [running-config]? AS5800-running-config
!!
3312 bytes copied in 0.140 secs

```

**Step 3** Save your running-configuration to your startup configuration in NVRAM.

```
Router# copy running-configuration start-up configuration
```



**Note** Do not modify your running configuration during the IOS upgrade process.

**Step 4** Determine the current boot image.

```
AS5800# sh bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image AC05EDDF 37A6B8 22 3384888 Dec 31 1999 18:08:09 c7200-boot-mz.120-4.XE
```

**Step 5** Backup the boot image (c7200-boot-mz.XXX) from bootflash to the TFTP server. Use the file name obtained in [Step 4](#).

```
AS5800# copy bootflash: tftp
Source filename [c]? c7200-boot-mz.120-4.XE
Address or name of remote host []? 171.71.219.167
Destination filename [c7200-boot-mz.120-4.XE]?
!!
!!
3384888 bytes copied in 89.920 secs (38032 bytes/sec)
```

**Step 6** Determine the router shelf's current flash image.

```
AS5800# sh flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image AAD4004B 719C50 25 7314384 May 02 2000 13:55:04
c5800-p4-mz_120-4_XL1.bin
```

**Step 7** Backup the current router shelf IOS image (C5800-p4-mz.XXX) stored in Flash memory. Use the file name obtained in [Step 6](#).

```
AS5800# copy flash tftp
Source filename []? c5800-p4-mz_120-4_XL1.bin
Address or name of remote host []? 171.71.219.167
Destination filename [c5800-p4-mz_120-4_XL1.bin]?
!!
!!
7314384 bytes copied in 218.684 secs (33552 bytes/sec)
```

**Step 8** On your TFTP Server, verify that files were copied (backed up).



**Note** By default, files are copied to and from the Cisco TFTP root directory.

## Installing New IOS Software on the Cisco AS5800

An AS5800 Cisco IOS upgrade requires a compatible Cisco IOS image upgrade on both the Dial Shelf Controller (DSC) cards and Router Shelf (RS) components of the system. Two distinct upgrade procedures are necessary, one for each component.



**Note** Cisco recommends upgrading the dial-shelf controller(s) first, since all upgrades are performed through the router shelf. Once DSC(s) are upgraded, the router shelf will not be able to communicate with the DSC(s) until a compatible IOS image is installed on the RS.

**Note**


---

Do not modify your running configuration during the IOS upgrade process.

---

**Note**


---

Upgrade verifications are performed after all necessary upgrades are complete, and all system components are reloaded.

---

## Upgrading the DSC Software

The following procedure outlines commands used to perform a Cisco 5814 Dial Shelf Controller (DSC) software upgrade from the Router Shelf.

---

**Step 1** Login to the AS5800 Router Shelf and enter Enable (privileged exec) mode.

**Step 2** Identify IOS images in the DSC bootflash.

```
AS5800# execute-on slot 12 sh bootflash:
DA-Slot12#
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   BC8CA85F 251C60  26 2169824 Nov 18 1999 22:12:15
dsc-c5800-mz.120-4.XL1.bin
```

**Step 3** Delete the current IOS image(s) from bootflash.

```
AS5800# execute-on slot 12 del bootflash:dsc-c5800-mz.120-4.XL1.bin
DA-Slot12#
Delete filename [dsc-c5800-mz.120-4.XL1.bin]?
Delete bootflash:dsc-c5800-mz.120-4.XL1.bin? [confirm]
AS5800#
```

**Step 4** Squeeze the DSC bootflash.

```
AS5800# execute-on slot 12 squeeze bootflash

DA-Slot12#
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of bootflash complete
```

**Step 5** Identify IOS images in the DSC flash.

```
AS5800# execute-on slot 12 sh flash

DA-Slot12#
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image   BC8CA85F 231C60  26 2169824 Sep 16 1999 18:10:32
dsc-c5800-mz.120-4.XL1.bin
2  .D image   8FDE1F61 45FEC8  18 2286056 Jan 25 2000 18:28:57 dsc-c5800-mz.Jan21
```

**Step 6** Delete images or files no longer required.

```
AS5800# execute-on slot 12 delete flash:dsc-c5800-mz.120-4.XL1.bin
DA-Slot12#
Delete filename [dsc-c5800-mz.120-4.XL1.bin]?
Delete slot0:dsc-c5800-mz.120-4.XL1.bin? [confirm]
AS5800#
```

- Step 7** Squeeze the DSC flash to remove deleted files.

```
AS5800# execute-on slot 12 squeeze flash:
DA-Slot12#
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Writing sector: 1
Squeeze of slot0 complete
```

- Step 8** Download the new DSC image from your TFTP server to the DSC flash.




---

**Note** By default, files are copied to and from the Cisco TFTP root directory.

---

```
AS5800# copy tftp:dsc-c5800-mz.120-7.T.bin dsc12-slot0
Address or name of remote host [171.71.219.167]?
Source filename [dsc-c5800-mz.120-7.T.bin ]?
Destination filename [dsc12-slot0]?
Accessing tftp://171.71.219.167/dsc-c5800-mz.120-7.T.bin ...
%Warning: File not a valid executable for this system
Abort Copy? [confirm]n
Loading dsc-c5800-mz.120-7.T.bin from 171.71.219.167 (via FastEthernet0/0/0):
!!
```

The following Warning message appears.

```
%Warning: File not a valid executable for this system
Abort Copy? [confirm]
```




---

**Note** Do not abort the copy process. This message implies that the file being downloaded is not router shelf compatible, which is true. However, the router assumes the file being downloaded will be executed on the router shelf, when, in fact, the file is a dial shelf controller file, being downloaded to the dial shelf through the router, that will ultimately be executed on the dial shelf.

---

- Step 9** Enter “n” to proceed with the download.

- Step 10** Copy the new DSC image to the DSC bootflash:

```
AS5800# execute-on slot 12 copy slot0:dsc-c5800-mz.120-7.T.bin
bootflash:
DA-Slot12#
Destination filename [dsc-c5800-mz.120-7.T.bin ]?
cc
cc
2169824 bytes copied in 24.464 secs (90409 bytes/sec)
```

- Step 11** Reload the DSC to load the new image.

```
Router# execute-on slot 12 reload
```

- Step 12** Repeat this procedure if you have a second DSC card to ensure both cards are running the same software release. The only change to the commands will be the slot number (“13” instead of “12”).




---

**Note** At this juncture, the DSC(s) and Router Shelf are not running the same IOS image, so you will not be able to communicate with the DSC through the Router Shelf.

---

## Upgrading the Router Shelf Software

The following procedure outlines commands used to perform a Cisco 7206 router shelf (RS) software upgrade from the Router Shelf.



**Note** Unless you installed new port adapters in the router shelf, do not upgrade the boot image. See [Upgrading the Router Shelf Boot Image](#).

### Step 1 Identify IOS images in the RS flash.

```
AS5800# sh flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image AAD4004B 719C50 25 7314384 May 02 2000 13:55:04
c5800-p4-mz_120-4_XL1.bin
9069488 bytes available (7314512 bytes used)
```

### Step 2 Delete images or files no longer required.

```
AS5800# delete slot0:c5800-p4-mz_120-4_XL1.bin
Delete filename [c5800-p4-mz_120-4_XL1.bin]?
Delete slot0:c5800-p4-mz_120-4_XL1.bin? [confirm]
```

### Step 3 Squeeze the flash to remove all deleted files.

```
AS5800# squeeze slot0:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Squeeze of slot0 complete
```

### Step 4 Download the new image from a TFTP server to the RS flash.



**Note** By default, files are copied to and from the Cisco TFTP root directory.

```
AS5800# copy tftp:c5800-p4-mz.120-7.T.bin slot0:
Address or name of remote host [171.71.219.167]?
Source filename [c5800-p4-mz.120-7.T.bin]?
Destination filename [c5800-p4-mz.120-7.T.bin]?
Accessing tftp://171.71.219.167/c5800-p4-mz.120-7.T.bin ...
Loading c5800-p4-mz.120-7.T.bin from 171.71.219.167 (via
FastEthernet0/0/0):!!
```

### Step 5 Upgrade the bootflash, if applicable. See “Upgrading the Router Shelf Boot Image”.



**Note** Unless you are installing new port adapters in the router shelf, do not upgrade the boot image. See “Upgrading the Router Shelf Boot Image”.

### Step 6 Reload the router shelf to load the new image.

```
Router# reload
```

## Upgrading the Router Shelf Boot Image

The following procedure outlines commands used to perform a Cisco 7206 router shelf (RS) boot image software upgrade from the router shelf.



**Note** Unless you installed new port adapters in the router shelf, do not upgrade the boot image.

**Step 1** Identify the current bootflash image.

```
AS5800# sh bootflash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image AC05EDDF 37A6B8 22 3384888 Dec 31 1999 18:08:09 c7200-boot-mz.120-4.XE

1 bytes available (3407872 bytes used)
```

**Step 2** Delete the current boot image from bootflash.

