



Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide

November 24, 2010

Americas 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: 408 527-0883

Text Part Number: OL-14127-08

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide
© 2008-2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xxi

Objectives xxi

Document Revision History xxi

Organization xxiii

Related Documentation xxvi

 Cisco IOS XE Features and Software Configuration xxvi

 Cisco ASR 1000 Series Aggregation Services Routers Documentation xxvi

Document Conventions xxvii

Obtaining Documentation and Submitting a Service Request xxviii

CHAPTER 1

Using Cisco IOS XE Software 1-1

 Accessing the CLI Using a Router Console 1-1

 Accessing the CLI Using a Directly-Connected Console 1-1

 Connecting to the Console Port 1-2

 Using the Console Interface 1-3

 Accessing the CLI from a Remote Console Using Telnet 1-3

 Preparing to Connect to the Router Console Using Telnet 1-3

 Using Telnet to Access a Console Interface 1-4

Using Keyboard Shortcuts 1-5

Using the History Buffer to Recall Commands 1-5

Understanding Command Modes 1-6

Getting Help 1-7

 Finding Command Options Example 1-7

Using the no and default Forms of Commands 1-10

Saving Configuration Changes 1-10

Filtering Output from the show and more Commands 1-10

Finding Support Information for Platforms and Cisco Software Images 1-11

 Using Cisco Feature Navigator 1-11

 Using Software Advisor 1-11

 Using Software Release Notes 1-11

CHAPTER 2

SIP and SPA Product Overview 2-1

 Introduction to SIPs and SPAs 2-1

SPA Interface Processors	2-1
Shared Port Adapters	2-2
SIP and SPA Compatibility	2-3
Modular Optics Compatibility	2-5

PART 1

SPA Interface Processor

CHAPTER 3

Overview of the SIP 3-1

Release History	3-1
Supported SIP Features	3-2
Cisco ASR1000-SIP10 Features	3-2
Cisco ASR1000-SIP40 Features	3-2
Cisco ASR1000-SIP10 High-Availability Features	3-3
Supported MIBS	3-3
Command Reference Information	3-3

CHAPTER 4

Configuring the SIP 4-1

Configuration Tasks	4-1
Identifying Slots and Subslots for the SIP and SPAs	4-1
Specifying the Slot Location for a SIP	4-1
Specifying the SIP Subslot Location for a SPA	4-2
Hardware Module Scheduling Commands	4-3
Ingress Scheduling	4-3
Resetting a SIP	4-5

CHAPTER 5

Troubleshooting the SIP 5-1

General Troubleshooting Information	5-1
Interpreting Console Error Messages	5-1
Using debug Commands	5-1
Using show Commands	5-2
Using the Cisco IOS Event Tracer to Troubleshoot Problems	5-2
Preparing for Online Insertion and Removal of the SIP and SPAs	5-2
Preparing for Online Removal of a SIP	5-3
Deactivating a SIP	5-3
Reactivating a SIP	5-3
Verifying Deactivation and Activation of a SIP	5-4
Preparing for Online Removal of a SPA	5-5
Deactivating a SPA	5-6

Reactivating a SPA	5-7
Verifying Deactivation and Activation of a SPA	5-8
Deactivation and Activation Configuration Examples	5-8
Deactivation of a SIP Configuration Example	5-8
Activation of a SIP Configuration Example	5-9
Deactivation of a SPA Configuration Example	5-9
Activation of a SPA Configuration Example	5-9

PART 2**ATM Shared Port Adapters****CHAPTER 6****Overview of the ATM SPAs 6-1**

Release History	6-2
Supported Features	6-2
Basic Features	6-2
SONET/SDH Error, Alarm, and Performance Monitoring	6-3
Layer 2 Features	6-4
Layer 3 Features	6-4
High Availability Features	6-6
Restrictions	6-6
Supported MIBs	6-7
SPA Architecture	6-8
Path of Cells in the Ingress Direction	6-8
Path of Packets in the Egress Direction	6-9
Displaying the SPA Hardware Type	6-9
Example of the show interfaces Command	6-10
Example of the show controllers Command	6-10

CHAPTER 7**Configuring the ATM SPAs 7-1**

Configuration Tasks	7-1
Required Configuration Tasks	7-2
Specifying the Interface Address on a SPA	7-4
Modifying the Interface MTU Size	7-4
Interface MTU Configuration Guidelines	7-4
Interface MTU Configuration Task	7-6
Verifying the MTU Size	7-6
Creating a Permanent Virtual Circuit	7-9
Verifying a PVC Configuration	7-11
Creating a PVC on a Point-to-Point Subinterface	7-11
Configuring a PVC on a Multipoint Subinterface	7-13

Verifying a Multipoint PVC Configuration	7-14
Configuring a Range of PVCs on a Multipoint Subinterface	7-15
Configuring Traffic Parameters for PVCs	7-17
Verifying the Traffic Parameter Configuration	7-19
Configuring Virtual Circuit Classes	7-20
Verifying the Virtual Circuit Class Configuration	7-21
Configuring SONET and SDH Framing	7-21
Verifying the SONET and SDH Framing Configuration	7-22
Configuring AToM VP Cell Mode Relay Support	7-23
VP Mode Configuration Guidelines	7-23
VP Mode Configuration Example	7-23
Verifying ATM Cell Relay VP Mode	7-24
Configuring QoS Features on ATM SPAs	7-24
Configuring PPPoEoA on ATM SPAs	7-24
Saving the Configuration	7-25
Shutting Down and Restarting an Interface on a SPA	7-25
Verifying the Interface Configuration	7-27
Verifying Per-Port Interface Status	7-27
Monitoring Per-Port Interface Statistics	7-28
Configuration Examples	7-28
Basic Interface Configuration Example	7-29
MTU Configuration Example	7-29
PVC on a Point-to-Point Subinterface Configuration Example	7-29
PVC Ranges on a Multipoint Subinterface for PPPoEoA Configuration Example	7-30
AToM VP Cell Mode Relay Configuration Example	7-30
PPPoEoA VC Class and PVC Range Configuration Example	7-30
SONET and SDH Framing Configuration Example	7-31

CHAPTER 8

Troubleshooting the ATM SPAs 8-1

General Troubleshooting Information	8-1
Interpreting Console Error and System Messages	8-1
Using debug Commands	8-2
General debug Commands	8-2
ATM debug Commands	8-2
Using show Commands	8-2
Performing Basic Interface Troubleshooting	8-3
Using the Ping Command to Verify Network Connectivity	8-4
Displaying Additional ATM SPA Data	8-5
Displaying ATM SPA Hardware Information	8-5

Displaying Information About PVCs	8-5
Using Loopback Commands	8-6
Using loopback diagnostic to Create a Local Loopback	8-6
Examples	8-8
Using loopback line	8-8
Using the Cisco IOS Event Tracer to Troubleshoot Problems	8-9
Preparing for Online Insertion and Removal of a SPA	8-9

PART 3**Ethernet Shared Port Adapters****CHAPTER 9****Overview of the Ethernet SPAs 9-1**

Release History	9-2
Supported Features	9-2
Restrictions	9-3
Synchronous Ethernet	9-3
Squelching	9-4
SSM and ESMC	9-5
Synchronization Status Message	9-5
Ethernet Synchronization Messaging Channel	9-5
Supported MIBs	9-6
Supported Ethernet SPAs	9-7
2-Port Gigabit Synchronous Ethernet SPA	9-7
SPA Architecture	9-7
Path of a Packet in the Ingress Direction	9-7
Path of a Packet in the Egress Direction	9-8
Displaying the SPA Hardware Type	9-8
Example of the show interfaces Command	9-8

CHAPTER 10**Configuring the Ethernet SPAs 10-1**

Configuration Tasks	10-1
Required Configuration Tasks	10-2
Specifying the Interface Address on a SPA	10-4
Modifying the MAC Address on an Interface	10-4
Verifying a MAC Address	10-4
Gathering MAC Address Accounting Statistics	10-5
Configuring the Hot Standby Router Protocol	10-5
Verifying HSRP	10-5
Modifying the Interface MTU Size	10-6

Interface MTU Configuration Guidelines	10-6
Interface MTU Configuration Task	10-7
Verifying the MTU Size	10-7
QoS Classification	10-7
Port-Level or Physical-Level QoS Classification	10-10
Configuring the Encapsulation Type	10-10
Configuring the Autonegotiation on an Interface	10-10
Disabling Autonegotiation	10-11
Configuring Speed and Duplex	10-11
Configuring the Media Type	10-12
Enabling Autonegotiation	10-12
Configuring a Subinterface on a VLAN	10-12
VLAN Classification	10-13
Verifying Subinterface Configuration on a VLAN	10-14
Saving the Configuration	10-15
Shutting Down and Restarting an Interface on a SPA	10-15
Verifying the Interface Configuration	10-15
Verifying Per-Port Interface Status	10-16
Using show Commands to Check SFP Module and XFP Module Status	10-16
Configuring the Network Clock for the 2-Port Gigabit Synchronous Ethernet SPA on a Cisco ASR 1000 Series Router	10-19
Configuring the Network Clock in Global Configuration Mode	10-19
Configuring the Network Clock in Interface Configuration Mode	10-23
Managing Synchronization	10-24
Sample Configuration	10-25
Verifying Synchronous Ethernet Configuration	10-26
Troubleshooting the Synchronous Ethernet Configuration	10-31
Configuration Examples	10-33
Basic Interface Configuration Example	10-33
MAC Address Configuration Example	10-33
MAC Address Accounting Configuration Example	10-34
MTU Configuration Example	10-34
VLAN Configuration Example	10-35

CHAPTER 11

Troubleshooting the Gigabit Ethernet SPAs 11-1

General Troubleshooting Information	11-1
Using debug Commands	11-2
Using show Commands	11-2
Performing Basic Interface Troubleshooting	11-2

Verifying the Interface Is Up	11-4
Verifying the Line Protocol Is Up	11-5
Verifying the CRC Counter	11-5
Verifying the Carrier Signal	11-5
Understanding SPA Automatic Recovery	11-6
When Automatic Recovery Occurs	11-6
If Automatic Recovery Fails	11-6
Using the Cisco IOS Event Tracer to Troubleshoot Problems	11-6
Preparing for Online Insertion and Removal of a SPA	11-7

PART 4**Packet over SONET Shared Port Adapters****CHAPTER 12**

Overview of the POS SPAs	12-1
Release History	12-2
POS Technology Overview	12-2
Supported Features	12-3
SONET/SDH Compliance Features	12-3
SONET/SDH Error, Alarm, and Performance Monitoring Features	12-3
SONET/SDH Synchronization Features	12-4
WAN Protocol Features	12-4
Network Management Features	12-4
Restrictions	12-5
Supported MIBs	12-5
SPA Architecture	12-6
4-Port OC-3c/STM-1 POS SPA Architecture	12-6
Path of a Packet in the Ingress Direction	12-6
Path of a Packet in the Egress Direction	12-6
2-Port OC-48c/STM-16 POS SPA Architecture	12-7
Path of a Packet in the Ingress Direction	12-7
Path of a Packet in the Egress Direction	12-8
1-Port OC-192c/STM-64 POS XFP SPA Architecture	12-8
Path of a Packet in the Ingress Direction	12-8
Path of a Packet in the Egress Direction	12-9
Displaying the SPA Hardware Type	12-9
Example of the show interfaces Command	12-9
Example of the show controllers Command	12-10

CHAPTER 13**Configuring the POS SPAs 13-1**

Configuration Tasks 13-1

Specifying the Interface Address on a SPA 13-1

Modifying the Interface MTU Size 13-2

Interface MTU Configuration Guidelines 13-2

Interface MTU Configuration Task 13-3

Verifying the MTU Size 13-3

Modifying the POS Framing 13-3

Verifying the POS Framing 13-4

Modifying the Keepalive Interval 13-5

Verifying the Keepalive Interval 13-5

Modifying the CRC Size 13-6

Verifying the CRC Size 13-6

Modifying the Clock Source 13-6

Verifying the Clock Source 13-7

Modifying SONET Payload Scrambling 13-8

Verifying SONET Payload Scrambling 13-8

Configuring the Encapsulation Type 13-8

Verifying the Encapsulation Type 13-8

Configuring POS Alarm Trigger Delays 13-9

Path-Level Triggers 13-9

Verifying POS Alarm Trigger Delays 13-9

Saving the Configuration 13-10

Shutting Down and Restarting an Interface on a SPA 13-10

Verifying the Interface Configuration 13-11

Verifying Per-Port Interface Status 13-11

Monitoring Per-Port Interface Statistics 13-11

Configuration Examples 13-12

Basic Interface Configuration Example 13-13

MTU Configuration Example 13-13

POS Framing Configuration Example 13-14

Keepalive Configuration Example 13-14

CRC Configuration Example 13-14

Clock Source Configuration Example 13-15

SONET Payload Scrambling Configuration Example 13-15

Encapsulation Configuration Example 13-15

POS Alarm Trigger Delays Configuration Example 13-16

PART 5**Serial Shared Port Adapters**

CHAPTER 14**Overview of the Serial SPAs 14-1**

- Release History 14-1
- Supported Features 14-2
- Restrictions 14-4
- Supported MIBs 14-5
- Displaying the SPA Hardware Type 14-7
 - Examples of the show interfaces Command 14-7
 - Examples of the show controllers Command 14-8

CHAPTER 15**Configuring the 8-Port Channelized T1/E1 SPA 15-1**

- Configuration Tasks 15-1
 - Required Configuration Tasks 15-1
 - Setting the Card Type 15-2
 - Enabling the Interfaces on the Controller 15-4
 - Verifying Controller Configuration 15-5
 - Setting the IP Address 15-6
 - Verifying Interface Configuration 15-6
 - Specifying the Interface Address on a SPA 15-6
 - Optional Configurations 15-7
 - Configuring Framing 15-8
 - Configuring Encapsulation 15-9
 - Configuring the CRC Size for T1 15-10
 - Configuring FDL 15-11
 - Invert Data on the T1/E1 Interface 15-11
 - Changing a Channel Group Configuration 15-12
 - Configuring QoS Features on Serial SPAs 15-12
 - Saving the Configuration 15-13
 - Verifying the Interface Configuration 15-13
 - Verifying Per-Port Interface Status 15-13
- Configuration Examples 15-14
 - Framing and Encapsulation Configuration Example 15-14
 - CRC Configuration Example 15-14
 - Facility Data Link Configuration Example 15-15
 - Invert Data on the T1/E1 Interface Example 15-15

CHAPTER 16**Configuring the 2-Port and 4-Port Channelized T3 SPAs 16-1**

- Configuration Tasks 16-1
 - Required Configuration Tasks 16-2

Configuring the T3 Controller	16-2
Configuring the Logical T1 Interfaces	16-3
Verifying T3 Controller Configuration	16-5
Verifying Interface Configuration	16-6
Specifying the Interface Address on a SPA	16-7
Optional Configurations	16-8
Configuring Data Service Unit Mode	16-8
Configuring Maintenance Data Link	16-9
Configuring Encapsulation	16-11
Configuring T3 Framing	16-13
Configuring FDL	16-13
Configuring Scramble	16-15
Saving the Configuration	16-16
Verifying the Interface Configuration	16-16
Verifying Per-Port Interface Status	16-16
Configuration Examples	16-17
DSU Configuration Example	16-18
MDL Configuration Example	16-18
Encapsulation Configuration Example	16-18
Framing in Unchannelized Mode Configuration Example	16-19
Facility Data Link Configuration Example	16-19
Scrambling Configuration Example	16-19
Creating a Multilink Bundle Configuration Example	16-19
Assigning a T1 Interface to a Multilink Bundle Configuration Example	16-20