```
AS5800# del bootflash:
Delete filename []? c7200-boot-mz.120-4.XE
Delete bootflash:c7200-boot-mz.120-4.XE? [confirm]
```

**Step 3** Squeeze the bootflash to remove all deleted files.

```
AS5800# squeeze bootflash:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of bootflash complete
```

**Step 4** Copy the boot image from the TFTP server (c7200-boot-mz.XXX) to bootflash.

```
AS5800# copy tftp bootflash:
Address or name of remote host []? 171.71.219.167
Source filename []? c7200-boot-mz.120-7.T.bin
Destination filename [c7200-boot-mz.120-7.T.bin]?
Accessing tftp://171.71.219.167/c7200-boot-mz.120-7.T.bin...
Loading c7200-boot-mz.120-7.T.bin from 171.71.219.167 (via FastEthernet0/0/0):!!!!
!!
[OK - 3384888/6769664 bytes]

3384888 bytes copied in 65.112 secs (52075 bytes/sec)
```

## Software Upgrade Verification

Perform the following steps to verify the Router Shelf and DSC(s) are running new IOS images, and the Bootflash is running a new boot image.

**Step 1** Check the Dial Shelf Controller(s) for a new IOS image.

```
AS5800# execute-on slot 12 show version

DA-Slot12>
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-DSC-M), Version 12.0(7)T
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 12-Aug-99 18:48 by ayeh
Image text-base: 0x600088F0, data-base: 0x60520000

ROM: System Bootstrap, Version 11.3(1)AA, ROM: 5800 Software (C5800-DSC-M),Version
12.0(7)T

DA-Slot12 uptime is 41 minutes
System returned to ROM by reload
System image file is "slot0:dsc-c5800-mz.120-7.T.bin "

Router# execute-on slot 13 show version (IF APPLICABLE)
```

**Step 2** Check the Router Shelf for a new IOS image.

```
AS5800# sh version
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.0(7)T, TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 12-Aug-99 13:16 by ayeh
Image text-base: 0x60008900, data-base: 0x611A6000

ROM: System Bootstrap, Version 12.0(19990210:195103) [12.7T 105], DEVELOPMENT SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 12.0(7)T

doc-rtr58-01 uptime is 9 minutes
System returned to ROM by reload at 16:04:24 CST Fri Jun 9 2000
System restarted at 16:05:39 CST Fri Jun 9 2000
System image file is "slot0:c5800-p4-mz.120-7.T.bin"
```

**Step 3** Check the Bootflash for a new boot image.

```
AS5800#sh bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image AC05EDDF 37A6B8 22 3384888 Jun 12 200014:00:23
c7200-boot-mz.120-7.T.bin

22856 bytes available (3385016 bytes used)
```

## Upgrading the Cisco AS5850 Universal Gateway

Verify that you are upgrading from a Cisco IOS release that supports high availability (Cisco IOS Release 12.2(2)XB or higher), then perform one of the following procedures:

- [Upgrading from a High-Availability Image](#)
- [Upgrading from a Nonhigh-Availability Image](#)

**Note**

If, for some reason, you later wish to downgrade to a nonhigh-availability release, configure your system to classic-split mode, then reset each RSC.



## Upgrading from a High-Availability Image



### Tips

- To minimize downtime, perform the following upgrade in handover-split mode. Just half the system is down at a time, for as little as one minute per RSC, compared to a total system downtime of over nine minutes in classic-split mode.
- Before any system handover, to gracefully disable associated modems and thus minimize dropped calls, enter the **modem busyout** or **modem busyout-threshold** (sometimes called *autobusyout*) command. After handover, to reenable the modems, enter the **no** form of the command.

- 
- Step 1** From RSC 1, do the following:
- Disable RSC 1 modems by entering the **modem busyout** or **modem busyout-threshold** command.
  - Force handover of all RSC 1 slots to RSC 0 by entering the **redundancy handover shelf-resources** command. Wait for RSC 1 to reload automatically.
- Step 2** From RSC 0, transfer back to RSC 1 the slots that should belong to it by entering the **redundancy handover peer-resources** command.
- Step 3** From RSC 1, reenable the disabled modems by entering the **no** form of the **modem-busyout** command used above.
- Step 4** From RSC 0, do the following:
- Disable RSC 0 modems by entering the **modem busyout** or **modem busyout-threshold** command.
  - Force handover of all RSC 0 slots to RSC 1 by entering the **redundancy handover shelf-resources** command. Wait for RSC 0 to reload automatically.
- Step 5** From RSC 1, transfer back to RSC 0 the slots that should belong to it by entering the **redundancy handover peer-resources** command.
- Step 6** From RSC 0, reenable the disabled modems by entering the **no** form of the **modem-busyout** command used above.
- 

## Upgrading from a Nonhigh-Availability Image



### Caution

You must upgrade both RSCs at the same time. Operating with a mix of high-availability and nonhigh-availability images, even in classic-split mode, may result in erratic system behavior.



### Tips

Before any system handover, to gracefully disable associated modems and thus minimize dropped calls, enter the **modem busyout** or **modem busyout-threshold** (sometimes called *autobusyout*) command. After handover, to reenable the modems, enter the **no** form of the command.

- 
- Step 1** Disable all system modems by entering the **modem busyout** or **modem busyout-threshold** command.

**Step 2** Do the following in rapid succession (do not wait for the first RSC to reboot before proceeding):

- a. From RSC 0, reload by entering the **reload** command.
- b. From RSC 1, reload by entering the **reload** command.

Wait for both reloads to complete.

**Step 3** Reenable the modems as follows:

- a. From RSC 0, reenable the disabled modems by entering the **no** form of the **modem-busyout** command used above.
  - b. From RSC 1, reenable the disabled modems by entering the **no** form of the **modem-busyout** command used above.
-



# Cisco Media Gateway Cable Specifications

---

## Overview

This appendix provides the following cabling and pinout information for the Cisco universal access servers:

- [Console and Auxiliary Port Cables and Pinouts for Access Servers, page A-1](#)
- [Ethernet Port Pinouts, page A-4](#)
- [T1/PRI and E1/PRI Card Port Pinouts, page A-5](#)
- [T1/PRI and E1/PRI Card Cable Assemblies and Pinouts, page A-5](#)



**Note**

---

This appendix specifies pinouts only for the pins used. Pins not listed in the tables in this appendix are not connected.

---

## Console and Auxiliary Port Cables and Pinouts for Access Servers

The access server arrives with a console and auxiliary cable kit, which contains the cable and adapters you need to connect a console (an ASCII terminal or PC running terminal emulation software) or modem to your access server. The console and auxiliary cable kit includes:

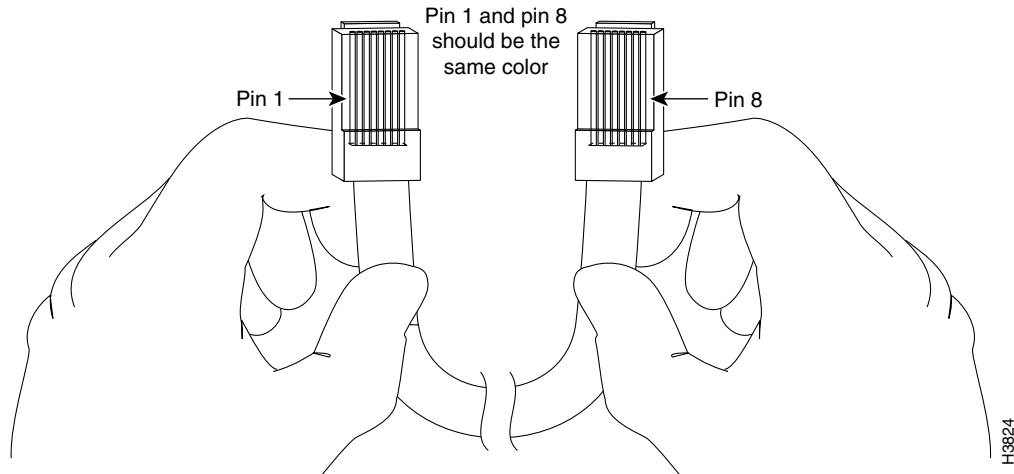
- RJ-45-to-RJ-45 rollover cable. (See the next section, “[Identifying a Rollover Cable](#),” for more information.)
- RJ-45-to-DB-9 female DTE adapter (labeled TERMINAL).
- RJ-45-to-DB-25 female DTE adapter (labeled TERMINAL).
- RJ-45-to-DB-25 male DCE adapter (labeled MODEM).

For console connections, proceed to the “[Console Port Cables and Pinouts](#)” section on page A-2; for modem connections, proceed to the “[Auxiliary Port Signals and Pinouts](#)” section on page A-4.

## Identifying a Rollover Cable

You can identify a rollover cable by comparing both ends of the cable. Holding the cables side-by-side, with the tab at the back, the wire connected to the pin on the outside of the left plug should be the same color as the wire connected to the pin on the outside of the right plug. (See [Figure A-1](#).) If your cable was purchased from Cisco Systems, pin 1 will be white on one connector, and pin 8 will be white on the other connector (a rollover cable reverses pins 1 and 8, 2 and 7, 3 and 6, and 4 and 5).

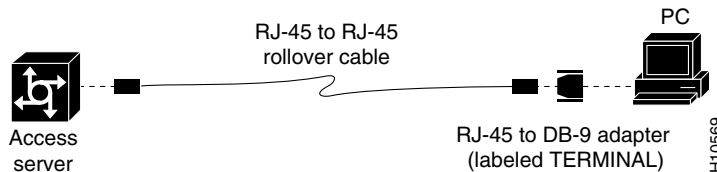
**Figure A-1** Identifying a Rollover Cable



## Console Port Cables and Pinouts

Use the RJ-45-to-RJ-45 rollover cable and the RJ-45-to-DB-9 female DTE adapter (labeled **TERMINAL**) to connect the console port to a PC running terminal emulation software. [Figure A-2](#) shows how to connect the console port to a PC. [Table A-1](#) lists the pinouts for the asynchronous serial console port, the RJ-45-to-RJ-45 rollover cable, and the RJ-45-to-DB-9 female DTE adapter (labeled **TERMINAL**).

**Figure A-2** Connecting the Console Port to a PC



**Table A-1** Console Port Signaling and Cabling Using a DB-9 Adapter

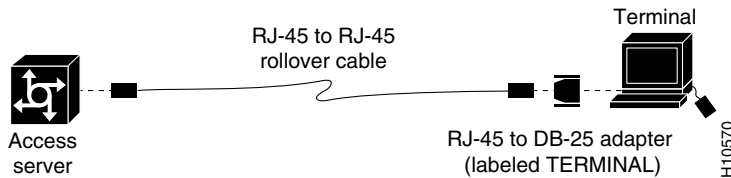
| Console Port (DTE) | RJ-45-to-RJ-45 Rollover Cable |           | RJ-45-to-DB-9 Terminal Adapter | Console Device |
|--------------------|-------------------------------|-----------|--------------------------------|----------------|
|                    | RJ-45 Pin                     | RJ-45 Pin | DB-9 Pin                       |                |
| RTS                | 1 <sup>1</sup>                | 8         | 8                              | CTS            |
| DTR                | 2                             | 7         | 6                              | DSR            |
| TxD                | 3                             | 6         | 2                              | RxD            |

**Table A-1 Console Port Signaling and Cabling Using a DB-9 Adapter (continued)**

| Console Port (DTE) | RJ-45-to-RJ-45 Rollover Cable |           | RJ-45-to-DB-9 Terminal Adapter | Console Device |
|--------------------|-------------------------------|-----------|--------------------------------|----------------|
|                    | RJ-45 Pin                     | RJ-45 Pin | DB-9 Pin                       |                |
| GND                | 4                             | 5         | 5                              | GND            |
| GND                | 5                             | 4         | 5                              | GND            |
| RxD                | 6                             | 3         | 3                              | TxD            |
| DSR                | 7                             | 2         | 4                              | DTR            |
| CTS                | 8 <sup>1</sup>                | 1         | 7                              | RTS            |

1. Pin 1 is connected internally to pin 8.

Use the RJ-45-to-RJ-45 rollover cable and RJ-45-to-DB-25 female DTE adapter (labeled TERMINAL) to connect the console port to a terminal. [Figure A-3](#) shows how to connect the console port to a terminal. [Table A-2](#) lists the pinouts for the asynchronous serial console port, the RJ-45-to-RJ-45 rollover cable, and the RJ-45-to-DB-25 female DTE adapter (labeled TERMINAL).

**Figure A-3 Connecting the Console Port to a Terminal****Table A-2 Console Port Signaling and Cabling Using a DB-25 Adapter**

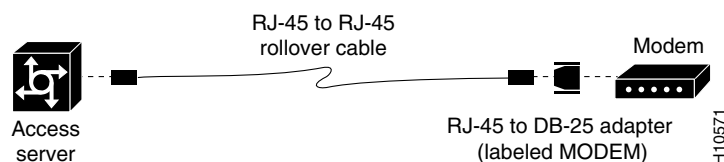
| Console Port (DTE) <sup>1</sup> | RJ-45-to-RJ-45 Rollover Cable |           | RJ-45-to-DB-25 Terminal Adapter | Console Device |
|---------------------------------|-------------------------------|-----------|---------------------------------|----------------|
|                                 | RJ-45 Pin                     | RJ-45 Pin | DB-25 Pin                       |                |
| RTS                             | 1 <sup>2</sup>                | 8         | 5                               | CTS            |
| DTR                             | 2                             | 7         | 6                               | DSR            |
| TxD                             | 3                             | 6         | 3                               | RxD            |