CHAPTER 17

Configuring the 2-Port and 4-Port Clear Channel T3/E3 SPAs 17-1

Configuration Tasks	17-1
Required Configuration Tasks	17-2
Setting the Card Type	17-2
Setting the IP Address	17-3
Verifying Controller Configuration	17-3
Verifying Interface Configuration	17-4
Specifying the Interface Address on a SPA	17-5
Optional Configurations	17-5
Configuring Data Service Unit Mode	17-5
Configuring Maintenance Data Link	17-7
Configuring Scramble	17-9
Configuring Framing	17-11
Configuring Encapsulation	17-12

Configuring Cable Length	17-13
Configuring Invert Data	17-14
Configuring the Trace Trail Buffer	17-15
Configuring QoS Features on Serial SPAs	17-16
Saving the Configuration	17-16
Verifying the Interface Configuration	17-16
Verifying Per-Port Interface Status	17-16
Monitoring Per-Port Interface Statistics	17-17
Configuration Examples	17-18
DSU Configuration Example	17-18
MDL Configuration Example	17-18
Scrambling Configuration Example	17-19
Framing Configuration Example	17-19
Encapsulation Configuration Example	17-19
Cable Length Configuration Example	17-19
Invert Data Configuration Example	17-20
Trace Trail Buffer Configuration Example	17-20

CHAPTER 18

Configuring the 4-Port Serial Interface SPA 18-1

Configuration Tasks	18-1
Configuring the 4-Port Serial Interface SPA	18-2
Verifying the Configuration	18-2
Using show Commands	18-3
Using the ping Command to Verify Network Connectivity	18-6
Using loopback Commands	18-6
Specifying the Interface Address on a SPA	18-7
Optional Configurations	18-7
Configuring Timing Signals	18-7
Inverting the Clock Signal	18-9
Configuring NRZI Format	18-9
Configuring Cyclic Redundancy Checks	18-10
Configuring Encapsulation	18-10
Saving the Configuration	18-12
Verifying the Interface Configuration	18-12
Verifying Per-Port Interface Status	18-12
Configuration Examples	18-13
Inverting the Clock Signal Configuration Example	18-13
NRZI Format Configuration Example	18-13
Cyclic Redundancy Checks Configuration Example	18-13

Encapsulation Configuration Example	18-14
Distributed Multilink PPP Configuration Example	18-14

CHAPTER 19

Configuring the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA 19-1

Restrictions for Configuring the 1-Port Channelized OC-12/STM-4 SPA	19-1
Configuration Tasks	19-2
Specifying the Physical Address for Controller and Interface Configuration	19-2
Naming the Interface	19-3
Required Configuration Tasks	19-3
Configuring the Controller for SONET or SDH Mode	19-4
Configuring SONET Mode	19-4
Configuring SDH Mode	19-6
Configuring Channelized DS3 Mode	19-8
Configuring DS1 (Channelized T3 mode)	19-9
Configuring E1 (Channelized T3/E3 mode)	19-12
Configuring Unchannelized E3 Serial Interface	19-13
Verifying the Interface Configuration	19-14
Optional Configurations	19-15
Configuring Encapsulation	19-15
Configuring the CRC Size for T1	19-16
Configuring FDL	19-17
Configuring FRF.12	19-18
Configuring Multilink Point-to-Point Protocol (Hardware-Based on the QFP)	19-18
Configuring LFI	19-21
Inverting Data on the T1/E1 Interface	19-21
Changing a Channel Group Configuration	19-22
Configuring BERT	19-22
Configuring QoS Features on Serial SPAs	19-24
Saving the Configuration	19-25
Verifying the Interface Configuration	19-25
Verifying Per-Port Interface Status	19-25
Configuration Examples	19-27
T3 Framing Configuration Example	19-27
Cyclic Redundancy Check Configuration Example	19-27
Facility Data Link Configuration Example	19-28
Invert Data on T1/E1 Interface Example	19-28

CHAPTER 20**Troubleshooting the Serial SPAs 20-1**

General Troubleshooting Information 20-1

Interpreting Console Error Messages 20-1

Using debug Commands 20-2

Using show Commands 20-2

Performing Basic Interface Troubleshooting 20-2

Serial Lines: show interfaces serial Status Line Conditions 20-3

Serial Lines: Increasing Output Drops on Serial Link 20-7

Serial Lines: Increasing Input Drops on Serial Link 20-8

Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic 20-9

Serial Lines: Troubleshooting Serial Line Input Errors 20-10

Serial Lines: Increasing Interface Resets on Serial Link 20-13

Serial Lines: Increasing Carrier Transitions Count on Serial Link 20-14

Using Bit Error Rate Tests 20-15

Configuring a BER Test 20-16

Viewing a BER Test 20-16

Interpreting BER Test Results 20-17

Using loopback Commands 20-18

Verifying Loopback Mode 20-18

Using the Cisco IOS Event Tracer to Troubleshoot Problems 20-19

Preparing for Online Insertion and Removal of a SPA 20-19

PART 6**Services Shared Port Adapters****CHAPTER 21****Overview of the Cisco WebEx Node for ASR 1000 Series 21-1**

Release History 21-1

Overview of the Cisco WebEx Node SPA Environment 21-1

Cisco WebEx Node Management System 21-3

Supported Features 21-4

Restrictions 21-4

Supported MIBs 21-5

Displaying the SPA Hardware Type 21-6

Example of the show interface service-engine Command 21-6

Example of the show hw-module subslot service-engine status Command 21-6

CHAPTER 22**Configuring the Cisco WebEx Node for ASR 1000 Series 22-1**

Prerequisites 22-1

Registering with the WebEx Data Center and the Cisco WebEx Node Management System 22-1

Obtaining an Account in the Cisco WebEx Node Management System	22-2
Registering a Cisco WebEx Node SPA in the Cisco WebEx Node Management System	22-3
Completing the Cisco WebEx Node SPA Configuration Prerequisites	22-4
Configuration Tasks	22-4
Specifying the Service Engine Interface Address on the Cisco WebEx Node SPA	22-4
Configuring the Virtual Service Engine Interface	22-5
Virtual Service-Engine Interface Configuration Guidelines	22-5
What To Do Next	22-7
Saving the Configuration	22-7
Shutting Down and Removing the Cisco WebEx Node SPA	22-8
Verifying the Service Engine Configuration	22-9
Showing Cisco WebEx Node SPA Settings and Activity	22-9
Showing Service Engine Status	22-9
Configuration Examples	22-10

CHAPTER 23

Troubleshooting the Cisco WebEx Node for the ASR 1000 Series 23-1

General Troubleshooting Information	23-1
Interpreting Console Error and System Messages	23-1
Using show Commands	23-2
show Commands to Display Cisco WebEx Node SPA Status	23-2
show Commands to Display Cisco WebEx Node SPA IDPROM	23-2
show Command to Display Cisco WebEx Node SPA Service Engine Status	23-2
show Command to Display Cisco WebEx Node SPA FPD version	23-3
show Command to Display Cisco WebEx Node SPA Error Messages on the RP Console	23-3
Accessing the SIP and SPA Consoles for Troubleshooting	23-3
Accessing the SIP Console	23-4
Accessing the Cisco WebEx Node SPA Console	23-4
Handling TraceBack and Core Dump Files on the Cisco WebEx Node SPA	23-5
Collecting Core Dump Files for the Cisco WebEx Node SPA	23-5
Collecting Traceback Information for the Cisco WebEx Node SPA	23-7
Performing Basic Troubleshooting	23-8
Troubleshooting Booting Failures	23-9
Troubleshooting Longer Booting Times in the Cisco WebEx Node SPA	23-9
Troubleshooting the Cisco WebEx Node SPA in an Out-of-Service State	23-10
Troubleshooting Hardware Failures	23-12
Troubleshooting Service Engine Application Status Errors	23-13
Using the ping Command from the Cisco ASR1000 Series Router to Verify Network Connectivity	23-14
Using the Cisco IOS Event Tracer to Troubleshoot Problems	23-15

Preparing for Online Insertion and Removal of a SPA 23-15

CHAPTER 24

Overview of the Cisco DSP SPA for ASR 1000 Series 24-1

Release History 24-1

Pre-requisites 24-2

Overview of the Cisco DSP SPA 24-2

High-Level System Details 24-2

Understanding Codecs and Maximum Channels Supported 24-3

Supported Features 24-4

Inband DTMF Interworking 24-4

Managing Jitters for Voice Packets 24-4

Comfort Noise and VAD 24-5

Restrictions 24-5

Supported MIBs 24-5

CHAPTER 25

Configuring the Cisco DSP SPA for the ASR 1000 Series 25-1

Voice Transcoding Overview 25-1

DSP Farm Profiles 25-1

Configuration Tasks 25-2

Configuring a DSP Farm Profile 25-2

What to Do Next 25-4

Enabling or Disabling Voice Activity Detection (VAD) 25-4

Configuration Examples for Universal Voice Transcoding 25-5

Additional References 25-7

Related Documents 25-7

Standards 25-7

MIBs 25-7

RFCs 25-7

Technical Assistance 25-8

PART 7

Field-Programmable Devices

CHAPTER 26

Upgrading Field-Programmable Devices 26-1

Release History 26-1

FPD Upgrade 26-1

Overview of FPD Images and Packages 26-2

Upgrading Your Cisco IOS Release and FPD Image 26-2

Upgrading Only Your Cisco IOS Release and Retaining Your Current FPD Image 26-2

Upgrading FPD Images in a Production System	26-2
Using a Non-Production System to Upgrade the Cisco ASR Series Router SPA FPD Image	26-3
Verifying System Compatibility First	26-3
Optional FPD Procedures	26-4
Manually Upgrading SPA FPD Images	26-4
Upgrading Multiple FPD Images	26-4
Displaying Current and Minimum Required FPD Image Versions	26-5
Displaying Information About the Default FPD Image Package	26-6
Verifying the FPD Image Upgrade Progress	26-7
FPD Image Upgrade Examples	26-7
Automatic FPD Image Upgrade Example	26-7
Manual FPD Image Upgrade Example	26-8
Troubleshooting Problems with FPD Image Upgrades	26-9
Power Failure or Removal of a SPA During an FPD Image Upgrade	26-9
Performing an FPD Recovery Upgrade	26-10
Verifying a Successful Upgrade	26-12

PART 8

Quality-of-Service (QoS)

CHAPTER 27

Classifying and Scheduling Packets for ASR 1000 Series 27-1

Release History	27-1
Overview of the Ingress Classification and Scheduling	27-2
Prerequisites for Ingress Classification and Scheduling	27-2
Classification and Scheduling Restrictions	27-3
Information About Ingress Classification	27-3
Ingress Classification Architecture	27-3
Resolving Oversubscription	27-5
Ingress Classification Overview	27-5
SPA-Based Classification	27-7
SIP-Based Classification	27-7
Default Classification	27-7
High Availability and Online Insertion and Removal	27-7
Configuring the Ingress Classification	27-7
Information About Ingress Scheduling	27-16
Scheduling Overview	27-17
Intra-CC Scheduling	27-17
Inter-CC Scheduling	27-17
Behavioral Changes in Scheduling	27-17

Configuring Intra-CC Scheduling	27-18
Configuring Inter-CC Scheduling	27-20

GLOSSARY

INDEX



Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains the following sections:

- [Objectives, page xxi](#)
- [Document Revision History, page xxi](#)
- [Organization, page xxiii](#)
- [Related Documentation, page xxvi](#)
- [Document Conventions, page xxvii](#)
- [Obtaining Documentation and Submitting a Service Request, page xxviii](#)

Objectives

This document describes the configuration and troubleshooting of SPA interface processors (SIPs) and shared port adapters (SPAs) that are supported on a Cisco ASR 1000 Series Routers.

Document Revision History

The Document Revision History records technical changes to this document. The table shows the Cisco IOS XE software release number and document revision number for the change, the date of the change, and a brief summary of the change.

Release No.	Revision	Date	Change Summary
Cisco IOS XE Release 3.2S	OL-14127-08	November 24, 2010	<div>Information pertaining to an overview and configuration of the following SPAs was added on the Cisco ASR 1000 Series Router.</div> <ul style="list-style-type: none">• introduction of a 2-Port Synchronous Gigabit Ethernet SPA• configuration of a 2-Port Synchronous Gigabit Ethernet SPA• introduction of a SPA DSP• configuration of a SPA DSP

Cisco IOS XE Release 3.1S	OL-14127-07	July 23, 2010	Information and features added to support the new SIP, Cisco ASR1000-SIP40 .
Cisco IOS XE Release 2.6	OL-14127-06	February 26, 2010	<p>Information added for support of the following SPA and other information updates:</p> <ul style="list-style-type: none"> • 1-Port Channelized OC-12/STM-4 SPA • Updates for optics module behavior and compatibility including: <ul style="list-style-type: none"> – Correction to show support for the GLC-GE-100FX optics module for the 5-Port and 10-Port Gigabit Ethernet SPA. – Correction to the autonegotiation behavior for the SFP-GE-T module. – Correction to show support for additional modules for the 2-Port, 4-Port, and 8-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA. • Added descriptions for the services SPAs and double-height SPAs.
Cisco IOS XE Release 2.5	OL-14127-05	November 25, 2009	<p>Information added for support of the following areas:</p> <ul style="list-style-type: none"> • 1-Port Clear Channel OC-12 ATM SPA • The hw-module subslot ethernet vlan unlimited command was introduced to remove the restriction of a maximum of 8100 802.1Q VLANs per Ethernet SPA. • Additional verification and troubleshooting information was added for the Cisco WebEx Node for ASR 1000 Series.

Cisco IOS XE Release 2.4	OL-14127-04	June 30, 2009	Information added for support of the following SPAs: <ul style="list-style-type: none"> • 2-Port, 4-Port, and 8-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA • 1-Port OC-48c/STM-16 POS SPA • 8-Port OC-3c/STM-1 POS SPA • 1-Port OC-192c/STM-64 POS/RPR XFP SPA • Cisco WebEx Node for ASR 1000 Series
Cisco IOS XE Release 2.3	OL-14127-03	November 24, 2008	Information added for support of the following SPA: <ul style="list-style-type: none"> • 1-Port and 3-Port Clear Channel OC-3 ATM SPA
Cisco IOS XE Release 2.2	OL-14127-02	September 10, 2008	Information added for support of the following SPAs: <ul style="list-style-type: none"> • 2-Port and 4-Port OC-48c/STM-16 POS SPA • 1-Port Channelized STM-1/OC-3 SPA
Cisco IOS XE Release 2.1	OL-14127-01	April 25, 2008	First release.

Organization

This document contains the following chapters:

Chapter	Title	Description
Chapter 1	Using Cisco IOS XE Software	Provides an introduction to accessing the command-line interface (CLI) and using the Cisco IOS software and related tools.
Chapter 2	SIP and SPA Product Overview	Provides a brief introduction to the SIP and SPA products on the Cisco ASR 1000 Series Routers, and information about the SIP and SPAs, and optics compatibility.
Chapter 3	Overview of the SIP	Describes release history, and feature and Management Information Base (MIB) support for the SIP on the Cisco ASR 1000 Series Routers.
Chapter 4	Configuring the SIP	Describes related configuration and verification information for the SIP on the Cisco ASR 1000 Series Routers.