| GND                             | 4                             | 5         | 7                               | GND            |
| GND                             | 5                             | 4         | 7                               | GND            |
| RxD                             | 6                             | 3         | 2                               | TxD            |
| DSR                             | 7                             | 2         | 20                              | DTR            |
| CTS                             | 8 <sup>1</sup>                | 1         | 4                               | RTS            |

1. You can use the same cabling to connect a console to the auxiliary port.
2. Pin 1 is connected internally to pin 8.

## Auxiliary Port Signals and Pinouts

Use the RJ-45-to-RJ-45 rollover cable and RJ-45-to-DB-25 male DCE adapter (labeled MODEM) to connect the auxiliary port to a modem. Figure A-4 shows how to connect the auxiliary port to a modem. Table A-3 lists the pinouts for the asynchronous serial auxiliary port, the RJ-45-to-RJ-45 rollover cable, and the RJ-45-to-DB-25 male DCE adapter (labeled MODEM).

**Figure A-4** Connecting the Auxiliary Port to a Modem



**Table A-3** Auxiliary Port Signaling and Cabling Using a DB-25 Adapter

| AUX Port (DTE) | RJ-45-to-RJ-45 Rollover Cable |           | RJ-45-to-DB-25 Modem Adapter | Modem  |
|----------------|-------------------------------|-----------|------------------------------|--------|
| Signal         | RJ-45 Pin                     | RJ-45 Pin | DB-25 Pin                    | Signal |
| RTS            | 1                             | 8         | 4                            | RTS    |
| DTR            | 2                             | 7         | 20                           | DTR    |
| TxD            | 3                             | 6         | 3                            | TxD    |
| GND            | 4                             | 5         | 7                            | GND    |
| GND            | 5                             | 4         | 7                            | GND    |
| RxD            | 6                             | 3         | 2                            | RxD    |
| DSR            | 7                             | 2         | 8                            | DCD    |
| CTS            | 8                             | 1         | 5                            | CTS    |

## Ethernet Port Pinouts

**Table A-4** 10BASE-T Port Pinout

| RJ-45 Pin | Description |
|-----------|-------------|
| 1         | TX+         |
| 2         | TX-         |
| 3         | RX+         |
| 4         | -           |
| 5         | -           |
| 6         | RX-         |
| 7         | -           |
| 8         | -           |

**Table A-5 100BASE-T Port Pinouts**

| RJ-45 Pin | Description |
|-----------|-------------|
| 1         | RXD+        |
| 2         | RXD-        |
| 3         | TXD+        |
| 4         | –           |
| 5         | –           |
| 6         | TXD-        |
| 7         | –           |
| 8         | –           |

## T1/PRI and E1/PRI Card Port Pinouts

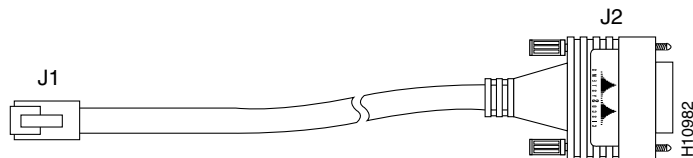
**Table A-6 Quad T1/PRI Card Port Pinouts**

| RJ-45 Pin | Description |
|-----------|-------------|
| 1         | RX Tip      |
| 2         | RX Ring     |
| 3         | RX Shield   |
| 4         | TX Tip      |
| 5         | TX Ring     |
| 6         | TX Shield   |
| 7         | –           |
| 8         | –           |

## T1/PRI and E1/PRI Card Cable Assemblies and Pinouts

**Table A-7 T1/PRI and E1/PRI Card Assemblies and Pinouts**

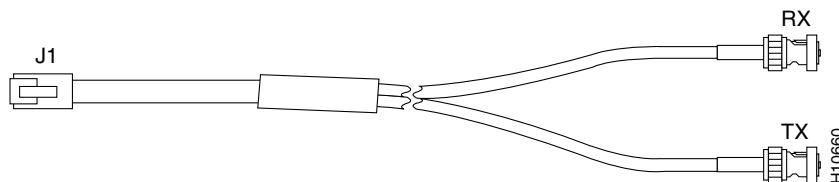
| Cable Description   | Part Number | Product Number    |
|---------------------|-------------|-------------------|
| RJ-45 to DB-15      | 72-1336-01  | CAB-E1-RJ45DB15=  |
| RJ-45 to DB-15 Null | 72-1337-01  | CAB-E1-RJ45DB15N= |
| RJ-45 to BNC        | 72-1338-01  | CAB-E1-RJ45BNC=   |
| RJ-45 to Twinax     | 72-1339-01  | CAB-E1-RJ45TWIN=  |
| RJ-45 to RJ-45 TE   | 72-1340-01  | CAB-E1-RJ45TE=    |
| RJ-45 to RJ-45 NT   | 72-1341-01  | CAB-E1-RJ45NT=    |
| RJ-45 to RJ-45 T1   | 72-1342-01  | CAB-E1-RJ45RJ45=  |
| RJ-45 to Bare       | 72-1343-01  | CAB-T1-RJ45BARE=  |

**Figure A-5 RJ-45-to-DB-15 Interface Cable****Table A-8 RJ-45-to-DB-15 Interface Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | DB-15 Pin |
|-----------|-----------|-----------------|-----------|-----------|
| Shield    | Ground    | Shell/Braid     |           | Shell     |
| J1-1      | RX Tip    | Twisted Pair #1 | ←         | J2-3      |
| J1-2      | RX Ring   | Twisted Pair #1 | ←         | J2-11     |
| J1-3      | RX Shield | Twisted Pair #3 |           | J2-4      |
| J1-4      | TX Tip    | Twisted Pair #2 | →         | J2-1      |
| J1-5      | TX Ring   | Twisted Pair #2 | →         | J2-9      |
| J1-6      | TX Shield | Twisted Pair #4 |           | J2-2      |

**Table A-9 RJ-45-to-Twinax Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | DB-15 Pin |
|-----------|-----------|-----------------|-----------|-----------|
| Shield    | Ground    | Shell/Braid     |           | Shell     |
| J1-1      | RX Tip    | Twisted Pair #1 | ←         | J2-1      |
| J1-2      | RX Ring   | Twisted Pair #1 | ←         | J2-9      |
| J1-3      | RX Shield | Twisted Pair #3 |           | J2-2      |
| J1-4      | TX Tip    | Twisted Pair #2 | →         | J2-3      |
| J1-5      | TX Ring   | Twisted Pair #2 | →         | J2-11     |
| J1-6      | TX Shield | Twisted Pair #4 |           | J2-4      |

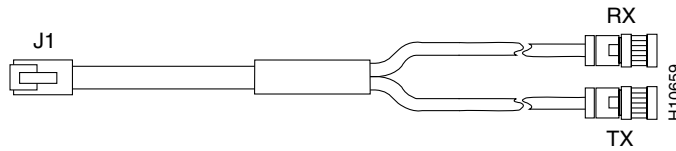
**Figure A-6 RJ-45-to-BNC Interface Cable for 75-Ohm, Unbalanced Connections****Table A-10 RJ-45-to-BNC Cable Pinouts**

| RJ-45 Pin | Signal  | Description     | Direction | BNC Pin        |
|-----------|---------|-----------------|-----------|----------------|
| Shield    | Ground  | Shell           |           | RX, TX Shields |
| J1-1      | RX Tip  | Twisted Pair #1 | ←         | RX-Tip         |
| J1-2      | RX Ring | Twisted Pair #1 | ←         | RX-Shield      |



**Table A-10 RJ-45-to-BNC Cable Pinouts (continued)**

| RJ-45 Pin | Signal    | Description     | Direction | BNC Pin   |
|-----------|-----------|-----------------|-----------|-----------|
| J1-3      | RX Shield | Twisted Pair #3 |           | RX-Shield |
| J1-4      | TX Tip    | Twisted Pair #2 | —>        | TX-Tip    |
| J1-5      | TX Ring   | Twisted Pair #2 | —>        | TX-Shield |
| J1-6      | TX Shield | Twisted Pair #4 |           | TX-Shield |

**Figure A-7 RJ-45-to-Twinax Interface Cable for 120-Ohm, Balanced Connections****Table A-11 RJ-45-to-Twinax Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | Twinax Pin     |
|-----------|-----------|-----------------|-----------|----------------|
| Shield    | Ground    | Shell           |           | RX, TX Shields |
| J1-1      | RX Tip    | Twisted Pair #1 | <—        | RX-1           |
| J1-2      | RX Ring   | Twisted Pair #1 | <—        | RX-2           |
| J1-3      | RX Shield | Twisted Pair #3 |           | RX Shield      |
| J1-4      | TX Tip    | Twisted Pair #2 | —>        | TX-1           |
| J1-5      | TX Ring   | Twisted Pair #2 | —>        | TX-2           |
| J1-6      | TX Shield | Twisted Pair #4 |           | TX Shield      |

**Figure A-8 RJ-45-to-RJ-45 Interface Cable****Table A-12 RJ-45-to-RJ-45 TE Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | RJ-45 TE Pin |
|-----------|-----------|-----------------|-----------|--------------|
| Shield    | Ground    | Shell/Braid     |           | Shield       |
| J1-1      | RX Tip    | Twisted Pair #1 | <—        | J2-1         |
| J1-2      | RX Ring   | Twisted Pair #1 | <—        | J2-2         |
| J1-3      | RX Shield | Twisted Pair #3 |           | J2-3         |
| J1-4      | TX Tip    | Twisted Pair #2 | —>        | J2-4         |
| J1-5      | TX Ring   | Twisted Pair #2 | —>        | J2-5         |
| J1-6      | TX Shield | Twisted Pair #4 |           | J2-6         |

**Table A-13 RJ-45-to-RJ-45 NT Cable Pinouts**

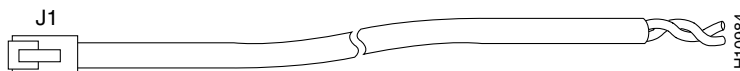
| RJ-45 Pin | Signal    | Description     | Direction | Signal    | RJ-45 NT Pin |
|-----------|-----------|-----------------|-----------|-----------|--------------|
| Shield    | Ground    | Shell/Braid     |           | Ground    | Shield       |
| J1-1      | RX Tip    | Twisted Pair #1 | ←         | TX Tip    | J2-4         |
| J1-2      | RX Ring   | Twisted Pair #1 | ←         | TX Ring   | J2-5         |
| J1-3      | RX Shield | Twisted Pair #3 |           | TX Shield | J2-6         |
| J1-4      | TX Tip    | Twisted Pair #2 | →         | RX Tip    | J2-1         |
| J1-5      | TX Ring   | Twisted Pair #2 | →         | RX Ring   | J2-2         |
| J1-6      | TX Shield | Twisted Pair #4 |           | RX Shield | J2-3         |

**Note**

Because this cable has polarity, the pinouts are different depending on which end of the cable you use.

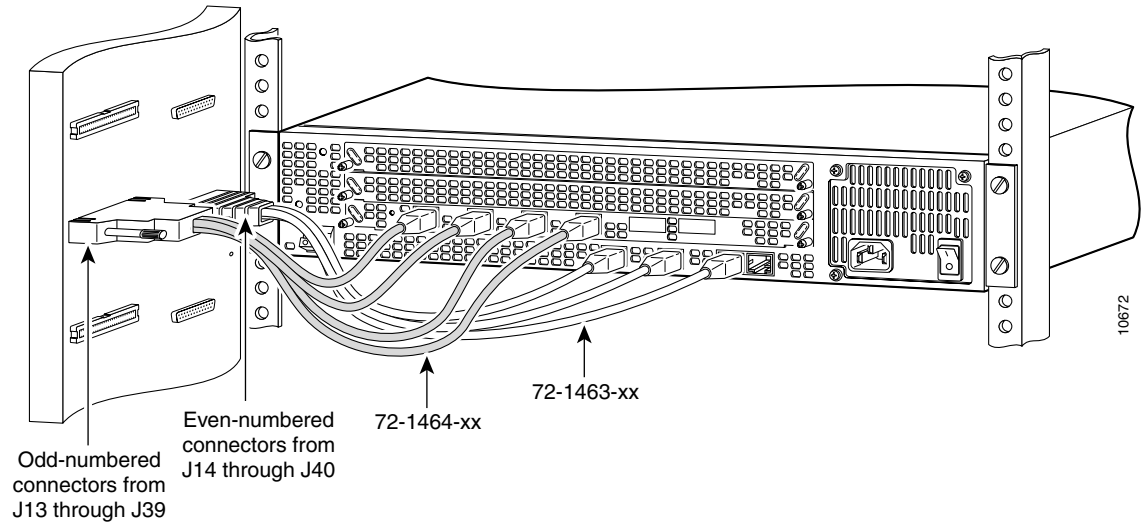
**Table A-14 RJ-45-to-RJ-45 T1 Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | RJ-45 T1 Pin |
|-----------|-----------|-----------------|-----------|--------------|
| Shield    | Ground    | Shell/Braid     |           | Shield       |
| J1-1      | RX Tip    | Twisted Pair #1 | ←         | J2-1         |
| J1-2      | RX Ring   | Twisted Pair #1 | ←         | J2-2         |
| J1-3      | RX Shield |                 |           |              |
| J1-4      | TX Tip    | Twisted Pair #2 | →         | J2-4         |
| J1-5      | TX Ring   | Twisted Pair #2 | →         | J2-5         |
| J1-6      | TX Shield |                 |           |              |

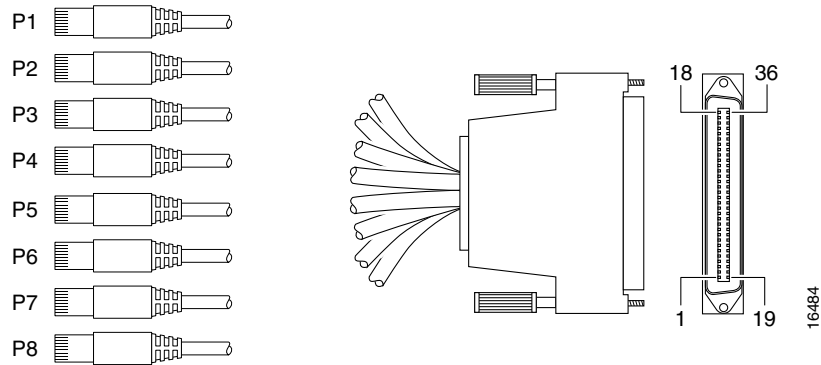
**Figure A-9 RJ-45-to-Bare Wire Interface Cable****Table A-15 RJ-45-to-Bare Wire Interface Cable Pinouts**

| RJ-45 Pin | Signal    | Description     | Direction | Bare   |
|-----------|-----------|-----------------|-----------|--------|
| Shield    | Ground    | Braid           |           |        |
| J1-1      | RX Tip    | Twisted Pair #1 | ←         | WIRE-1 |
| J1-2      | RX Ring   | Twisted Pair #1 | ←         | WIRE-2 |
| J1-3      | RX Shield |                 |           |        |
| J1-4      | TX Tip    | Twisted Pair #2 | →         | WIRE-3 |
| J1-5      | TX Ring   | Twisted Pair #2 | →         | WIRE-4 |
| J1-6      | TX Shield |                 |           |        |

**Figure A-10 T1/E1 (8) PRI Cable (72-1492-xx) Used in an Access Server Shelf**



**Figure A-11 T1/E1 (8) PRI Cable (72-1492-xx)**

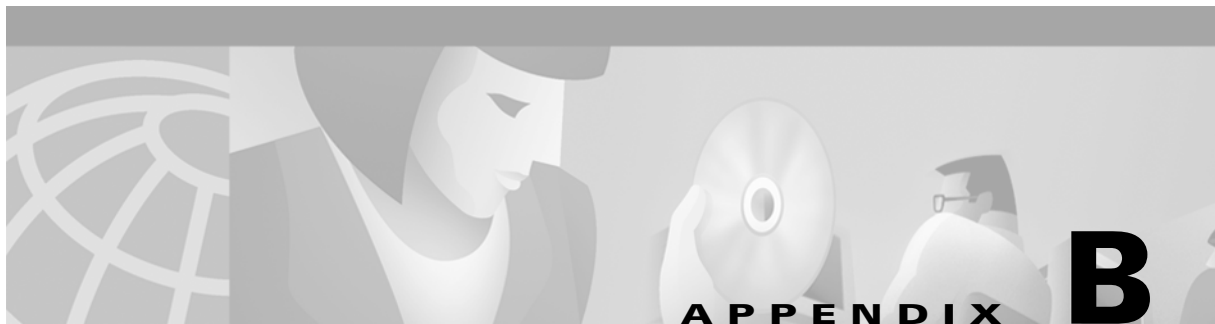


**Table A-16 Access Server Shelf T1/E1 (8) PRI Cable (72-1492-xx)**

| RJ-45 Plug | Shelf Connection | RJ-45 Pin | Twisted Pair | Signal   | Description          | 36 Pin |
|------------|------------------|-----------|--------------|----------|----------------------|--------|
| 1 (tan)    | PRI 0            | 1         | 2            | T1-1 Rx- | T1/E1 PRI Receive -  | 20     |
|            |                  | 2         |              | T1-1 Rx+ | T1/E1 PRI Receive +  | 2      |
|            |                  | 4         | 1            | T1-1 Tx- | T1/E1 PRI Transmit - | 21     |
|            |                  | 5         |              | T1-1 Tx+ | T1/E1 PRI Transmit + | 3      |
| 2 (tan)    | PRI 1            | 1         | 2            | T1-2 Rx- | T1/E1 PRI Receive -  | 22     |
|            |                  | 2         |              | T1-2 Rx+ | T1/E1 PRI Receive +  | 4      |
|            |                  | 4         | 1            | T1-2 Tx- | T1/E1 PRI Transmit - | 23     |
|            |                  | 5         |              | T1-2 Tx+ | T1/E1 PRI Transmit + | 5      |

Table A-16 Access Server Shelf T1/E1 (8) PRI Cable (72-1492-xx) (continued)

| RJ-45 Plug | Shelf Connection | RJ-45 Pin | Twisted Pair | Signal   | Description          | 36 Pin |
|------------|------------------|-----------|--------------|----------|----------------------|--------|
| 3 (tan)    | PRI 2            | 1         | 2            | T1-3 Rx- | T1/E1 PRI Receive -  | 24     |
|            |                  | 2         |              | T1-3 Rx+ | T1/E1 PRI Receive +  | 6      |
|            |                  | 4         | 1            | T1-3 Tx- | T1/E1 PRI Transmit - | 25     |
|            |                  | 5         |              | T1-3 Tx+ | T1/E1 PRI Transmit + | 7      |
| 4 (tan)    | PRI 3            | 1         | 2            | T1-4 Rx- | T1/E1 PRI Receive -  | 26     |
|            |                  | 2         |              | T1-4 Rx+ | T1/E1 PRI Receive +  | 8      |
|            |                  | 4         | 1            | T1-4 Tx- | T1/E1 PRI Transmit - | 27     |
|            |                  | 5         |              | T1-4 Tx+ | T1/E1 PRI Transmit + | 9      |
|            |                  | 4         | 1            | T1-1 Tx- | T1/E1 PRI Transmit - | 21     |
|            |                  | 5         |              | T1-1 Tx+ | T1/E1 PRI Transmit + | 3      |
| 5 (tan)    | PRI 4            | 1         | 2            | T1-2 Rx- | T1/E1 PRI Receive -  | 28     |
|            |                  | 2         |              | T1-2 Rx+ | T1/E1 PRI Receive +  | 10     |
|            |                  | 4         | 1            | T1-2 Tx- | T1/E1 PRI Transmit - | 29     |
|            |                  | 5         |              | T1-2 Tx+ | T1/E1 PRI Transmit + | 11     |
| 6 (tan)    | PRI 5            | 1         | 2            | T1-2 Rx- | T1/E1 PRI Receive -  | 30     |
|            |                  | 2         |              | T1-2 Rx+ | T1/E1 PRI Receive +  | 12     |
|            |                  | 4         | 1            | T1-2 Tx- | T1/E1 PRI Transmit - | 31     |
|            |                  | 5         |              | T1-2 Tx+ | T1/E1 PRI Transmit + | 13     |
| 7 (tan)    | PRI 6            | 1         | 2            | T1-3 Rx- | T1/E1 PRI Receive -  | 32     |
|            |                  | 2         |              | T1-3 Rx+ | T1/E1 PRI Receive +  | 14     |
|            |                  | 4         | 1            | T1-3 Tx- | T1/E1 PRI Transmit - | 33     |
|            |                  | 5         |              | T1-3 Tx+ | T1/E1 PRI Transmit + | 15     |
| 8 (tan)    | PRI 7            | 1         | 2            | T1-4 Rx- | T1/E1 PRI Receive -  | 34     |
|            |                  | 2         |              | T1-4 Rx+ | T1/E1 PRI Receive +  | 16     |
|            |                  | 4         | 1            | T1-4 Tx- | T1/E1 PRI Transmit - | 35     |
|            |                  | 5         |              | T1-4 Tx+ | T1/E1 PRI Transmit + | 17     |



## Managing Cisco Media Gateway Software

---

This appendix includes the following topics:

- [Software Management Change Process, page B-2](#)
- [Making a Baseline of Your Software Library, page B-2](#)
- [Synchronizing the Images in Your Software Library, page B-3](#)
- [Creating an Approver List, page B-3](#)
- [Checking for Outstanding Software Defects, page B-4](#)
- [Performing Software Upgrades, page B-4](#)
- [Planning the Upgrade, page B-5](#)
- [Determining the Impact of an Upgrade, page B-5](#)
- [Determining the Prerequisites for the Upgrade, page B-5](#)
- [Determining the Upgrade Sequence and Timing, page B-5](#)
- [Running the Upgrade Analysis Report, page B-6](#)
- [Running the Library Upgrade Analysis, page B-6](#)
- [Getting Software Images, page B-7](#)
- [Getting Backup Images for the Rollback Option, page B-7](#)
- [Software Downloading Processes, page B-7](#)
- [Directions for Browsing and Downloading from the Web, page B-7](#)
- [Retrieving Software Images Using the Cisco.com FTP, page B-9](#)
- [Setting Up a Software Image Upgrade, page B-10](#)
- [Setting Up a Device Upgrade, page B-11](#)
- [Job Control, page B-12](#)
- [Rescheduling an Upgrade, page B-12](#)
- [Tracking a Scheduled Software Upgrade, page B-12](#)
- [Verifying the Upgrade, page B-13](#)

# Software Management Change Process

The following sections describe a typical software management workflow. The network administrator should perform the necessary steps to set up, identify, plan, and execute a software upgrade for a group of devices.

Setting up your environment is crucial to successfully updating your software. Setting up your environment includes:

- [Making a Baseline of Your Software Library](#)
- [Synchronizing the Images in Your Software Library](#)
- [Creating an Approver List](#)
- [Checking for Outstanding Software Defects](#)

## Making a Baseline of Your Software Library

You need to create a baseline of your software library to ensure that you have all of the software images required to run your network.

The Add Image to Library function lets you import images from all Software- Management-supported devices in your network into the software image library. This function shows the images running on the network and the devices running each image. You can select any image to import into the software image library.

Use this function and the Synchronize Report option to ensure that the images running on your network always exist in the software image library.

If you want to add images running on devices on your network image library, use the following procedure to create a baseline of your software library:

---

**Step 1** Select **Tasks> Software Management> Add Image to Library**:

**Step 2** Select **Network**, then click **Next**.

The Select device Type dialog box displays network options.

- Cisco IOS—Cisco IOS software
- Catalyst—Cisco modular switching system software

**Step 3** Select the device type, then click **Next**.

The Network Baseline Status Summary displays the valid software images and devices on which they are running.

**Step 4** Click **Update** to display summary status progress, until devices processed are completed.

**Step 5** Click **Next**.

The Network Baseline dialog box displays a summary of valid software images and the devices on which they are running.

**Step 6** Click **Next**.

The Verify Network Baseline dialog box appears.

Click **Next** to continue.

The Job Control Information dialog box appears.

- Step 7** Enter the job description, optional e-mail address, and download time, then Click **Finish**.  