Chapter	Title	Description
Chapter 5	Troubleshooting the SIP	Describes techniques that you can use to troubleshoot the operation of the SIP on the Cisco ASR 1000 Series Routers.
Chapter 6	Overview of the ATM SPAs	Describes release history, feature and Management Information Base (MIB) support, and an introduction to the ATM SPA architecture on the Cisco ASR 1000 Series Routers.
Chapter 7	Configuring the ATM SPAs	Describes the related configuration and verification information for the ATM SPAs on the Cisco ASR 1000 Series Routers.
Chapter 8	Troubleshooting the ATM SPAs	Describes techniques that you can use to troubleshoot the operation of the ATM SPAs on the Cisco ASR 1000 Series Routers.
Chapter 9	Overview of the Ethernet SPAs	Describes release history, feature and Management Information Base (MIB) support, and an introduction to the Gigabit Ethernet SPA architecture on the Cisco ASR 1000 Series Routers.
Chapter 10	Configuring the Ethernet SPAs	Describes the related configuration and verification information for the Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Routers.
Chapter 11	Troubleshooting the Gigabit Ethernet SPAs	Describes techniques that you can use to troubleshoot the operation of the Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Routers.
Chapter 12	Overview of the POS SPAs	Describes release history, feature and Management Information Base (MIB) support, and an introduction to the POS SPA architecture on the Cisco ASR 1000 Series Routers.
Chapter 13	Configuring the POS SPAs	Describes the related configuration and verification information for the POS SPAs on the Cisco ASR 1000 Series Routers.
Chapter 14	Overview of the Serial SPAs	Describes release history, feature and Management Information Base (MIB) support, and an introduction to the serial SPA architecture on the Cisco ASR 1000 Series Routers.
Chapter 15	Configuring the 8-Port Channelized T1/E1 SPA	Describes the related configuration and verification information for the 8-Port Channelized T1/E1 Serial SPAs on the Cisco ASR 1000 Series Routers.
Chapter 16	Configuring the 2-Port and 4-Port Channelized T3 SPAs	Describes the related configuration and verification information for the 2-Port and 4-Port Channelized T3 SPAs on the Cisco ASR 1000 Series Routers.
Chapter 17	Configuring the 2-Port and 4-Port Clear Channel T3/E3 SPAs	Describes the related configuration and verification information for the 2-Port and 4-Port T3/E3 Serial SPAs on the Cisco ASR 1000 Series Routers.

Chapter	Title	Description
Chapter 18	Configuring the 4-Port Serial Interface SPA	Describes the related configuration and verification information for the 4-Port Serial Interface SPA on the Cisco ASR 1000 Series Routers.
Chapter 19	Configuring the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA	Describes the related configuration and verification information for the 1-Port Channelized STM-1/OC-3 SPA on the Cisco ASR 1000 Series Routers.
Chapter 20	Troubleshooting the Serial SPAs	Describes techniques that you can use to troubleshoot the operation of the serial SPAs on the Cisco ASR 1000 Series Routers.
Chapter 21	Overview of the Cisco WebEx Node for ASR 1000 Series	Describes release history, feature and Management Information Base (MIB) support, and an introduction to the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to as the Cisco WebEx Node services shared port adapter (SPA).
Chapter 22	Configuring the Cisco WebEx Node for ASR 1000 Series	Describes the related configuration and verification information for the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, including information about registering the Cisco WebEx Node SPA with the Cisco WebEx Data Center and Cisco WebEx Node Management System.
Chapter 23	Troubleshooting the Cisco WebEx Node for the ASR 1000 Series	Describes techniques that you can use to troubleshoot the operation of the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers.
Chapter 24	Overview of the Cisco DSP SPA for ASR 1000 Series	Describes the release history, features, and Management Information Base (MIB) support, and an introduction to the Cisco DSP SPA for the ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers. The Cisco DSP SPA is referred to as the SPA-DSP shared port adapter (SPA).
Chapter 25	Configuring the Cisco DSP SPA for the ASR 1000 Series	Describes the related configuration information pertaining to the Cisco DSP SPA for the ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, including information about enabling DSP SPA, and creating the profiles and commands used to configure the DSP SPA.

Chapter	Title	Description
Chapter 26	Upgrading Field-Programmable Devices	Provides information about upgrading the field-programmable devices on the Cisco ASR 1000 Series Routers.
Chapter 27	Classifying and Scheduling Packets for ASR 1000 Series	Provides information about classifying and scheduling the ingress packets on the Cisco ASR 1000 Series Aggregation Service Routers.

Related Documentation

This section refers you to other documentation that also might be useful as you configure your Cisco ASR 1000 Series Routers.

Cisco IOS XE Features and Software Configuration

- Information about supported features and their configuration on the Cisco ASR 1000 Series Routers are available in the Cisco IOS XE software configuration guides at:
http://www.cisco.com/en/US/products/ps9587/products_installation_and_configuration_guides_list.html
- A summary of new features in a particular release can be found at:
http://www.cisco.com/en/US/products/ps9587/products_feature_guides_list.html
- Command documentation for the Cisco ASR 1000 Series Routers is available at:
http://www.cisco.com/en/US/products/ps9587/prod_command_reference_list.html

Cisco ASR 1000 Series Aggregation Services Routers Documentation

As you configure SIPs and SPAs on your Cisco Aggregation Services Router 1000 Series, you should also refer to the following companion publication for important hardware installation information:

- Cisco Aggregation Services Router 1000 Series SIP and SPA Hardware Installation Guide*

Some of the following other Cisco ASR 1000 Series Routers publications might be useful to you as you configure your Cisco ASR 1000 Series Routers.

- Cisco ASR 1000 Series Routers Hardware Installation Guide*
- Three Quick Start Guides:
 - Cisco ASR 1002 Router Quick Start Guide*
 - Cisco ASR 1004 Router Quick Start Guide*
 - Cisco ASR 1006 Router Quick Start Guide*
- Command Reference Guide:
 - Cisco IOS Quality of Service Solutions Command Reference guide at the URL:*
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html
- Regulatory Compliance and Safety Information for the Cisco ASR 1000 Series Routers*

- *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*
- *Cisco ASR 1000 Series Routers MIB Specifications Guide*
- *Release Notes for Cisco ASR 1000 Series Aggregation Services Routers*

Several other publications are also related to the Cisco ASR 1000 Series Routers. For a complete reference of related documentation, refer to the *Cisco ASR 1000 Series Routers Documentation Roadmap* located at the following URL:

http://www.cisco.com/en/US/products/ps9343/products_documentation_roadmaps_list.html

Your router and the Cisco IOS software running on it contain extensive features. You can find documentation for Cisco products at the following URL:

<http://www.cisco.com/cisco/web/psa/default.html?mode=prod>

Document Conventions

Within the SIP and SPA software configuration guides, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

This documentation uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP <i>community</i> string to <i>public</i> , do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
bold screen	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:



Caution

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



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.



Tip

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



CHAPTER 1

Using Cisco IOS XE Software

This chapter provides information to prepare you to configure a SPA interface processor (SIP) or shared port adapter (SPA) using the Cisco IOS XE software. It includes the following sections:

- [Accessing the CLI Using a Router Console, page 1-1](#)
- [Using Keyboard Shortcuts, page 1-5](#)
- [Using the History Buffer to Recall Commands, page 1-5](#)
- [Understanding Command Modes, page 1-6](#)
- [Getting Help, page 1-7](#)
- [Using the no and default Forms of Commands, page 1-10](#)
- [Saving Configuration Changes, page 1-10](#)
- [Filtering Output from the show and more Commands, page 1-10](#)
- [Finding Support Information for Platforms and Cisco Software Images, page 1-11](#)

Accessing the CLI Using a Router Console

The following sections describe how to access the command-line interface (CLI) using a directly-connected console or by using Telnet to obtain a remote console:

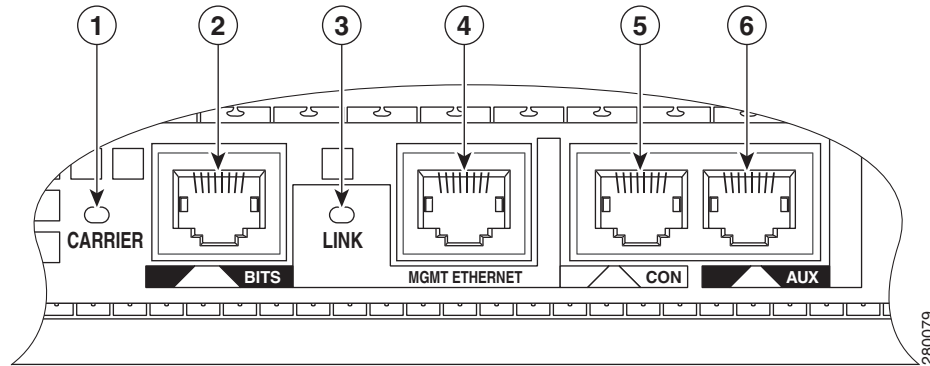
- [Accessing the CLI Using a Directly-Connected Console, page 1-1](#)
- [Accessing the CLI from a Remote Console Using Telnet, page 1-3](#)

For more detailed information about configuring and accessing a router through various services, refer to the *Cisco IOS Terminal Services Configuration Guide* and *Cisco IOS Terminal Services Command Reference* publications.

Accessing the CLI Using a Directly-Connected Console

This section describes how to connect to the console port on the router and use the console interface to access the CLI.

The console port on a Cisco ASR 1000 Series Router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is located on the front panel of each Route Processor, as shown in [Figure 1-1](#).

Figure 1-1 Cisco ASR 1000 Series Routers Console Port Connector

1	CARRIER LED	4	MGMT Ethernet connector
2	BITS connector	5	CON connector
3	LINK LED	6	AUX connector

Connecting to the Console Port

Before you can use the console interface on the router using a terminal or PC, you must perform the following steps:

Step 1 Configure your terminal emulation software with the following settings:

- 9600 bits per second (b/s)
- 8 data bits
- No parity
- 1 stop bit
- No flow control



Note

These are the default serial communication parameters on the router. For information about how to change the default settings to meet the requirements of your terminal or host, refer to the *Cisco IOS Terminal Services Configuration Guide*.

Step 2 Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or using the RJ-45-to-DB-9 DTE adapter (labeled “Terminal”).

Using the Console Interface

To access the CLI using the console interface, complete the following steps:

-
- Step 1** After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the following prompt appears:
- Press Return for Console prompt
- Step 2** Press **Return** to enter user EXEC configuration mode. The following prompt appears:
- Router>
- Step 3** From user EXEC configuration mode, enter the **enable** command as shown in the following example:
- Router> **enable**
- Step 4** At the password prompt, enter your system password. The following example shows entry of the password called “enablepass”:
- Password: **enablepass**
- Step 5** When your enable password is accepted, the privileged EXEC mode prompt appears:
- Router#
- Step 6** You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.
- Step 7** To exit the console session, enter the **quit** command as shown in the following example:
- Router# **quit**
-

Accessing the CLI from a Remote Console Using Telnet

This section describes how to connect to the console interface on a router using Telnet to access the CLI.

Preparing to Connect to the Router Console Using Telnet

Before you can access the router remotely using Telnet from a TCP/IP network, you need to configure the router to support virtual terminal lines (vty) using the **line vty** global configuration command. You also should configure the vty to require login and specify a password.

**Note**

To prevent disabling login on the line, be careful that you specify a password with the **password** command when you configure the **login** line configuration command. If you are using authentication, authorization, and accounting (AAA), you should configure the **login authentication** line configuration command. To prevent disabling login on the line for AAA authentication when you configure a list with the **login authentication** command, you must also configure that list using the **aaa authentication login** global configuration command. For more information about AAA services, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

In addition, before you can make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, refer to the *Cisco IOS Terminal Services Configuration Guide*.

Using Telnet to Access a Console Interface

To access a console interface using Telnet, complete the following steps:

Step 1 From your terminal or PC, enter one of the following commands:

- **connect** *host* [*port*] [*keyword*]
- **telnet** *host* [*port*] [*keyword*]

In this syntax, *host* is the router hostname or an IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information, refer to the *Cisco IOS Terminal Services Command Reference*.



Note

If you are using an access server, then you will need to specify a valid port number such as **telnet 172.20.52.40 2004**, in addition to the hostname or IP address.

The following example shows the **telnet** command to connect to the router named *router*:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

Step 2 At the password prompt, enter your login password. The following example shows entry of the password called “mypass”:

User Access Verification

Password: **mypass**



Note

If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command as shown in the following example:

```
Router> enable
```

Step 4 At the password prompt, enter your system password. The following example shows entry of the password called “enablepass”:

Password: **enablepass**

Step 5 When the enable password is accepted, the privileged EXEC mode prompt appears:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

```
Router# logout
```


Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

Table 1-1 lists the keyboard shortcuts for entering and editing commands.

Table 1-1 Keyboard Shortcuts

Keystrokes	Purpose
Ctrl-B or the Left Arrow key ¹	Move the cursor back one character
Ctrl-F or the Right Arrow key ¹	Move the cursor forward one character
Ctrl-A	Move the cursor to the beginning of the command line
Ctrl-E	Move the cursor to the end of the command line
Esc B	Move the cursor back one word
Esc F	Move the cursor forward one word

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

Table 1-2 lists the history substitution commands.

Table 1-2 History Substitution Commands

Command	Purpose
Ctrl-P or the Up Arrow key ¹	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the Down Arrow key ¹	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.
Router# show history	While in EXEC mode, list the last several commands you have just entered.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding Command Modes

You use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1-3 describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

Table 1-3 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the logout command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal privileged EXEC command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the exit or end command.
Interface configuration	From global configuration mode, specify an interface using an interface command.	Router(config-if)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
ROM monitor	From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the continue command.

For more information on command modes, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.

Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands, shown in [Table 1-4](#):

Table 1-4 Help Commands and Purpose

Command	Purpose
help	Provides a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry</i> <Tab>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
<i>command ?</i>	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Finding Command Options Example

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS XE software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

[Table 1-5](#) shows examples of how you can use the question mark (?) to assist you in entering commands.