The Import Summary appears.
- Step 8** Make a note of the job identification number. You will use this number to track the job progress.
- Step 9** Click **Browse Job Status** to display the Job Status Report.
- Step 10** Click the job identification number for this job to display job details.  
Use this report to move the images to the software image library.
- Step 11** Click **Close** to close the report.
- 

## Synchronizing the Images in Your Software Library

The Schedule Synchronization Job option allows you to specify the time and frequency of the software synchronization job. This job finds Software Management supported devices that are running software images not in the software image library.

To synchronize the running images and the software image library, you need to schedule a synchronization job. This job generates a report of devices that are running images not in the library. You can then optionally add these images to the library.

To schedule the synchronization job, perform the following steps:

- 
- Step 1** Select **Admin > Software Management > Schedule Synchronization Job**.  
The Schedule Periodic Job for Synchronization Report dialog box appears.  
Select from the pull-down menu:
- The time (hours and minutes) and date the job begins
  - The frequency (daily, weekly, or monthly)
  - The e-mail address to which results are sent
- Step 2** Click **Finish**. A confirmation message appears.
- 

## Creating an Approver List

You can assign different people to perform different steps of the software upgrade process. This is done using the Create Approver List option to create one or more Make Checker approver lists. The Maker Checker feature allows you to require job upgrade approvals before running a scheduled job. It enforces the approval process by sending upgrade job requests by e-mail to the individuals who authorize network changes. Examples of roles and scenarios are listed below:

- The *system administrator* sets the Maker Checker Options.
- The *planner* analyzes the images to be used during a software image upgrade.
- The *network engineer* uses the Distribute Images option to create a software upgrade job.
- The *approver*, who might be an IS Administrator, accesses the approval page by double-clicking the link in the upgrade notification e-mail.
- The *job approver* approves or rejects the job and provides comments.

To create an approver list, perform the following steps:

- 
- Step 1** Select **Admin > Software Management > Create Approver List**.
- The Create Approver List dialog box appears.
- Step 2** Assign a name to the list, then click **Next**.
- Step 3** Use this dialog box to do the following functions:
- Add a name—Select the name from the User Name list box, then click **Add**.
  - Delete a name—Select the name from the Selected Approver list box, then click **Delete**.
  - Clear the Selected Approver List—Click **Delete All**.
- Step 4** Select **Finish**.
- 

## Checking for Outstanding Software Defects

The Bug Toolkit is a set of integrated applications that can be used to identify, evaluate, and receive status defects that have real or potential impact on your network. You can find the Bug Toolkit and instructions for use here:

<http://www.cisco.com/support/bugtools/>

The Bug Toolkit consists of three tools: Bug Navigator, Bug Watcher, and Watcher Agents. Together these three tools allow you to locate (Navigator, ID Search), and subscribe to either specific defects (Watcher) or defects matching a network profile that you create (Alerts).

- Bug Navigator allows you to search for defects and to create the Alert Agents and Watcher Bins (see below) to constantly monitor your specific network situation. Once a Bin or Agent has been created, it can be edited at any time to change the alert conditions, the defects being watched, or the network profile.
- Bug Watcher allows you to create collections, or bins of defects, that you can use to monitor the status of specific defects. When the status of a defect changes (for example, when its fix is integrated into a software release), you can view the status of that defect in real time, or you can also opt to receive e-mail or fax notifications of those changes. Watcher Bins can also be continuously updated with new defects that match a specific Agent Profile by means of Bug Watcher Agents. When a new defect that matches an Agent Profile is received, it appears on your Watcher Bin display under the list of watched defects. You then have the option of selecting any of the new defects to watch.
- Bug Watcher Agents are linked with Watcher Bins to feed new defects that match your Agent Profile to the bins. Multiple agents can feed a single bin. Agents can be as specific or as generic as you like. Using agents, you can stay continuously updated on any new defect issues critical to your successful network operations.

## Performing Software Upgrades

The software upgrade consists of the following steps:

- [Planning the Upgrade](#)
- [Getting Software Images](#)
- [Setting Up a Software Image Upgrade](#)



- [Setting Up a Device Upgrade](#)
- [Job Control](#)

## Planning the Upgrade

During the planning phase, consider the following points:

- [Determining the Impact of an Upgrade](#)
- [Determining the Prerequisites for the Upgrade](#)
- [Determining the Upgrade Sequence and Timing](#)

## Determining the Impact of an Upgrade

You can run the Cisco.com Upgrade Analysis and Library Upgrade Analysis Options to determine the impact of and prerequisites for deploying new software. These options allow you to compare your current network images to the images available on Cisco.com and show you the boot, Flash, RAM, and Telnet upgrades necessary for the devices you select.

**Note**

---

You must have Cisco.com login privileges. If you do not have a user account and password on CCO, contact your channel partner or enter a request on the standard CCO web site ([www.cisco.com](http://www.cisco.com)).

---

## Determining the Prerequisites for the Upgrade

You need to know the following information before you schedule your upgrades:

- ROM version numbers for the affected devices
- Board revisions

Use the Cisco Essentials Inventory options to determine the specifics.

## Determining the Upgrade Sequence and Timing

Schedule your upgrades and reboots so that you do not compromise your device path. Ensure that you reboot from the bottom of the path up.

Schedule your upgrades so that you do not have too many devices out of service at one time. The recommended maximum number of devices you should schedule per job is 12. More than 12 devices out of service at a time could affect your network performance adversely.

Tools can help you plan the sequence and timing of your upgrade:

- [Running the Upgrade Analysis Report](#)
- [Running the Library Upgrade Analysis](#)

## Running the Upgrade Analysis Report

To determine the sequence and timing of the upgrade, perform the following steps:

---

**Step 1** Select **Tasks > Software Management > CCO Upgrade Analysis**.

The Select Filtering Criteria dialog box appears.

**Step 2** Select any or all of the following filtering criteria, then click **Next**.

- Images newer than running image lists only images that have been released after the images running on your network.
- Same image feature subset as running image lists all subsets for your devices. Select this if you do not want to limit your list to the subsets currently running on the device.
- General deployment (GD) lists only images with the GD status.
- Latest maintenance release lists only the most recent maintenance release.

The Select Devices dialog box appears.

**Step 3** Select the views and devices to display, then click **Next**.

**Step 4** Select images, then click **Finish**.

The Upgrade Analysis Report displays upgrade recommendations.



**Note**

---

You can switch between List Format and Table Format by clicking the appropriate button at the top of the report.

---

**Step 5** Click **Close** to close the report.

---

## Running the Library Upgrade Analysis

Before you continue with the upgrade, you want to ensure that you have satisfied all prerequisites for devices whose software you want to upgrade. To do this, you run the Library Upgrade Analysis option to show you the boot ROM, Flash memory, RAM, and Telnet upgrades necessary for your selected devices.

---

**Step 1** Select **Tasks > Software Management > Library Upgrade Analysis**.

The Library Upgrade Analysis dialog box appears.

**Step 2** Select the image to analyze from the pull-down menu, then click **Next**.

The Select Devices dialog box appears.

**Step 3** Select the devices to upgrade, then click **Next**.

The Image Selection dialog box displays the images that are running on the selected devices.

**Step 4** Click **Finish**.

**Step 5** Click **Close** to close the report.

---

## Getting Software Images

Perform the following tasks when getting software images:

- [Getting Backup Images for the Rollback Option](#)
- [Software Downloading Processes](#)

### Getting Backup Images for the Rollback Option

If you want the rollback option to be available, you must check out a backup copy of the current software image for each device you want to back up into the software library. See “Retrieving Software Images” for more information.

If you decide later to use the previous software image, you can perform or schedule a device upgrade, specifying the old revision. See “Setting Up a Software Image Upgrade” for more information.

### Software Downloading Processes

File downloads over the World Wide Web actually require the use of the underlying File Transfer Protocol (FTP). Almost all World Wide Web browsers support FTP to one degree or another and most should have no problem.

As of November 1995, Cisco.com offers a new FTP system called “Cisco Connection Online Electronic Software Distribution” (CCOESD). This new FTP server allows for normal, hierarchical FTP directories and for better user features and administrative control over the site.

The new process for downloading files follows a general procedure, although some files, such as controlled software releases and special access files, might require additional steps before you can perform the download.

**Note**

---

You can now browse the Cisco.com Software Center either through the Web (which is preferred, because you can take advantage of hyperlinks for information) or by direct FTP access.

---

## Directions for Browsing and Downloading from the Web

This is the preferred method for customers to view and download files from CCO, which takes full advantage of hypertext links, graphics, forms, and other offerings of the World Wide Web. The process for downloading from CCO on the Web does not change significantly with the advent of CCOESD.

**Step 1**

---

Enter Cisco.com either as a registered user or as an anonymous guest. Go to the Cisco home page (<http://www.cisco.com>) to enter Cisco Connection Online as a guest or as a registered user.

Guest users are granted limited access to the Cisco Software Image Library. Check with your Cisco service representative to obtain Special File privileges beforehand. Registered users with software service contracts will be granted full access privileges to the Software Center. If you do not have access to the Software Image Library, check the terms of your service contract before contacting Cisco (or your sponsoring Cisco partner, for PICA customers).

**Step 2** Browse the Cisco.com Software Center on the Web to locate the topic that contains the files you need. Cisco.com allows users to navigate to the software image they want to download, using standard HyperText Markup Language (HTML) pages and forms.

- For Special Files Only—Enter the special access code in the field as instructed. There are some areas of the Software Center to which you can gain access only by entering a special access code. Special access codes are provided either through a postal letter (through electronic or regular mail) informing you of an upgrade's availability on Cisco.com, or through a conversation with authorized Cisco personnel.
- For Controlled Files only—Review all articles in the Software Update Planner before proceeding and then fill out the Software Release Checklist and select **Execute**.

After reviewing the Software Upgrade Planner, customers are next presented with the Software Release Checklist, which verifies information about the customer's hardware platform, to ensure that it meets minimal hardware and software compatibility requirements.

**Step 3** Click the radio button of the file you wish to download from the list of available software images then select Execute.

The listing of available files includes the following information:

- Filename—Same as listed in the Cisco.com FTP directory.
  - Files that end in “.bin” are binaries.
  - Those with “.Z” in the filename are compressed images. “.Z” files can be uncompressed using the UNIX **uncompress** command or similar utilities on other platforms.
  - Others ending in “.tar” are UNIX system archive images. These can be unarchived by using the **untar** command or similar utilities on other platforms.
  - Files labeled “.EXE” are DOS/Windows executable programs.
- Description—Usually includes the hardware platform, feature set and version for software images.
- Release—The software release or version number.
- Size—The size of the file in bytes.
- File Checksum—The file checksum value listed is a 5-digit BSD UNIX checksum.
- Router Checksum—This value should reflect what you see after loading the software into the router and performing a **show flash detail** command.
- MD5—This is an electronic fingerprint for the file. MD5 is the latest implementation of the internet Message Digest standard more fully described in RFC 1321: MD5 Message-Digest Algorithm and is useful for data security as well as for integrity.

**Step 4** Review the information on the “Confirm FTP Get” page, including the information about work-arounds if the download does not work through your Web browser.

**Step 5** Select the option in your browser to save the next link to your disk drive. For most files and browsers, this happens automatically, however, some files require manual intervention.

Examples:

- Netscape—Hold down the mouse button on the hyperlink and select “Save This Link As...”
- NCSA Mosaic—From the “Options” menu, select **Load to Local Disk**.




**Step 6** Click the hyperlink that reads, “Please confirm the transfer of this file, {filename} by clicking here.”

---

# Retrieving Software Images Using the Cisco.com FTP

With the advent of CIO ESD's restructured File Transfer Protocol (FTP) services, users who are experienced with the more technical aspects of the Internet, FTP, and the Web can perform more direct access of the Cisco FTP directories. We recommend this only for advanced users, because it bypasses many of the features found in the Web interface for the Cisco Software Image Library, such as Software Upgrade Planners and Software Checklists.

To use the File Transfer Protocol (FTP) perform the following steps:

- 
- Step 1** Enter Cisco.com as a registered user or as an anonymous guest. Please go to the Cisco FTP site by connecting to ftp.cisco.com.
- Step 2** To enter as a registered user, enter your CCO user id and password at the appropriate prompts. With a Web browser, enter the URL, "ftp://(user id) password, @ftp.cisco.com.
-  **Note** To be more secure, so passers-by will not see your password in the URL box of your Web browser, Netscape Navigator supports a feature so you can leave off "password" and then you will be prompted for the password separately.
- 
-  **Note** To enter with a special access code, enter the special access code as a user ID, and type your e-mail address in the form of "user@host.domain" as a password.
- 
- Example: Bob smith has an email address of bsmith@bigcompany.com, and wants to retrieve a file "smith\_file.txt" which has been put on CCO with a special access code: "bigcofiles". Bob would put the url of "ftp://bigcofiles:bsmith@ftp.cisco.com" into his web browser.
-  **Note** To enter as an anonymous guest, enter "anonymous" as your user ID and enter your e-mail address in the form of "user@host.domain" as a password. In a Web browser, enter the URL "ftp://ftp.cisco.com". No user ID or password is needed.
- 
- Step 3** Read carefully the login and directory messages you see on the screen, as there will be banners as you FTP login to CCO or change directories within the FTP structure that might contain important notes regarding explanations, changes, or updates to our CCO FTP services and content.
- Step 4** Use the **ls** or **dir** command to see files and directories in the FTP service. This command will list all files (including their file size and posting date) and subdirectories in the current directory you're in. If you are using a Web browser or graphical FTP client, you will automatically do a **dir** command that enters the directory and shows you the contents.
- Step 5** Read the "README" document in each subdirectory to get additional information about the posted files. The README file (which is also aliased as "README.txt" lists the files by filename, description, version, file size, checksums, and MD5, as listed above.
- Step 6** Do a **get** or **mget** command to download files to your computer. The **get [filename]** command copies a single file from CCO to your computer. The **mget [filename]** command can be used with a wildcard (\*\*.bin, for example) to fetch multiple files at one time and download them to your computer.

**Caution**

Be careful if you have a slow-speed network connection when invoking the **mget** command, in case it ties up your computer doing a very long download. For graphical browsers, selecting the file with a keyboard command or click of the mouse should enable the download.

## Setting Up a Software Image Upgrade

To set up an upgrade, perform the following steps:

**Step 1** Select **Tasks > Software Management > Distribute Images**.

The Select Device Type dialog box appears.

**Step 2** Select one of the following, then click **Next**.

- Cisco IOS
- Catalyst