Table 1-5 Finding Command Options

Command	Comment
Router> enable Password: <password> Router#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “#” from the “>”; for example, Router> to Router#.
Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
Router(config)# interface serial ? <0-6> Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? <0-3> Serial interface number Router(config)# interface serial 4/0 ? <cr> Router(config)# interface serial 4/0 Router(config-if)#	Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command. Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash. When the <cr> symbol is displayed, you can press Enter to complete the command. You are in interface configuration mode when the prompt changes to Router(config-if)#.
Router(config-if)# ? Interface configuration commands: ip Interface Internet Protocol config commands keepalive Enable keepalive lan-name LAN Name command llc2 LLC2 Interface Subcommands load-interval Specify interval for load calculation for an interface locaddr-priority Assign a priority group logging Configure logging for interface loopback Configure internal loopback on an interface mac-address Manually set interface MAC address mls mls router sub/interface commands mpoa MPOA interface configuration commands mtu Set the interface Maximum Transmission Unit (MTU) netbios Use a defined NETBIOS access list or enable name-caching no Negate a command or set its defaults nrzi-encoding Enable use of NRZI encoding ntp Configure NTP Router(config-if)#	Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

Table 1-5 Finding Command Options (continued)

Command	Comment
<pre>Router(config-if)# ip ? Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time Router(config-if)# ip</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>
<pre>Router(config-if)# ip address ? A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip address command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the negotiated keyword.</p> <p>A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 ? A.B.C.D IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	<p>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ? secondary Make this IP address a secondary address <cr> Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you can enter the secondary keyword, or you can press Enter.</p> <p>A <cr> is displayed; you can press Enter to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, Enter is pressed to complete the command.</p>

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the command **default command-name**, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function of the **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (**|**); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

```
show command | {begin | include | exclude} regular-expression
```