**Step 3** The Select IOS Devices dialog box appears. Select Device Family, Current Cisco IOS Versions, and Boot ROM Version from the view windows; click **Query** to add the items to the Devices list; then select the devices.

**Step 4** Click **Next**.

If your CCO user name and password have not been added to the database, the CCO login dialog box appears. Enter your CCO user name and CCO password to update the user profile, then click **Next**. Click **Skip** if you do not want images from CCO included in the recommended images list.

The Recommended Image Upgrade dialog box appears.

To view the running status of the selected devices, (running image, Flash details, and so on) click **Details**. The Details report appears. Click **Close** to close the report.

**Step 5** Select the devices to upgrade, then click **Next**.

**Step 6** For each device, select the desired image upgrade. Clear check boxes for any devices you do not want to upgrade. If you selected images located on CCO, a message informs you that the images will be downloaded to the software image library at the scheduled time before the device is upgraded. Click **OK** to continue.

**Step 7** Verify that all the information is correct, then click **Next**.

The Verify Image Upgrade dialog box appears.

**Step 8** Check the verification status, make any necessary changes by going back to the Image Dialog box, then click **Next**.

The Distribution Sequence dialog box appears if more than one upgrade is being scheduled.



**Note** The Job Control Information dialog box appears if only one upgrade is being scheduled.

**Step 9** Move the upgrades up or down the distribution sequence list as desired, then click **Next**.

The Job Control Information dialog box appears.

- Step 10** Enter the job description and optional e-mail address, schedule the job, then click **Next**.  
The Work Order Report appears.
- Step 11** Click **Finish**.  
The Schedule Time Verification Box appears.
- Step 12** Click **Finish**.  
If the job was scheduled successfully, the Distribute Image Summary dialog box appears.
- Step 13** Click **Browse Job Status** to see the job details and change schedule options, if required.  
This report has two parts:
- The top part contains current job information, device information, and the Work Order report.
  - The bottom part contains either the schedule change dialog box or the job log file, depending on the state of the job.
- Step 14** You can optionally change the schedule, then close the report.



---

**Note** When the Make Checker option is on, you cannot change the upgrade time and date.

---

## Setting Up a Device Upgrade

If you want to upgrade your devices, you need to have the approval of your network administrator. This procedure assumes that you have selected the appropriate Make Checker options using **Admin > Software Management > Edit Preferences**.

To set up the upgrade, perform the following steps:

- 
- Step 1** Select **Tasks > Software Management > Distribute Images**.  
The Job Approval Information dialog box appears.
- Step 2** Select the Job Approver from the pull-down menu and add any comments, then click **Next**.  
The Distribute Image Summary appears.
- Step 3** Click **Browse Job Status**.  
The Job Status Report appears.  
The approver is then sent the request notification, which contains the URL used to launch the job request. The approver can open the request using any supported browser. The job request appears.
- Step 4** After reviewing the request, the approver can scroll to the bottom of the page and click **Approve** or **Reject**.  
The approval or rejection is sent to the job request originator.
- Step 5** Click **Close**.
-

# Job Control

The following job control tasks can be performed:

- [Rescheduling an Upgrade](#)
- [Tracking a Scheduled Software Upgrade](#)
- [Verifying the Upgrade](#)

## Rescheduling an Upgrade

To reschedule upgrades, perform the following steps:

---

**Step 1** Select **Admin > Software Management > Browse Job Status**

A new browser window displays the Job Status Report.

**Step 2** Click on the underlined job number.

The Job Details Report displays information about the job and access to any tasks that might apply.




---

**Note** To sort the report contents, click a column heading. The column by which the report is sorted is highlighted.

---

**Step 3** Click **Browse Jobs** to change another job, or click **Close** to close the report.

---

## Tracking a Scheduled Software Upgrade

Change Audit lets you filter messages from Essentials applications. You can use Change Audit to filter messages from Software Management and thereby confirm that a scheduled upgrade occurred.

To track a scheduled upgrade, perform the following steps:

---

**Step 1** Select **Tasks > Change Audit > Search Change Audit**.

The Change Audit - Filter Options dialog box appears.

**Step 2** Select the views and devices, then click **Next**. A second Change Audit- Filter Options dialog box appears.

**Step 3** Select **All** from the Applications pull-down menu, then select **Custom** and enter the date and time the upgrade is to occur.

The Change Audit - Searching report is displayed.

**Step 4** Select highlighted Details text in the View Details column to view the details of a particular device.

**Step 5** Select highlighted More Records text in the Grouped Records column to view records that stem from the same event.

**Step 6** Click **Close** to close the report.

---



## Verifying the Upgrade

After you upgrade device software images, you should check the status of your upgrades to verify that the process has been completed successfully.

The verification options are:

- Browse History, which summarizes the device software upgrade results stored in the history database for all devices on the network.
- Search History by device, which summarizes all software upgrades for selected devices.
- Search History by user, which summarizes all software upgrades performed by a particular user.
- Software Version Report, which summarizes software information for each device.
- Software Upgrade Report, which summarizes the device software upgrade results during the last 24 hours.
- To verify upgrades, perform the following steps:

---

**Step 1** Select **Tasks > Software Management > Search History by Device**.

The Select Devices dialog box appears.

**Step 2** In the devices field, enter the names of the devices for which you scheduled an upgrade, then click **Next**.

**Step 3** Alternatively, select the view and the devices in the view for which you set up an upgrade, then click **Next**.

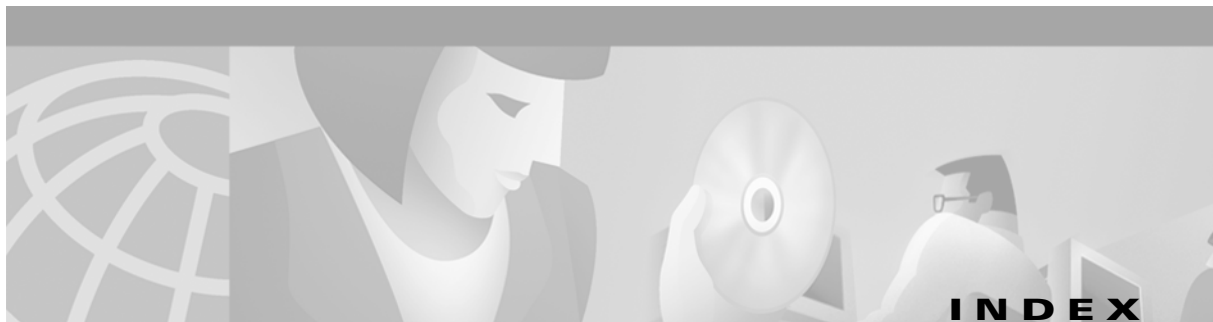
The Select Search Options dialog box appears.

**Step 4** Select the date range and time, then click **Finish**.

The Software Modification History Report appears for the selected devices.

---





---

## A

aaa protocol local [3-7](#)  
about this guide [vii](#)  
access servers solution  
    overview [1-1](#)  
adapter pinouts [A-3](#)  
Auxiliary [A-4](#)  
auxiliary port  
    adapter [A-3](#)  
    pinouts [A-3](#)

---

## C

cables  
    E1 [A-5](#)  
    E1/T1 card pinouts [A-5](#)  
    rollover cable [A-2](#)  
    T1 [A-5](#)  
call hairpinning [3-17](#)  
call treatment profile [3-7](#)  
call treatment resource [3-7](#)  
call types  
    discrimination [3-7](#)  
caution  
    symbol, defined [ix](#)  
Cisco SS7 interconnect for voice gateways solution [1-1](#)  
command  
    configure terminal [2-6, 2-8, 2-9, 3-4](#)  
    conventions [xi](#)  
    dialer dnis group [3-8](#)  
    enable mode [2-6, 2-8, 2-9, 3-4](#)  
    global configuration [3-4](#)

    range port [3-7](#)  
    resource pool [3-7](#)  
    rlm group [2-6, 2-8, 2-10, 3-5](#)  
    show isdn status [2-11, 3-6](#)  
    show rlm group [2-11, 3-5](#)  
configuration  
    information [2-3, 3-3](#)  
    rules [3-7](#)  
configuring  
    EIGRP [2-6, 3-5](#)  
    RPM [3-7](#)  
console port  
    adapter [A-3](#)  
    cables [A-2](#)  
    pinouts [A-2, A-3](#)  
conventions  
    command [xi](#)

---

## D

delete flash command [4-4](#)  
DNIS  
    number [3-7](#)  
documentation [ix](#)  
    conventions used in [viii](#)

---

## E

E1 card  
    cables [A-5](#)  
    port pinouts [A-5](#)

---

**H**

hairpinning [3-17](#)

---

**I****ISDN**

Network Side PRI Signalling, Trunking, and Switching

configuring classes of restrictions [3-19](#)

**PRI**

configuring classes of restrictions [3-19](#)

configuring trunk groups [3-18](#)

---

**M**

Media [vii](#)

media gateway [1-1](#)

MGC [vii](#)

**MGW**

See media gateway [1-1](#)

---

**P**

PSTN [vii](#)

---

**R**

range limit [3-7](#)

**redundancy**

feature enhancement [3-4](#)

**Redundant Link Manager**

configuring [3-4](#)

related documentation [ix](#)

**resource pool manager**

configuring [3-6](#)

RJ [A-6](#)

**RLM**

client [3-4](#)

rollover cable, identifying [A-2](#)

RPMS [3-7](#)

---

**S****services**

dial [3-7](#)

squeeze flash command [4-4](#)

SS7 interconnect for access servers solution [1-1](#)

symbols, defined [ix](#)

---

**T****T1 card**

cables [A-5](#)

port pinouts [A-5](#)

timesaver symbol, defined [ix](#)

---

**V****voice**

solution [1-1](#)