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
```

```
Serial4/3 is administratively down, line protocol is down
```

For more information on the search and filter functionality, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.

Finding Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or the software release notes.

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Using Software Advisor

To see if a feature is supported by a Cisco IOS release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com at <http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl>.

You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

Cisco IOS XE software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- New feature information
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. Refer to Cisco Feature Navigator for cumulative feature information.



CHAPTER 2

SIP and SPA Product Overview

This chapter provides an introduction to SPA interface processors (SIPs) and shared port adapters (SPAs). It includes the following sections:

- [Introduction to SIPs and SPAs, page 2-1](#)
- [SIP and SPA Compatibility, page 2-3](#)
- [Modular Optics Compatibility, page 2-5](#)

For more hardware details for the specific SIPs and SPAs that are supported on the Cisco ASR 1000 Series Aggregation Services Routers, refer to the companion publication, *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide*.

Introduction to SIPs and SPAs

Cisco ASR 1000 Series Routers SIPs and SPAs are a carrier card and port adapter architecture that increases modularity, flexibility, and density across Cisco routers for network connectivity. This section describes the SIPs and SPAs and provides some guidelines for their use.

SPA Interface Processors

The following list describes some of the general characteristics of a SIP:

- A SIP is a carrier card that inserts into a router slot like a line card. It provides no network connectivity on its own.
- A SIP contains one or more subslots, which are used to house one or more SPAs. The SPA provides interface ports for network connectivity.
- During normal operation, the SIP should reside in the router fully populated either with functional SPAs in all subslots, or with a blank filler plate (SPA-BLANK=) inserted in all empty subslots.
- SIPs support online insertion and removal (OIR) with SPAs inserted in their subslots. SPAs also support OIR and can be inserted or removed independently from the SIP.



Note

Fully populate all slots and subslots with blank filler plates or functional SPAs for maximum efficiency of the cooling system.

Shared Port Adapters

The following list describes some of the general characteristics of a SPA:

- A SPA is a modular type of port adapter that inserts into a subslot of a compatible SIP carrier card to provide network connectivity and increased interface port density. A SIP can hold one or more SPAs, depending on the SIP type.
- Some SPAs provide services rather than network connectivity, and can be inserted into subslots of a compatible SIP. For example, the Cisco WebEx Node for ASR 1000 Series, which provides WebEx meeting services, and the DSP SPA which provides voice transcoding and transrating capabilities.
- SPAs are available in the following sizes, as shown in [Figure 2-1](#) and [Figure 2-2](#):
 - Single-height SPA—Inserts into one SIP subslot.
 - Double-height SPA—Inserts into two single, vertically aligned SIP subslots.

Figure 2-1 Single-Height and Double-Height SPA Sizes

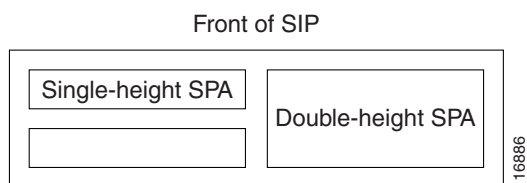
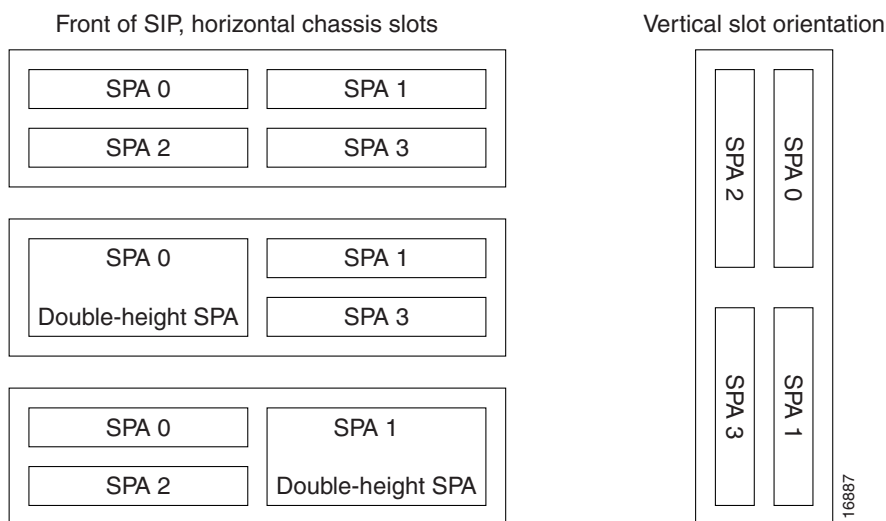


Figure 2-2 Horizontal and Vertical Chassis Slot Orientation for SPAs



SIP subslot 0 is not available on the Cisco ASR 1002 Router as that is the slot occupied by the integrated Route Processor with native Gigabit Ethernet ports.

- Each SPA provides a certain number of connectors, or ports, that are the interfaces to one or more networks. These interfaces can be individually configured using the Cisco IOS command-line interface (CLI).

- Either a blank filler plate or a functional SPA should reside in every subslot of a SIP during normal operation to maintain cooling integrity. Blank filler plates are available in single-height form only.
- SPAs support online insertion and removal (OIR). They can be inserted or removed independently from the SIP. SIPs also support OIR with SPAs inserted in their subslots.

SIP and SPA Compatibility

Table 2-1, Table 2-2, Table 2-3, Table 2-4, and Table 2-5 show SIP and SPA compatibility by SPA technology area on the Cisco ASR 1000 Series Aggregation Services Routers.



Note

For more information about the support for different SIPs and SPAs, refer to the “Release History” section in the “*Overview of the SIP*” chapter of the *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide*.

Table 2-1 SIP and SPA Compatibility for ATM SPAs

SPA	Product ID	SIP Supported: Cisco ASR1000-SIP10	SIP Supported: Cisco ASR1000-SIP40
1-Port Clear Channel OC-3 ATM SPA	SPA-1XOC3-ATM-V2	Yes	Yes
3-Port Clear Channel OC-3 ATM SPA	SPA-3XOC3-ATM-V2	Yes	Yes
1-Port Clear Channel OC-12 ATM SPA	SPA-1XOC12-ATM-V2	Yes	Yes

Table 2-2 SIP and SPA Compatibility for Ethernet SPAs

SPA	Product ID	SIP Supported: Cisco ASR1000-SIP10	SIP Supported: Cisco ASR1000-SIP40
4-Port and 8-Port Fast Ethernet SPA	SPA-4X1FE-TX-V2 SPA-8X1FE-TX-V2	Yes	Yes
1-Port 10-Gigabit Ethernet SPA	SPA-1X10GE-L-V2	Yes	Yes
2-Port Gigabit Ethernet SPA	SPA-2X1GE-V2	Yes	Yes
5-Port Gigabit Ethernet SPA	SPA-5X1GE-V2	Yes	Yes
8-Port Gigabit Ethernet SPA	SPA-8X1GE-V2	Yes	Yes
10-Port Gigabit Ethernet SPA	SPA-10X1GE-V2	Yes	Yes
2-Port Gigabit Synchronous Ethernet SPA	SPA-2X1GE-SYNC E	Yes	Yes

Table 2-3 SIP and SPA Compatibility for Packet Over SONET SPAs

SPA	Product ID	SIP Supported: Cisco ASR1000-SIP10	SIP Supported: Cisco ASR1000-SIP40
1-Port OC-12c/STM-4 POS SPA	SPA-1XOC12-POS	Yes	Yes
2-Port, 4-Port, and 8-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA	SPA-2XOC12-POS SPA-4XOC12-POS SPA-8XOC12-POS	Yes	Yes
2-Port, 4-Port, and 8-Port OC-3c/STM-1 POS SPA	SPA-2XOC3-POS SPA-4XOC3-POS SPA-8XOC3-POS	Yes	Yes
1-Port OC-48c/STM-16 POS SPA	SPA-1XOC48-POS	Yes	Yes
2-Port and 4-Port OC-48c/STM-16 POS/RPR SPA	SPA-2XOC48-POS/R PR SPA-4XOC48-POS/R PR	Yes	Yes
1-Port OC-192c/STM-64 POS/RPR XFP SPA	SPA-1XOC192POS-X FP	Yes	Yes

Table 2-4 SIP and SPA Compatibility for Serial SPAs

SPA	Product ID	SIP Supported: Cisco ASR1000-SIP10	SIP Supported: Cisco ASR1000-SIP40
2-Port and 4-Port T3/E3 Clear Channel Serial SPA	SPA-2XT3/E3 SPA-4XT3/E3	Yes	Yes
2-Port and 4-Port Channelized T3 Serial SPA	SPA-2XCT3/DS0 SPA-4XCT3/DS0	Yes	Yes
4-Port Serial Interface SPA	SPA-4XT-Serial	Yes	Yes ¹
8-Port Channelized T1/E1 Serial SPA	SPA-8XCHT1/E1	Yes	Yes
1-Port Channelized OC-3/STM-1 SPA	SPA-1XCHSTM1/OC3	Yes	Yes
1-Port Channelized OC-12/STM-4 SPA	SPA-1XCHOC12/DS0	Yes	Yes

1. The SPA-4XT-Serial SPA is supported on SIP-40 with the initial Cisco IOS XE Release 3.1.1S when plugged into an ASR1000 SIP-40 linecard.

Table 2-5 SIP and SPA Compatibility for Service SPAs

SPA	Product ID	SIP Supported: Cisco ASR1000-SIP10	SIP Supported: Cisco ASR1000-SIP40
Cisco WebEx Node for ASR 1000 Series	SPA-WMA-K9	Yes	Yes
Cisco DSP SPA for ASR 1000 Series	SPA-DSP	Yes	Yes

Modular Optics Compatibility

Some SPAs implement small form-factor pluggable (SFP) optical transceivers to provide network connectivity. An SFP module is a transceiver device that mounts into the front panel to provide network connectivity.

Cisco qualifies the SFP modules that can be used with SPAs.



Note

The SPAs will only accept the SFP modules listed as supported in this document. An SFP module check is run every time an SFP module is inserted into a SPA and only SFP modules that pass this check will be usable.

Table 2-6, Table 2-7, Table 2-8, Table 2-9, Table 2-10 and Table 2-11 show the types of optics modules that have been qualified for use with a SPA.

For more information about any of the supported transceivers for SPAs in these tables, refer to the Cisco Transceiver Modules site for that module on Cisco.com at:

http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

Table 2-6 ATM SPA Optics Compatibility

SPA	Qualified Optics Modules (Cisco Part Numbers)
1-Port Clear Channel OC-3 ATM SPA	<ul style="list-style-type: none"> • SFP-OC3-MM • SFP-OC3-IR-1 • SFP-OC3-LR-1
3-Port Clear Channel OC-3 ATM SPA	<ul style="list-style-type: none"> • SFP-OC3-MM • SFP-OC3-IR-1 • SFP-OC3-LR-1
1-Port Clear Channel OC-12 ATM SPA	<ul style="list-style-type: none"> • SFP-OC12-MM • SFP-OC12-SR • SFP-OC12-IR1 • SFP-OC12-LR1 • SFP-OC12-LR2

Table 2-7 Gigabit Ethernet SPA Optics Compatibility

SPA	Qualified Optics Modules (Cisco Part Numbers)
1-Port 10-Gigabit Ethernet SPA	<ul style="list-style-type: none"> • XFP-10GLR-OC192SR • XFP-10GER-OC192IR • XFP-10GZR-OC192LR • XFP-10G-MM-SR
2-Port Gigabit Ethernet SPA	<ul style="list-style-type: none"> • GLC-BX-D • GLC-BX-U • SFP-GE-S • SFP-GE-L • SFP-GE-Z • SFP-GE-T
5-Port Gigabit Ethernet SPA	<ul style="list-style-type: none"> • GLC-BX-D • GLC-BX-U • GLC-GE-100FX • SFP-GE-S • SFP-GE-L • SFP-GE-Z • SFP-GE-T
8-Port Gigabit Ethernet SPA	<ul style="list-style-type: none"> • SFP-GE-S • SFP-GE-L • SFP-GE-Z • SFP-GE-T
10-Port Gigabit Ethernet SPA	<ul style="list-style-type: none"> • GLC-BX-D • GLC-BX-U • GLC-GE-100FX • SFP-GE-S • SFP-GE-L • SFP-GE-Z
2-Port Gigabit Synchronous Ethernet SPA	<ul style="list-style-type: none"> • GLC-BX-D • GLC-BX-U • SFP-GE-S • SFP-GE-L • SFP-GE-Z • SFP-GE-T

Table 2-8 *Gigabit Ethernet SPA CWDM Optics Compatibility for All Gigabit Ethernet SPAs Supported on the Cisco ASR 1000 Series Routers*

Qualified Optics Modules (Cisco Part Numbers)
CWDM-SFP-1470=
CWDM-SFP-1490=
CWDM-SFP-1510=
CWDM-SFP-1530=
CWDM-SFP-1550=
CWDM-SFP-1570=
CWDM-SFP-1590=
CWDM-SFP-1610=

Table 2-9 Gigabit Ethernet SPA DWDM Optics Compatibility

SPA	Qualified Optics Modules (Cisco Part Numbers)
2-Port Gigabit Ethernet SPA	DWDM-SFP-3033=
5-Port Gigabit Ethernet SPA	DWDM-SFP-3112=
8-Port Gigabit Ethernet SPA	DWDM-SFP-3190=
10-Port Gigabit Ethernet SPA	DWDM-SFP-3268=
	DWDM-SFP-3425=
	DWDM-SFP-3504=
	DWDM-SFP-3582=
	DWDM-SFP-3661=
	DWDM-SFP-3819=
	DWDM-SFP-3898=
	DWDM-SFP-3977=
	DWDM-SFP-4056=
	DWDM-SFP-4214=
	DWDM-SFP-4294=
	DWDM-SFP-4373=
	DWDM-SFP-4453=
	DWDM-SFP-4612=
	DWDM-SFP-4692=
	DWDM-SFP-4772=
	DWDM-SFP-4851=
	DWDM-SFP-5012=
	DWDM-SFP-5092=
	DWDM-SFP-5172=
	DWDM-SFP-5252=
	DWDM-SFP-5413=
	DWDM-SFP-5494=
	DWDM-SFP-5575=
	DWDM-SFP-5655=
	DWDM-SFP-5817=
	DWDM-SFP-5898=
	DWDM-SFP-5979=
	DWDM-SFP-6061=

Table 2-10 POS SPA SFP Optics Compatibility

SPA	Qualified Optics Modules (Cisco Part Numbers)
2-Port, 4-Port, and 8-Port OC-3c/STM-1 POS SPA	<ul style="list-style-type: none"> • SFP-OC3-MM • SFP-OC3-SR • SFP-OC3-IR1 • SFP-OC3-LR1 • SFP-OC3-LR2
1-Port OC-48c/STM-16 POS SPA	<ul style="list-style-type: none"> • SFP-OC48-SR • SFP-OC48-IR1 • SFP-OC48-LR2
2-Port and 4-Port OC-48c/STM-16 POS/RPR SPA	<ul style="list-style-type: none"> • SFP-OC48-SR • SFP-OC48-IR1 • SFP-OC48-LR2
2-Port, 4-Port, and 8-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA	<ul style="list-style-type: none"> • SFP-OC3-MM, SFP-OC12-MM • SFP-OC3-SR, SFP-OC12-SR • SFP-OC3-IR1, SFP-OC12-IR1 • SFP-OC3-LR1, SFP-OC12-LR1 • SFP-OC3-LR2, SFP-OC12-LR2
1-Port OC-12c/STM-4 POS SPA	<ul style="list-style-type: none"> • SFP-OC12-MM • SFP-OC12-SR • SFP-OC12-IR1 • SFP-OC12-LR1 • SFP-OC12-LR2
1-Port OC-192c/STM-64 POS/RPR XFP SPA	<ul style="list-style-type: none"> • XFP-10GLR-OC192SR • XFP-10GER-OC192IR • XFP-10GZR-OC192LR

Table 2-11 *Serial SPA SFP Optics Compatibility*

SPA	Qualified Optics Modules (Cisco Part Numbers)
1-Port Channelized OC-3/STM-1 SPA	<ul style="list-style-type: none"> • SFP-OC3-MM • SFP-OC3-SR • SFP-OC3-IR1 • SFP-OC3-LR1 • SFP-OC3-LR2
1-Port Channelized OC-12/STM-4 SPA	<ul style="list-style-type: none"> • SFP-OC12-MM • SFP-OC12-SR • SFP-OC12-IR1 • SFP-OC12-LR1 • SFP-OC12-LR2



PART 1

SPA Interface Processor



CHAPTER 3

Overview of the SIP

This chapter provides an overview of the release history, and feature and Management Information Base (MIB) support for the Cisco ASR1000-SIP10 and Cisco ASR1000-SIP40.

This chapter includes the following sections:

- [Release History, page 3-1](#)
- [Supported SIP Features, page 3-2](#)
- [Supported MIBS, page 3-3](#)
- [Command Reference Information, page 3-3](#)

Release History



Note

For release history information about the introduction of SPA support on the SIP, refer to the corresponding “Overview” chapters in the SPA technology sections of this document. In addition, features specific to certain SPA technologies are documented in the corresponding SPA sections of this document.

Release	Modification
Cisco IOS XE 3.1S	Information about the new Cisco ASR1000-SIP40 added.
Cisco IOS XE 2.4	Information added for the following SPAs: <ul style="list-style-type: none">• 2-Port, 4-Port, and 8-Port OC-12 POS SPA• 1-Port OC-48 POS SPA• 8-Port OC-3 POS SPA• 1-Port OC-192 POS SPA• WMA-K9 SPA
Cisco IOS XE 2.3	Information added for the following SPAs: <ul style="list-style-type: none">• 1-Port and 3-Port OC-3 ATM SPA

Cisco IOS XE 2.2	Information added for the following SPAs: <ul style="list-style-type: none"> • 2-Port and 4-Port OC-48c/STM-16 POS/RPR SPA • 1-Port Channelized STM-1/OC-3 SPA
Cisco IOS XE 2.1	First release.

Supported SIP Features

The Cisco ASR1000-SIP10, is a high-performance, feature-rich SPA interface processor that functions as a carrier card for shared port adapters (SPAs) on the Cisco ASR 1000 Series Aggregation Services Routers. The SIP is supported on the Cisco ASR 1000 Series Routers, and is compatible with one or more platform-independent SPAs. For more information on SPA compatibility, see the [“SIP and SPA Compatibility” section on page 2-3](#).

This section provides a list of some of the primary features supported by the SIP hardware and software. For feature compatibility information by SIP and SPA combination, and information about configuring these features, see [Chapter 4, “Configuring the SIP.”](#)

Cisco ASR1000-SIP10 Features

The Cisco ASR1000-SIP10 supports the standard FPD upgrade methods for the Cisco ASR 1000 Series Routers. For more information about FPD support, see [Chapter 26, “Upgrading Field-Programmable Devices.”](#)

Cisco ASR1000-SIP40 Features

The Cisco ASR1000-SIP40 supports upto 40 Gbps total bandwidth for the four SPA bays and 46 Gbps sustained through carrier card when utilizing two four-link 6.25 GHz ESIs. Following are the features of the Cisco ASR1000-SIP40:

- Supports 40 Gbps of nonoversubscribed throughput.
- Compatible with existing and future SPAs, ESPs, and RPs.
- Supports online-insertion-and-removal (OIR) of all SIP-10 SPAs and Cisco ASR1000-SIP40.
- Provides higher port density support of 48 point dual priority, and 96 point single priority.
- Enables enhanced QoS and timestamp support.
- Performs ingress packet prioritization based on Layer 2 or Layer 3 headers.
- Enables the flow-control the SPAs.
- Distributes line clocking reference from a single SPA to the RPs.
- Supports Onboard Failure Logging (OBFL).
- All the SPAs on Cisco ASR1000-SIP40 provide FPD support.



Note

The Cisco ASR1000-SIP40 supports four half-height SPAs, two full-height SPAs, and a combination of two half-height and one full-height SPAs. The Cisco ASR1000-SIP40 does not support double-wide SPAs, double-high SPAs having two connectors.

Cisco ASR1000-SIP10 High-Availability Features

- Online insertion and removal (OIR) of the SIP and SPAs
- Nonstop Forwarding (NSF)
- Stateful switchover (SSO)
- Frame Relay switching
- VC bundle Class of Service (CoS) precedence mapping

Supported MIBS

The following MIBs are supported in Cisco IOS XE Release 2.2 and later releases for the Cisco ASR1000-SIP10 on a Cisco ASR 1000 Series Router:

- ENTITY-MIB (RFC 4133)
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-ALARM-MIB
- ENTITY-SENSOR-MIB (RFC 3433)
- CISCO-ENTITY-SENSOR-MIB
- CISCO-EXTENDED-EXT-MIB

The following MIBs are supported in Cisco IOS XE Release 3.1S and later for the Cisco ASR1000-SIP40 on a Cisco ASR 1000 Series Router:

- ENTITY-MIB (RFC 4133)
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-ALARM-MIB
- ENTITY-SENSOR-MIB (RFC 3433)
- CISCO-ENTITY-SENSOR-MIB
- CISCO-EXTENDED-EXT-MIB

Command Reference Information

For command reference information, refer to the Cisco IOS command reference and master index publications.



CHAPTER 4

Configuring the SIP

This chapter provides information about configuring the SIP on the Cisco ASR 1000 Series Routers. It includes the following sections:

- [Configuration Tasks, page 4-1](#)
- [Resetting a SIP, page 4-5](#)

For information about managing your system images and configuration files, refer to other sections of this document, and the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications that correspond to your Cisco IOS XE software release.

Configuration Tasks

This section describes how to configure the SIP.

It includes the following topics:

- [Identifying Slots and Subslots for the SIP and SPAs, page 4-1](#)
- [Hardware Module Scheduling Commands, page 4-3](#)

Some of the Cisco IOS XE software features on the Cisco ASR 1000 Series Routers are supported on the SIPs. Use this chapter while also referencing the list of supported features on the SIPs in [Chapter 3, “Overview of the SIP.”](#)



Note

When referring to other platform documentation, be sure to note any SIP-specific configuration guidelines described in this document.

Identifying Slots and Subslots for the SIP and SPAs

This section describes how to specify the physical locations of a SIP and SPA on the Cisco ASR 1000 Series Routers within the command-line interface (CLI) to configure or monitor the devices.

Specifying the Slot Location for a SIP

The Cisco ASR 1000 Series Routers support different chassis models, each of which supports a certain number of chassis slots.

- The Cisco ASR 1006 Router supports three chassis slots for SIPs.
- The Cisco ASR 1004 Router supports two chassis slots for SIPs.
- The Cisco ASR 1002 Router supports one chassis slot for a SIP that is permanently installed, and the integrated Route Processor and Gigabit Ethernet ports reside in SPA subslot 0.
- The Cisco ASR 1013 Router supports six chassis slot for SIPs.

Some commands such as **show platform**, **show diag**, and **show diag subslot** allow you to display information about the SIP. However, you must specify the chassis slot location where the SIP about which you want information is installed.

Specifying the SIP Subslot Location for a SPA

SIP subslots begin their numbering with “0” and have a horizontal orientation, as shown in [Figure 4-1](#).

The Cisco ASR 1000 Series SIP supports four subslots for the installation of SPAs. The subslot locations are oriented as follows:

- SIP subslot 0—Top-left subslot
- SIP subslot 1—Top-right subslot
- SIP subslot 2—Bottom-left subslot
- SIP subslot 3—Bottom-right subslot



Note

In the Cisco ASR 1002 Router, SIP subslot 0 is not available for SPA insertion. It is the slot that is used for the integrated Route Processor and Gigabit Ethernet ports.

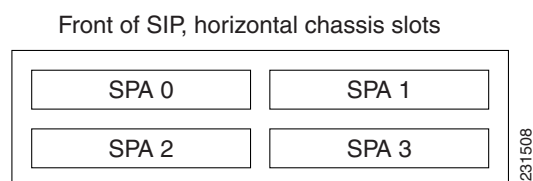


Warning

The slots 4 and 5 on Cisco ASR 1013 Series Router has limitation to support ASR-SIP40 at 40G mode.

[Figure 4-1](#) shows the SPA numbering sequence on a Cisco ASR 1000 Series Routers SIP.

Figure 4-1 Cisco ASR 1000 Series SIP SPA Numbering



The SIP subslot numbering is indicated by a small numeric label beside the subslot on the faceplate.

Just as with the SIPs, some commands allow you to display information about the SPA itself, such as **show diag subslot**. These commands require you to specify both the physical location of the SIP and SPA in the format, *slot/subslot*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Aggregation Services Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.

To display the operational status for a SPA installed in the SIP, enter the **show platform** command.



Note

The Cisco ASR1000-SIP40 supports four half-height SPAs, two full-height SPAs, and a combination of two half-height and one full-height SPAs. The Cisco ASR1000-SIP40 does not support double-wide SPAs and double-high SPAs having two connectors.

The Cisco ASR1000-SIP40 runs on the Cisco ASR1006 and the Cisco ASR 1013 router.



Caution

The ASR 1000-SIP40 is not supported on the Cisco ASR 1002, Cisco ASR 1002-F routers, and Cisco ASR 1004 routers in Cisco IOS XE Software Release 3.1S. Moreover, the ASR1000-SIP40 is supported only on RP-2 and later route processors (not supported on RP-1). From ESP perspective, ASR1000-SIP40 is primarily supported on ESP-40. If you are using RP-1 or ESP-10 or ESP-20, you need to first upgrade the RP-1 to RP-2 followed by upgrading ESP10 or ESP-20 to ESP-40 and then inserting ESP-40 in the system.

The Cisco ASR1000-SIP40 is also compatible with both Cisco ASR1000-RPs and the Cisco ASR 1000 ESP10, ASR1000-ESP20 and the Cisco ASR1000-ESP40 modules. The LEDs on the modules are the same for both the Cisco ASR1000-SIP10 and Cisco ASR1000-SIP40.

Hardware Module Scheduling Commands

The following hardware module scheduling commands are supported on the Cisco ASR 1000 Series Routers.

Command	Purpose
Router(config)# hw-module slot <i>slot-number</i> qos input [bandwidth <i>value_in_Kbps</i> strict priority weight <i>weight</i>]	<p>This is a global configuration command.</p> <ul style="list-style-type: none"> <i>slot-number</i>—Specifies the number of the SIP slot. bandwidth <i>value_in_Kbps</i>—Sets the minimum bandwidth in Kbps for QoS strict priority—Sets the minimum bandwidth for a high priority QoS queue weight <i>weight</i>—Indicates the excess QoS scheduling weight <p>By default, without using this command, each SIP slot has zero minimum bandwidth and its scheduled base has an excess sharing weight proportional to CC's aggregated bandwidth.</p> <p>The no form of this command sets scheduling parameters back to the default.</p>

Ingress Scheduling

Use the following command for ingress scheduling.

Command	Purpose
Router(config)# plim qos input map ip precedence-based	<p>This command enables IP precedence-based classification. By default, without using this command, the Gigabit Ethernet SPA enables IP precedence-based classification for the Cisco ASR 1000 Series Router.</p> <p>The no form of this command disables precedence-based classification.</p>

Resetting a SIP

To reset a SIP, use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# hw-module module slot reload start stop	<p>Resets the SIP in the specified slot, where:</p> <ul style="list-style-type: none"> • <i>slot</i>—Specifies the chassis slot number where the SIP is installed. • reload—Stops the SIP, then automatically restarts the SIP. • start—Starts the SIP taking it out of reset mode. • stop—Stops the SIP holding it in reset mode.



CHAPTER 5

Troubleshooting the SIP

This chapter describes techniques that you can use to troubleshoot the operation of your SIPs.

It includes the following sections:

- [General Troubleshooting Information, page 5-1](#)
- [Using the Cisco IOS Event Tracer to Troubleshoot Problems, page 5-2](#)
- [Preparing for Online Insertion and Removal of the SIP and SPAs, page 5-2](#)

The first section provides information about basic interface troubleshooting.

To perform more advanced troubleshooting, see the other sections in this chapter.

General Troubleshooting Information

This section describes general information for troubleshooting SIPs and SPAs. It includes the following sections:

- [Interpreting Console Error Messages, page 5-1](#)
- [Using debug Commands, page 5-1](#)
- [Using show Commands, page 5-2](#)

Interpreting Console Error Messages

System error messages are organized according to the particular system facility that produces the messages. The SIP error messages use the following facility names:

- ASR1000_SIP
- ASR1000_SIP_SPA

Using debug Commands

Along with the other **debug** commands supported on the Cisco ASR 1000 Series Routers, you can obtain specific debug information for the SIP on the Cisco ASR 1000 Series Aggregation Services Routers using the **debug hw-module** command in privileged EXEC mode.

The **debug hw-module** command is intended for use by Cisco technical support personnel.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

For information about other **debug** commands supported on the Cisco ASR 1000 Series Routers, refer to the *Cisco IOS Debug Command Reference* publications for relevant Cisco IOS releases.

Using show Commands

There are several **show** commands that you can use to monitor and troubleshoot the SIP and SPA on the Cisco ASR 1000 Series Aggregation Services Routers. This chapter describes using the **show hw-module subslot** command to perform troubleshooting of your SPA.

Using the Cisco IOS Event Tracer to Troubleshoot Problems

This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, Route Processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

For more information about using the Event Tracer feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/evnttrcr.html.

Preparing for Online Insertion and Removal of the SIP and SPAs

The Cisco ASR 1000 Series Routers support online insertion and removal (OIR) of the SPA interface processor (SIP), in addition to each of the shared port adapters (SPAs). Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This section includes the following topics on OIR support:

- [Preparing for Online Removal of a SIP, page 5-3](#)
- [Verifying Deactivation and Activation of a SIP, page 5-4](#)
- [Preparing for Online Removal of a SPA, page 5-5](#)

- [Verifying Deactivation and Activation of a SPA, page 5-8](#)
- [Deactivation and Activation Configuration Examples, page 5-8](#)

Preparing for Online Removal of a SIP

The Cisco ASR 1000 Series Routers support OIR of a SIP. To do this, you can power down a SIP (which automatically deactivates any installed SPAs) and remove the SIP with the SPAs still intact.

Although graceful deactivation of a SIP is preferred using the **hw-module slot stop** command, the Cisco ASR 1000 Series Routers do support removal of the SIP without deactivating it first. If you plan to remove a SIP, you can deactivate the SIP first, using the **hw-module slot stop** command in global configuration mode. When you deactivate a SIP using this command, it automatically deactivates each of the SPAs that are installed in that SIP. Therefore, it is not necessary to deactivate each of the SPAs prior to deactivating the SIP.



Note

Either a blank filler plate or a functional SPA should reside in every subslot of a SIP during normal operation.

For more information about the recommended procedures for physical removal of the SIP, refer to the *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide*.

Deactivating a SIP

To deactivate a SIP and its installed SPAs prior to removal of the SIP, use the following command in global configuration mode:

Command	Purpose
Router(config)# hw-module slot slot-number stop	Shuts down any installed interfaces, and deactivates the SIP in the specified slot, where: <ul style="list-style-type: none"> • <i>slot-number</i>—Specifies the chassis slot number where the SIP is installed. • stop—Deactivates the SIP and places it in reset mode.

For more information about chassis slot numbering, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Reactivating a SIP

If you did deactivate the SIP using the **hw-module slot stop** command, then you do not need to reactivate the SPAs after an OIR of the SIP. The installed SPAs automatically reactivate upon reactivation of the SIP in the Cisco ASR 1000 Series Routers.

For example, consider the case where you remove a SIP from the Cisco ASR 1000 Series Routers to replace it with another SIP. You reinstall the same SPAs into the new SIP. When you enter the **hw-module slot start** command on the Cisco ASR 1000 Series Routers, the SPAs automatically reactivate with the new SIP.

To activate a SIP and its installed SPAs after the SIP has been deactivated, use the following command in global configuration mode:

Command	Purpose
Router(config)# hw-module slot <i>slot-number</i> start	<p>Activates the SIP in the specified slot and its installed SPAs, where:</p> <ul style="list-style-type: none"> <i>slot-number</i>—Specifies the chassis slot number where the SIP is installed. start—Activates the SIP and removes it from reset mode.

For more information about chassis slot numbering, see the [“Identifying Slots and Subslots for the SIP and SPAs”](#) section on page 4-1.

Verifying Deactivation and Activation of a SIP

To verify the deactivation of a SIP, enter the **show platform** command in privileged EXEC configuration mode. Observe the State field associated with the SIP that you want to verify.

The following example shows that the Cisco ASR1000-SIP10 located in slot 1 is deactivated.

```
Router# show platform
Chassis type: ASR1006
```

Slot	Type	State	Insert time (ago)
0	ASR1000-SIP10	ok	2d20h
0/0	SPA-1XOC12-POS	ok	2d20h
0/1	SPA-1XOC12-POS	ok	1d21h
0/2	SPA-5X1GE-V2	ok	2d20h
0/3	SPA-4XOC3-POS-V2	ok	2d20h
1	ASR1000-SIP10	disabled	1d23h
R0	ASR1000-RP1	ok, active	1w3d
F0	ASR1000-ESP10	ok, active	1w3d
P0	Unknown	ps, fail	never
P1	Unknown	ps, fail	never

Slot	CPLD Version	Firmware Version
0	06120701	12.2(20071009:051408) [gschnorr-mcp_...
1	07091401	12.2(20070807:170946) [gschnorr-mcp_...
R0	07010515	12.2(33r)XN2
F0	07021400	12.2(20071030:180953) [gschnorr-mcp_...

To verify activation and proper operation of a SIP, enter the **show platform** command and observe “ok” in the State field as shown in the following example:

```
Router# show platform
Chassis type: ASR1006
```

Slot	Type	State	Insert time (ago)
0	ASR1000-SIP10	ok	03:19:46
0/0	SPA-5X1GE-V2	ok	03:18:28

0/1	SPA-8X1FE-TX-V2	ok	03:18:28
0/2	SPA-2XCT3/DS0	ok	03:18:19
1	ASR1000-SIP10	ok	03:19:46
1/0	SPA-2XOC3-POS	ok	03:18:28
1/1	SPA-8XCHT1/E1	ok	03:18:28
1/2	SPA-2XT3/E3	ok	03:18:18
R0	ASR1000-RP1	ok, active	03:19:46
F0	ASR1000-ESP10	ok, active	03:19:46
P0	ASR1006-PWR-AC	ok	03:19:14
P1	ASR1006-FAN	ok	03:19:14

The following example shows the Cisco ASR 1000-SIP10 installed in slot 0 and Cisco ASR1000-SIP40 installed in slots 1,2,3, and 4 for the Cisco ASR 1013 Router:

```
Router#show platform
Chassis type: ASR1013
```

Slot	Type	State	Insert time (ago)
0	ASR1000-SIP10	ok	1w0d
1	ASR1000-SIP40	ok	1w0d
1/1	SPA-5X1GE-V2	ok	1w0d
2	ASR1000-SIP40	ok	1w0d
2/1	SPA-1X10GE-L-V2	ok	1w0d
2/3	SPA-1X10GE-L-V2	ok	1w0d
3	ASR1000-SIP40	ok	1w0d
3/3	SPA-4XT3/E3	ok	1w0d
4	ASR1000-SIP40	ok	1w0d
4/2	SPA-5X1GE-V2	ok	1w0d
4/3	SPA-4XCT3/DS0	ok	1w0d
5	ASR1000-SIP40	ok	1w0d
R0	ASR1000-RP2	ok, active	1w0d
R1	ASR1000-RP2	ok, standby	1w0d
F0	ASR1000-ESP40	ok, active	1w0d
P0	ASR1013-PWR-AC	ok	1w0d
P1	ASR1013-PWR-AC	ps, fail	1w0d
P2	ASR1013-PWR-AC	ok	1w0d
P3	ASR1013-PWR-AC	ps, fail	1w0d

Slot	CPLD Version	Firmware Version
0	00200800	15.0(1r)S
1	00200800	15.0(1r)S
2	00200800	15.0(1r)S
3	00200800	15.0(1r)S
4	00200800	15.0(1r)S
5	00200800	15.0(1r)S
R0	10021901	15.0(1r)S
R1	10021901	15.0(1r)S
F0	1001270D	15.0(1r)S

Preparing for Online Removal of a SPA

The Cisco ASR 1000 Series Routers support OIR of a SPA independently of removing the SIP. This means that a SIP can remain installed in the Cisco Aggregation Services Router-1 with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

If you are planning to remove a SIP along with its SPAs, then you do not need to follow the instructions in this section. To remove a SIP, see the [“Preparing for Online Removal of a SIP”](#) section on page 5-3.

Deactivating a SPA

Although graceful deactivation of a SPA is preferred using the **hw-module subslot stop** command in EXEC mode, the Cisco ASR 1000 Series Routers support removal of the SPA without deactivating it first. Before deactivating a SPA, ensure that the SIP is seated securely into the slot before pulling out the SPA itself.

**Note**

If you are preparing for an OIR of a SPA, it is not necessary to independently shut down each of the interfaces prior to deactivation of the SPA. The **hw-module subslot stop** command in global configuration mode automatically stops traffic on the interfaces and deactivates them along with the SPA in preparation for OIR. In similar fashion, you do not need to independently restart any interfaces on a SPA after OIR of a SPA or SIP.

Choosing the Mode of the hw-module subslot Command

You can deactivate a SPA and all of its interfaces by using the **hw-module subslot** command in one of two modes:

- If you choose to use the **hw-module subslot shutdown** command in global configuration mode, you change the configuration so that no matter how many times the router is rebooted, the SPA will not boot. This command is useful when you need to shut down a SPA in a remote location and ensure that it does not come back up if the router is rebooted.
- If you choose to use the **hw-module subslot stop** command in global configuration mode, you cause the SPA to gracefully shut down. However, the SPA will come up again when executing the **hw-module subslot start** command.

To deactivate a SPA and all of its interfaces prior to removal of the SPA, use the following commands in global configuration mode:

Command	Purpose
Router(config)# hw-module subslot <i>slot-number/subslot-number shutdown [powered unpowered]</i>	Deactivates the SPA in the specified slot and subslot of the SIP, where: <ul style="list-style-type: none"> • <i>slot-number</i>—Specifies the chassis slot number where the SIP is installed. • <i>subslot-number</i>—Specifies the subslot number on a SIP where a SPA is installed. • powered—(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state with power enabled. This is the default state. • unpowered—(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state without power.
Router(config)# hw-module subslot <i>slot-number/subslot-number {reload stop start}</i>	Deactivates the SPA in the specified slot and subslot of the SIP, where: <ul style="list-style-type: none"> • <i>slot-number</i>—Specifies the chassis slot number where the SIP is installed. • <i>subslot-number</i>—Specifies the subslot number on a SIP where a SPA is installed. • reload—Stops and restarts the specified SPA. • stop—Stops the specified SPA. • start—Starts the specified SPA.

For more information about chassis slot and SIP subslot numbering, refer to the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Reactivating a SPA



Note

You do not need to reactivate a SPA after an OIR of either the SIP or a SPA if you did not deactivate the SPA prior to removal when using the **hw-module subslot** command in global configuration mode. If the Cisco Aggregation Services Router-1 is running, then the SPAs automatically start upon insertion into the SIP or with insertion of a SIP into the Cisco Aggregation Services Router-1.

If you deactivate a SPA using the **hw-module subslot stop** command, and need to reactivate it without performing an OIR, you must use the **hw-module subslot start** command to reactivate the SPA and its interfaces.

To activate a SPA and its interfaces after the SPA has been deactivated, use the following command in global configuration mode:

Command	Purpose
Router(config)# no hw-module subslot slot-number/subslot-number shutdown	<p>Activates the SPA and its interfaces in the specified slot and subslot of the SIP, where:</p> <ul style="list-style-type: none"> <i>slot-number</i>—Specifies the chassis slot number where the SIP is installed. <i>subslot-number</i>—Specifies subslot number on a SIP where a SPA is installed.

Verifying Deactivation and Activation of a SPA

When you deactivate a SPA, the corresponding interfaces are also deactivated. This means that these interfaces will no longer appear in the output of the **show interface** command.

To verify the deactivation of a SPA, enter the **show hw-module subslot all oir** command in privileged EXEC mode. Observe the Operational Status field associated with the SPA that you want to verify.

In the following example, the SPA located in subslot 1 of the SIP in slot 2 of the Cisco Aggregation Services Router-1 is administratively down from the **hw-module subslot shutdown** command:

```
Router# show hw-module subslot all oir
Module           Model           Operational Status
-----
subslot 2/0      SPA-1X10GE-L-V2   ok
subslot 2/1      SPA-8X1GE-V2      admin down
```

To verify activation and proper operation of a SPA, enter the **show hw-module subslot all oir** command and observe “ok” in the Operational Status field as shown in the following example:

```
Router# show hw-module subslot all oir
Module           Model           Operational Status
-----
subslot 2/0      SPA-1X10GE-L-V2   ok
subslot 2/1      SPA-8X1GE-V2      ok
```

Deactivation and Activation Configuration Examples

This section provides the following examples of deactivating and activating SIPs and SPAs:

- [Deactivation of a SIP Configuration Example, page 5-8](#)
- [Activation of a SIP Configuration Example, page 5-9](#)
- [Deactivation of a SPA Configuration Example, page 5-9](#)
- [Activation of a SPA Configuration Example, page 5-9](#)

Deactivation of a SIP Configuration Example

Deactivate a SIP when you want to perform OIR of the SIP. The following example deactivates the SIP that is installed in slot 1 of the Cisco Aggregation Services Router-1, its SPAs, and all of the interfaces:

```
Router(config)# hw-module slot 1 stop
```

Activation of a SIP Configuration Example

Activate a SIP if you have previously deactivated it. If you did not deactivate the SPAs, the SPAs automatically reactivate with reactivation of the SIP.

The following example activates the SIP that is installed in slot 1 of the Cisco Aggregation Services Router-1, its SPAs, and all of the interfaces (as long as the **hw-module subslot shutdown** command was not issued to also deactivate the SPA):

```
Router(config)# hw-module slot 1 start
```

There are no corresponding console messages shown with activation using this command. If you re-enter the **hw-module slot start** command, a message is displayed indicating that the module is already enabled.

Deactivation of a SPA Configuration Example

Deactivate a SPA when you want to perform OIR of that SPA. The following example deactivates the SPA (and its interfaces) that is installed in subslot 0 of the SIP located in slot 1 of the Cisco Aggregation Services Router-1 and removes power to the SPA:

```
Router(config)# hw-module subslot 1/0 shutdown unpowered
```

Activation of a SPA Configuration Example

Activate a SPA if you have previously deactivated it. If you have not deactivated a SPA and its interfaces during OIR of a SIP, then the SPA is automatically reactivated upon reactivation of the SIP.

The following example activates the SPA that is installed in subslot 0 of the SIP located in slot 1 of the Cisco Aggregation Services Router-1:

```
Router(config)# no hw-module subslot 1/0 shutdown
```




PART 2

ATM Shared Port Adapters



CHAPTER 6

Overview of the ATM SPAs

This chapter provides an overview of the release history, features, and MIB support for the ATM SPAs on the Cisco ASR 1000 Series Aggregation Services Routers. This chapter includes the following sections:

- [Release History, page 6-2](#)
- [Supported Features, page 6-2](#)
- [Restrictions, page 6-6](#)
- [Supported MIBs, page 6-7](#)
- [SPA Architecture, page 6-8](#)
- [Displaying the SPA Hardware Type, page 6-9](#)

Release History

Release	Modification
Cisco IOS XE Release 2.5	<p>The following SPA support was introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.5:</p> <ul style="list-style-type: none"> • 1-Port Clear Channel OC-12 ATM SPA <p>The following new feature support was introduced for the ATM SPAs in Cisco IOS XE Release 2.5:</p> <ul style="list-style-type: none"> • Access Node Control Protocol (ANCP) • ATM Multipoint Subinterfaces • ATM PVC Ranges • CISCO-PPPOE-MIB • Local Template-Based ATM PVC Provisioning • Point-to-Point Protocol Over Ethernet Over ATM (PPPoEoA) • PPPoE Connection Throttling <p>In addition to the “Configuring the ATM SPAs” chapter in this guide, see also the new features list for Cisco IOS XE Release 2.5 for more details about these features at:</p> <p>http://www.cisco.com/en/US/products/ps9587/products_feature_guides_list.html</p>
Cisco IOS XE Release 2.3	Initial release for the 1-Port Clear Channel OC-3 ATM SPA and 3-Port Clear Channel OC-3 ATM SPA for Cisco ASR 1000 Series Routers.

Supported Features

This section provides a list of some of the primary features supported by the ATM hardware and software:

- [Basic Features, page 6-2](#)
- [SONET/SDH Error, Alarm, and Performance Monitoring, page 6-3](#)
- [Layer 2 Features, page 6-4](#)
- [Layer 3 Features, page 6-4](#)
- [High Availability Features, page 6-6](#)

Basic Features

- Bellcore GR-253-CORE SONET/SDH compliance (ITU-T G.707, G.783, G.957, G.958)
- Interface-compatible with other Cisco ATM adapters

**Note**

The ATM SPA is functionally similar to other ATM port adapters on the Cisco ASR 1000 Series Routers, but because it is a different card type, the configuration for the slot is lost when you replace an existing ATM port adapter with an ATM SPA in a SIP.

- RFC 2684: *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (formerly RFC 1483).
- Supports permanent virtual circuits (PVCs)
- IEEE 802.1QinQ
- ATM adaptation layer 5 (AAL5) for data traffic.
- Uses small form-factor pluggable (SFP) optical transceivers, allowing the same ATM SPA hardware to support multimode (MM), single-mode intermediate (SMI), or single-mode long (SML) reach, depending on the capabilities of the SPA.
- ATM section, line, and path alarm indication signal (AIS) cells, including support for F4 and F5 flows, loopback, and remote defect indication (RDI).
- Operation, Administration, and Maintenance (OAM) cells.
- Online insertion and removal (OIR) of individual ATM SPAs from the SIP, as well as OIR of the SIPs with ATM SPAs installed.

SONET/SDH Error, Alarm, and Performance Monitoring

- Fiber removed and reinserted
- Signal failure bit error rate (SF-BER)
- Signal degrade bit error rate (SD-BER)
- Signal label payload construction (C2)
- Path trace byte (J1)
- Section Diagnostics:
 - Loss of signal (SLOS)
 - Loss of frame (SLOF)
 - Error counts for B1
 - Threshold crossing alarms (TCA) for B1 (B1-TCA)
- Line Diagnostics:
 - Line alarm indication signal (LAIS)
 - Line remote defect indication (LRDI)
 - Line remote error indication (LREI)
 - Error counts for B2
 - Threshold crossing alarms for B2 (B2-TCA)
- Path Diagnostics:
 - Path alarm indication signal (PAIS)
 - Path remote defect indication (PRDI)
 - Path remote error indication (PREI)

- Error counts for B3
 - Threshold crossing alarms for B3 (B3-TCA)
 - Loss of pointer (PLOP)
 - New pointer events (NEWPTR)
 - Positive stuffing event (PSE)
 - Negative stuffing event (NSE)
- The following loopback tests are supported:
 - Network (line) loopback
 - Internal (diagnostic) loopback
- Supported SONET/SDH synchronization:
 - Local (internal) timing (for inter-router connections over dark fiber or wavelength division multiplexing [WDM] equipment)
 - Loop (line) timing (for connecting to SONET/SDH equipment)
 - +/- 4.6 ppm clock accuracy over full operating temperature

Layer 2 Features

- Supports the following encapsulation types:
 - AAL5SNAP (LLC/SNAP)
 - AAL5MUX (VC multiplexing)
 - AAL5NLPID
- Supports the following ATM traffic classes and per-VC traffic shaping modes:
 - Constant bit rate (CBR) with peak rate
 - Unspecified bit rate (UBR) with peak cell rate (PCR)
 - Non-real-time variable bit rate (VBR-nrt)
 - Variable bit rate real-time (VBR-rt)



Note ATM shaping is supported, but class queue-based shaping is not.

- ATM multipoint connections (beginning in Cisco IOS XE Release 2.5)
- ATM point-to-point connections
- Explicit Forward Congestion Indication (EFCI) bit in the ATM cell header
- AToM VP and VC Mode Cell Relay support
- RFC 2225, *Classical IP and ARP over ATM* (obsoletes RFC 1577)

Layer 3 Features

- ATM over MPLS (AToM) in AAL0 VC and VP mode

- No limitation on the maximum number of VCs per VPI, up to the maximum number of 4,096 total VCs per interface (so there is no need to configure this limit using the **atm vc-per-vp** command, which is required on other ATM SPAs)
- OAM flow connectivity using OAM ping for segment or end-to-end loopback
- PVC multicast (Protocol Independent Multicast [PIM] dense and sparse modes)
- PVC ranges (beginning in Cisco IOS XE Release 2.5)
- Supports oversubscription by default
- Routing protocols:
 - Border Gateway Protocol (BGP)
 - Enhanced Interior Gateway Routing Protocol (EIGRP)
 - Interior Gateway Routing Protocol (IGRP)
 - Integrated Intermediate System-to-Intermediate System (IS-IS)
 - Open Shortest Path First (OSPF)
 - Routing Information Protocol version 1 and version 2 (RIPv1 and RIPv2)

High Availability Features

- Route Processor Redundancy (RPR)
- OSPF Nonstop Forwarding (NSF)
- Stateful Switchover (SSO)

Restrictions

- The ATM SPAs in the Cisco ASR 1000 Series Routers do not support APS reflector and reflector channel modes. (These modes require a facing path terminating element [PTE], which is typically a Cisco ATM switch.)
- The ATM SPAs in the Cisco ASR 1000 Series Routers do not support a data path on the main interface. Data is only supported in subinterface configuration.
- Link Fragmentation and Interleaving (LFI) processing is not supported.
- Integrated Local Management Interface (ILMI) is not supported.
- Multipoint subinterfaces are not supported in releases prior to Cisco IOS XE Release 2.5.
- Routed Bridge Encapsulation Subinterface Grouping is not supported.
- For best performance, we recommend the following maximums:

Releases Prior to Cisco IOS XE Release 2.5

In releases before Cisco IOS XE Release 2.5, an absolute maximum of 1,000 (1K) configured VCs per ATM SPA (1,000 [1K] per interface) with the following recommended limitations:

- A recommended maximum number of 1,000 PVCs on all point-to-point subinterfaces for all ATM SPAs in a SIP.
- A recommended maximum number of 1,024 PVCs using service policies for all ATM SPAs in a SIP.

Cisco IOS XE Release 2.5 and Later

Beginning in Cisco IOS XE Release 2.5, the following recommended limits are supported:

- 4,000 VCs per interface
- 12,000 VCs per SPA
- 32,000 VCs per system (Cisco ASR 1000 Series Router)

**Note**

These limits are flexible and depend on all factors that affect performance in the router, such as processor card, type of traffic, and so on.

- A maximum number of 4,000 PVCs configured with Modular QoS CLI (MQC) policy maps.
- In the default configuration of the transmit path trace buffer, the ATM SPA does not support automatic updates of remote host name and IP address (as displayed by the **show controllers atm** command). This information is updated only when the interface is shut down and reactivated (using the **shutdown** and **no shutdown** commands). Information for the received path trace buffer, however, is automatically updated.

- For ATM SPAs on the Cisco ASR1000 series routers, ISSU from releases prior to Cisco IOS XE Release 2.5.0 to Cisco IOS XE Release 2.5.0, or from Cisco IOS XE Release 2.5.0 to a release prior to Cisco IOS XE Release 2.5.0, is not supported. If you want to perform ISSU in this environment, you must first remove the configuration from the ATM SPAs on the router, and then shut down the SPAs using the **shutdown** command prior to running the ISSU process.

Supported MIBs

The following MIBs are supported in Cisco IOS XE Release 2.3 and later releases for the ATM SPAs on the Cisco ASR 1000 Series Routers.

- ATM-MIB
- CISCO-AAL5-MIB
- CISCO-ATM-EXT-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-MPLS-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-MQC-MIB
- CISCO-PPPOE-MIB (beginning in Cisco IOS XE Release 2.5)
- CISCO-SONET-MIB
- ENTITY-MIB
- ENTITY-SENSOR-MIB
- IF-MIB
- MIB-II
- MPLS-CEM-MIB
- OLD-CISCO-CHASSIS-MIB
- SONET-MIB

For more information about MIB support on a Cisco ASR 1000 Series Routers, refer to the *Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide*, at the following URL:

<http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1kmib.html>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

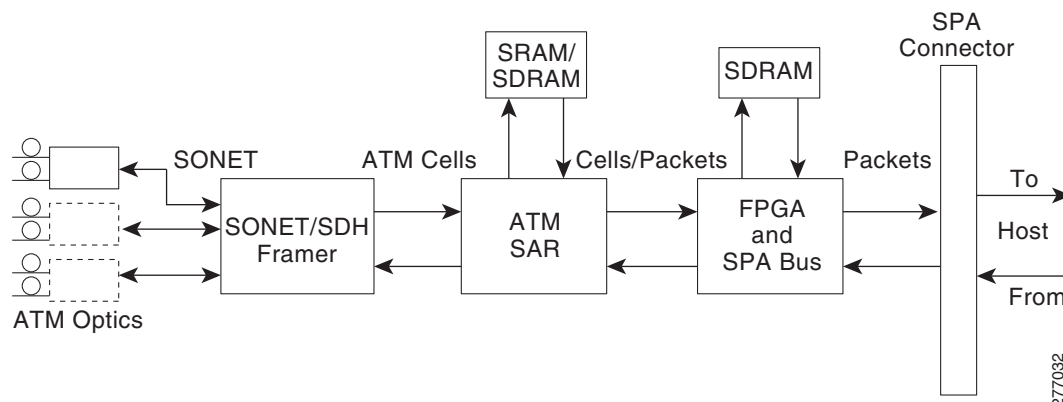
To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

SPA Architecture

This section provides an overview of the data path for the ATM SPAs, for use in troubleshooting and monitoring. Figure 6-1 shows the data path for ATM traffic as it travels between the ATM optical connectors on the front panel of the ATM SPA to the backplane connector that connects the SPA to the SIP.

Figure 6-1 ATM SPA Data Architecture



Note

LFI processing is not supported on the Cisco ASR 1000 Series Routers.

Path of Cells in the Ingress Direction

The following steps describe the path of an ingress cell as it is received from the ATM network and converted to a data packet before transmission through the SIP to the router's processors for switching, routing, or further processing:

1. The SONET/SDH framer device receives incoming cells on a per-port basis from the SPA's optical circuitry. The actual number of optical ports depends on the model of ATM SPA on the Cisco ASR 1000 Series Routers.
2. The SONET/SDH framer removes the SONET overhead information, performs any necessary clock and data recovery, and processes any SONET/SDH alarms that might be present. The framer then extracts the 53-byte ATM cells from the data stream and forwards each cell to the ATM segmentation and reassembly (SAR) engine using one channel per physical port supported by the SPA.

3. The SAR engine receives the cells from the framer and reassembles the cells into the original packets, temporarily storing them in a per-port receive buffer until they can be forwarded (using one channel per physical port) to the field-programmable gate array (FPGA). The SAR engine discards any cells that have been corrupted in transit.

**Note**

Although the SAR in SPA Hardware has two channels to send EBFC and WRED statistics packets to FPGA, the ASR does not enable WRED on SPA. Hence, WRED statistics packets are not sent by SAR to FPGA, but EBFC statistics packets are sent by SAR to FPGA.

4. The FPGA receives the packets from the SAR engine and forwards them to the host processor (using one channel per physical port) for further routing, switching, or additional processing. The FPGA also collects the traffic statistics for the packets that it passes.

Path of Packets in the Egress Direction

The following steps describe the path of an egress packet as the SPA receives it from the router through the SIP and converts it to ATM cells for transmission on the ATM network:

1. The FPGA receives the packets from the host processor (using one channel per physical port) and stores them in its packet buffers until the SAR engine is ready to receive them. The ATM shim header is replaced by the appropriate canonical header for the SAR and the whole packet is forwarded to the SAR.

The FPGA also collects the traffic statistics for the packets that it passes, and any errored packets are flagged and forwarded to the SAR. The FPGA uses two channels to forward traffic to the SAR: one for AAL5 traffic and one for cell unbundling traffic.

2. The SAR engine receives the packets from the FPGA. If any errored data is detected, it is dropped within the SAR. The SAR controls all of the traffic shaping and will drop traffic as necessary due to congestion. The ATM cells are transmitted to the SONET/SDH framer using one channel per physical port.

**Note**

The SPA based L3 QoS features such as WRED and CBWFQ are not enabled for ATM SPAs on Cisco ASR 1000 series routers. The WRED and CBWFQ features are done in the QFP (central processing engine in ESP) as the QFP is more capable of handling these features on Cisco ASR 1000 series routers.

3. The SONET/SDH framer receives the cells from the SAR engine, optionally adds a header check sequence (HCS) and scrambles the cell, and then inserts each cell into the SONET payload, adding the necessary clocking, SONET overhead, and alarm information. The framer also inserts idle cells as needed to fill the payload. The framer then transmits the payload along with the SONET frame complete with all the appropriate section, line and path overhead.
4. The optical port conveys the optical data onto the physical layer of the ATM network.

Displaying the SPA Hardware Type

To verify the SPA hardware type that is installed in your Cisco ASR 1000 Series Routers, use the **show interfaces**, or **show controllers** commands. A number of other **show** commands also provide information about the SPA hardware.

Table 6-1 shows the hardware description that appears in the **show interfaces** command output for each ATM SPA that is supported on the Cisco ASR 1000 Series Routers:

Table 6-1 ATM SPA Hardware Descriptions in show interfaces Command

SPA	Description in show interfaces Command
SPA-1XOC3-ATM-V2	“Hardware is SPA-1XOC3-ATM-V2”
SPA-3XOC3-ATM-V2	“Hardware is SPA-3XOC3-ATM-V2”
SPA-1XOC12-ATM-V2	“Hardware is SPA-1XOC12-ATM-V2”

Example of the show interfaces Command

The following example shows output from the **show interfaces atm** command on a Cisco ASR 1000 Series Routers with an ATM SPA installed in the second subslot of a SIP that is installed in slot 0:

```
Router#show interfaces atm 0/2/2
ATM0/2/2 is up, line protocol is up
  Hardware is SPA-3XOC3-ATM-V2, address is 001a.3044.7522 (bia 001a.3044.7522)
  MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s): AAL5 AAL0
  4095 maximum active VCs, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  4 carrier transitions
  Last input never, output 00:04:11, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 540 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 540 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Example of the show controllers Command

The following example shows output from the **show controllers atm** command on a Cisco ASR 1000 Series Routers with an ATM SPA installed in the second subslot of a SIP that is installed in slot 0:

```
Router# show controllers atm 0/2/2
Interface ATM0/2/2 (SPA-3XOC3-ATM-V2[0/2]) is up
  Framing mode: SONET OC3 STS-3c
  SONET Subblock:
  SECTION
    LOF = 0          LOS   = 1          BIP(B1) = 0
  LINE
    AIS = 0          RDI    = 1          FEBE = 55          BIP(B2) = 0
  PATH
    AIS = 0          RDI    = 1          FEBE = 21          BIP(B3) = 0
```

```
LOP = 1          NEWPTR = 0          PSE = 0          NSE = 0

Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

ATM framing errors:
  HCS (correctable):  0
  HCS (uncorrectable): 0

APS
not configured
COAPS = 0          PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = 13
PATH TRACE BUFFER : STABLE

BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

Clock source:  line
```




CHAPTER 7

Configuring the ATM SPAs

This chapter provides information about configuring the ATM SPAs on the Cisco ASR 1000 Series Aggregation Services Routers. It includes the following sections:

- [Configuration Tasks, page 7-1](#)
- [Verifying the Interface Configuration, page 7-27](#)
- [Configuration Examples, page 7-28](#)

For information about managing your system images and configuration files, refer to the following publications:

- [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#)
- [Cisco IOS XE Configuration Fundamentals Configuration Guide](#), Release 2.

For information about configuration of other features supported in the Cisco IOS XE software on the Cisco ASR 1000 Series Routers, and the commands used in this chapter, see the “[Related Documentation](#)” section on page xxvi.

Configuration Tasks

This section describes the most common configurations for the ATM SPAs on Cisco ASR 1000 Series Router. It contains procedures for the following configurations:

- [Required Configuration Tasks, page 7-2](#)
- [Specifying the Interface Address on a SPA, page 7-4](#)
- [Modifying the Interface MTU Size, page 7-4](#)
- [Creating a Permanent Virtual Circuit, page 7-9](#)
- [Creating a PVC on a Point-to-Point Subinterface, page 7-11](#)
- [Configuring a PVC on a Multipoint Subinterface, page 7-13](#)
- [Configuring a Range of PVCs on a Multipoint Subinterface, page 7-15](#)
- [Configuring Traffic Parameters for PVCs, page 7-17](#)
- [Configuring Virtual Circuit Classes, page 7-20](#)
- [Configuring SONET and SDH Framing, page 7-21](#)
- [Configuring AToM VP Cell Mode Relay Support, page 7-23](#)

- [Configuring QoS Features on ATM SPAs, page 7-24](#)
- [Configuring PPPoEoA on ATM SPAs, page 7-24](#)
- [Saving the Configuration, page 7-25](#)
- [Shutting Down and Restarting an Interface on a SPA, page 7-25](#)

Required Configuration Tasks

Some of the required configuration commands implement default values that might or might not be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command.

To perform the basic configuration on a primary ATM interface, complete the following steps beginning in global configuration mode:



Note

No data path is supported on the primary ATM interface for ATM SPAs on the Cisco ASR 1000 Series Routers.

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port</i>	Enters interface configuration mode for the indicated port on the specified ATM SPA.
Step 2	Router(config-if)# atm clock internal	<p>(Required in back-to-back router configuration) Configures the interface for internal clocking.</p> <p>The default clocking on all ATM interfaces is line clocking, or retrieval of the clock signal from the receive data stream. Therefore, you must configure an internal clock when the ATM link is in back-to-back configuration between two routers. In this case, one end of the link must be configured to use the internal clock.</p> <p>You do not need to configure clocking when the router is connected to a switch, which also uses line clocking by default.</p>
Step 3	Router(config-if)# no atm ilmi-keepalive	Integrated Local Management Interface (ILMI) is not supported on ATM SPAs on the Cisco ASR 1000 Series Routers. This command is the default for all ATM SPAs on the Cisco ASR 1000 Series Routers.
Step 4	Router(config-if)# description <i>string</i>	(Optional) Assigns an arbitrary string, up to 80 characters long, to the interface. This string can identify the purpose or owner of the interface, or any other information that might be useful for monitoring and troubleshooting.
Step 5	Router(config-if)# no shutdown	Enables the interface.
	Note Repeat Step 1 through Step 5 for each port on the ATM SPA to be configured.	
Step 6	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

To perform the basic configuration on each subinterface, use the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.sub-interface</i> [point-to-point multipoint]	Enters subinterface configuration mode for the specified subinterface, where: <ul style="list-style-type: none"> • point-to-point—(Optional) Specifies a point-to-point subinterface for a single PVC configuration. • multipoint—(Optional) Specifies a multipoint subinterface to support PVCs for multiple routers.
Step 2	Router(config-subif)# ip address <i>address mask</i> [secondary]	Assigns the specified IP address and subnet mask to the interface. Repeat the command with the optional secondary keyword to assign additional, secondary IP addresses to the port.
Step 3	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i>	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for <i>vpi/vci</i> are: <ul style="list-style-type: none"> • <i>name</i>—(Optional) An arbitrary string that identifies this PVC. • <i>vpi</i>—Specifies the virtual path identifier (VPI) ID. The valid range is 0 to 255. • <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.
Note When using the pvc command, remember that the <i>vpi/vci</i> combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a <i>vpi/vci</i> combination that has been used on another subinterface, the Cisco IOS software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.		
Step 4	Router(config-subif)# description <i>string</i>	(Optional) Assigns an arbitrary string, up to 80 characters long, to the interface. This string can identify the purpose or owner of the interface, or any other information that might be useful for monitoring and troubleshooting.
Step 5	Router(config-subif)# no shutdown	Enables the interface.
Step 6	Note Repeat Step 1 through Step 5 for each ATM SPA subinterface to be configured.	
Step 7	Router(config-subif)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Specifying the Interface Address on a SPA

Up to four ATM SPAs can be installed in a SIP. SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed.
- *subslot*—Specifies the secondary slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 3:

```
Router(config)# interface serial 3/0/0
```

This command shows a serial SPA as a representative example, however the same *slot/subslot/port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

For more information about identifying slots and subslots, see [Chapter 4, “Identifying Slots and Subslots for the SIP and SPAs”](#).

Modifying the Interface MTU Size

The maximum transmission unit (MTU) values might need to be reconfigured from their defaults on the ATM SPAs to match the values used in your network.

Interface MTU Configuration Guidelines

When configuring the interface MTU size on an ATM SPA, consider the following guidelines.

The Cisco IOS software supports several types of configurable MTU options at different levels of the protocol stack. You should ensure that all MTU values are consistent to avoid unnecessary fragmentation of packets. These MTU values are the following:

- Interface MTU—Configured on a per-interface basis and defines the maximum packet size (in bytes) that is allowed for traffic received on the network. The ATM SPA checks traffic coming in from the network and drops packets that are larger than this maximum value. Because different types of Layer 2 interfaces support different MTU values, choose a value that supports the maximum possible packet size that is possible in your particular network topology.
- IP MTU—Configured on a per-interface or per-subinterface basis and determines the largest maximum IP packet size (in bytes) that is allowed on the IP network without being fragmented. If an IP packet is larger than the IP MTU value, the ATM SPA fragments it into smaller IP packets before forwarding it on to the next hop.
- Multiprotocol Label Switching (MPLS) MTU—Configured on a per-interface or per-subinterface basis and defines the MTU value for packets that are tagged with MPLS labels or tag headers. When an IP packet that contains MPLS labels is larger than the MPLS MTU value, the ATM SPA fragments it into smaller IP packets. When a non-IP packet that contains MPLS labels is larger than the MPLS MTU value, the ATM SPA drops it.

All devices on a particular physical medium must have the same MPLS MTU value to allow proper MPLS operation. Because MPLS labels are added on to the existing packet and increase the packet's size, choose appropriate MTU values so as to avoid unnecessarily fragmenting MPLS-labeled packets.

If the IP MTU or MPLS MTU values are currently the same size as the interface MTU, changing the interface MTU size also automatically sets the IP MTU or MPLS MTU values to the new value. Changing the interface MTU value does not affect the IP MTU or MPLS MTU values if they are not currently set to the same size as the interface MTU.

Different encapsulation methods and the number of MPLS MTU labels add additional overhead to a packet. For example, Subnetwork Access Protocol (SNAP) encapsulation adds an 8-byte header, and each MPLS label adds a 4-byte header. Consider the maximum possible encapsulations and labels that are to be used in your network when choosing the MTU values.

**Tip**

The MTU values on the local ATM SPA interfaces must match the values being used in the ATM network and remote ATM interface. Changing the MTU values on an ATM SPA does not reset the local interface, but be aware that other platforms and ATM SPAs do reset the link when the MTU value changes. This could cause a momentary interruption in service, so we recommend changing the MTU value only when the interface is not being used.

**Note**

The interface MTU value on the ATM SPA also determines which packets are recorded as “giants” in the **show interfaces atm** command. The interface considers a packet to be a giant packet when it is more than 24 bytes larger than the interface MTU size. For example, if using an MTU size of 1500 bytes, the interface increments the giants counter when it receives a packet larger than 1524 bytes.

Interface MTU Configuration Task

To change the MTU values on the ATM SPA interfaces, use the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port</i> or Router(config)# interface atm <i>slot/subslot/port.subinterface</i>	Enters interface configuration mode for the indicated port on the specified ATM SPA, where: <ul style="list-style-type: none"> <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. <i>port</i>—Specifies the number of the individual interface port on a SPA. <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-if)# mtu <i>bytes</i>	(Optional) Configures the maximum transmission unit (MTU) size for the interface. The valid range for <i>bytes</i> is from 64 to 9216 bytes, with a default of 4470 bytes. As a general rule, do not change the MTU value unless you have a specific application need to do so. Note If the IP MTU or MPLS MTU values are currently the same size as the interface MTU, changing the interface MTU size also automatically sets the IP MTU or MPLS MTU values to the same value.
Step 3	Router(config-if)# ip mtu <i>bytes</i>	(Optional) Configures the MTU value, in bytes, for IP packets on this interface. The valid range for an ATM SPA is 64 to 9288, with a default value equal to the MTU value configured in Step 2.
Step 4	Router(config-if)# mpls mtu <i>bytes</i>	(Optional) Configures the MTU value, in bytes, for MPLS-labeled packets on this interface. The valid range for an ATM SPA is 64 to 9216 bytes, with a default value equal to the MTU value configured in Step 2.
	Note Repeat Step 1 through Step 4 for each port on the ATM SPA to be configured.	
Step 5	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the MTU Size

To verify the MTU sizes for an interface, use the **show interfaces**, **show ip interface**, and **show mpls interface** commands, as in the following examples:



Note

The output of the **show interfaces atm** command can display configuration of AAL5 encapsulation, but only AAL0 is supported on the Cisco ASR 1000 Series Routers.

Router# **show interfaces atm 0/2/2**

```
ATM0/2/2 is up, line protocol is up
  Hardware is SPA-3XOC3-ATM-V2, address is 001a.3044.7522 (bia 001a.3044.7522)
  MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s): AAL5 AAL0
  4095 maximum active VCs, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  4 carrier transitions
  Last input never, output 00:04:11, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 540 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 540 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Router# **show ip interface atm 0/2/2.1**

```
ATM0/2/2.1 is up, line protocol is up
  Internet address is 10.4.0.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 4470 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is disabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is disabled
  IP CEF switching turbo vector
  IP Null turbo vector
  Associated unicast routing topologies:
    Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
```

```

Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

```

```
Router# show mpls interface atm 0/3/2.1
```

Interface	IP	Tunnel	BGP	Static	Operational
ATM0/3/2.1	Yes (ldp)	No	No	No	Yes

```
CE1#sh mpls int atm0/3/2.1 det
```

```

Interface ATM0/3/2.1:
  IP labeling enabled (ldp):
    Interface config
  LSP Tunnel labeling not enabled
  BGP labeling not enabled
  MPLS operational
  MTU = 4470

```

To view the maximum possible size for datagrams passing out the interface using the configured MTU value, use the **show atm interface atm** command:

```
Router# show atm interface atm 0/2/2
```

```

Interface ATM0/2/2:
AAL enabled:  AAL0 , Maximum VCs: 4095, Current VCCs: 1

```

```

Max. Datagram Size: 4528
PLIM Type: SONET - 155000Kbps, TX clocking: LINE
Cell-payload scrambling: ON
sts-stream scrambling: ON
5 input, 5 output, 0 IN fast, 0 OUT fast, 0 out drop
  Avail bw = 149760
Config. is ACTIVE

```

Creating a Permanent Virtual Circuit

To use a permanent virtual circuit (PVC), configure the PVC in both the router and the ATM switch. PVCs remain active until the circuit is removed from either configuration. To create a PVC on the ATM interface and enter interface ATM VC configuration mode, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.subinterface</i>	Enters subinterface configuration mode for the specified port on the ATM SPA, where: <ul style="list-style-type: none"> <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. <i>port</i>—Specifies the number of the individual interface port on a SPA. <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-if)# ip address <i>address mask</i>	Assigns the specified IP address and subnet mask to the interface or subinterface.
Step 3	Router(config-if)# atm tx-latency <i>milliseconds</i>	(Optional) Configures the default transmit latency for VCs on this ATM SPA interface. The valid range for <i>milliseconds</i> is from 1 to 200, with a default of 100 milliseconds.
Step 4	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i>	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for <i>vpi/vci</i> are: <ul style="list-style-type: none"> <i>name</i>—(Optional) An arbitrary string that identifies this PVC. <i>vpi</i>—Specifies the VPI ID. The valid range is 0 to 255. <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.

Note When using the **pvc** command, remember that the *vpi/vci* combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a *vpi/vci* combination that has been used on another subinterface, the Cisco IOS software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.

	Command or Action	Purpose
Step 5	Router(config-if-atm-vc)# protocol <i>protocol</i> { <i>protocol-address</i> inarp } [[no] broadcast]	<p>Configures the PVC for a particular protocol and maps it to a specific <i>protocol-address</i>.</p> <ul style="list-style-type: none"> <i>protocol</i>—Typically set to ip or pppoe, but other values are possible. <p>Note PPP is not supported on the Cisco ASR 1000 Series Routers, and PPPoE is supported beginning in Cisco IOS XE Release 2.5.</p> <ul style="list-style-type: none"> <i>protocol-address</i>—Destination address or virtual interface template for this PVC (if appropriate for the <i>protocol</i>). inarp—Specifies that the PVC uses Inverse ARP to determine its address. [no] broadcast—(Optional) Specifies that this mapping should (or should not) be used for broadcast packets.
Step 6	Router(config-if-atm-vc)# inarp <i>minutes</i>	(Optional) If using Inverse ARP, configures how often the PVC transmits Inverse ARP requests to confirm its address mapping. The valid range is 1 to 60 minutes, with a default of 15 minutes.
Step 7	Router(config-if-atm-vc)# encapsulation { aal5mux <i>protocol</i> aal5nlpid aal5snap }	<p>(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where:</p> <ul style="list-style-type: none"> aal5mux <i>protocol</i>—AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. Possible values for the <i>protocol</i> argument are as follows: aal5nlpid—AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. aal5snap—AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default.
Step 8	Router(config-if-atm-vc)# tx-limit <i>buffers</i>	(Optional) Specifies the number of transmit buffers for this VC. The valid range is from 1 to 57343, with a default value that is based on the current VC line rate and on the latency value that is configured with the atm tx-latency command.
	Note Repeat Step 4 through Step 7 for each PVC to be configured on this interface.	
Step 9	Router(config-if-atm-vc)# end	Exits ATM VC configuration mode and returns to privileged EXEC mode.

Verifying a PVC Configuration

To verify the configuration of a particular PVC, use the **show atm pvc** command:

```
Router# show atm pvc
```

Interface	VCD / Name	VPI	VCI	Type	Encaps	SC	Peak Kbps	Av/Min Kbps	Burst Cells	St
0/2/2.1	1	2	32	PVC	SNAP	UBR	149760			UP



Tip

To verify the configuration and current status of all PVCs on a particular interface, you can also use the **show atm vc interface atm** command.

Creating a PVC on a Point-to-Point Subinterface

Use point-to-point subinterfaces to provide each pair of routers with its own subnet. When you create a PVC on a point-to-point subinterface, the router assumes it is the only point-to-point PVC that is configured on the subinterface, and it forwards all IP packets with a destination IP address in the same subnet to this VC. To configure a point-to-point PVC, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.subinterface point-to-point</i>	Creates the specified point-to-point subinterface on the given port on the specified ATM SPA, and enters subinterface configuration mode, where: <ul style="list-style-type: none"> <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. <i>port</i>—Specifies the number of the individual interface port on a SPA. <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-subif)# ip address <i>address mask</i>	Assigns the specified IP address and subnet mask to this subinterface.
Step 3	Router(config-subif)# pvc [<i>name</i>] <i>vpi/vci</i>	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for <i>vpi/vci</i> are: <ul style="list-style-type: none"> <i>name</i>—(Optional) An arbitrary string that identifies this PVC. <i>vpi</i>—Specifies the VPI ID. The valid range is 0 to 255. <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.

	Command or Action	Purpose
	<p>Note When using the pvc command, remember that the <i>vpi/vci</i> combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a <i>vpi/vci</i> combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.</p>	
Step 4	Router(config-if-atm-vc)# protocol <i>protocol</i> <i>protocol-address</i> [[no] broadcast]	<p>Configures the PVC for a particular protocol and maps it to a specific <i>protocol-address</i>.</p> <ul style="list-style-type: none"> <i>protocol</i>—Typically set to ip or pppoe for point-to-point subinterfaces, but other values are possible. <p>Note PPP is not supported on the Cisco ASR 1000 Series Routers, and PPPoE is supported beginning in Cisco IOS XE Release 2.5.</p> <ul style="list-style-type: none"> <i>protocol-address</i>—Destination address or virtual template interface for this PVC (as appropriate for the specified <i>protocol</i>). [no] broadcast—(Optional) Specifies that this mapping should (or should not) be used for broadcast packets. <p>The protocol command also has an inarp option, but this option is not meaningful on point-to-point PVCs that use a manually configured address.</p>
Step 5	Router(config-if-atm-vc)# encapsulation { aal5mux <i>protocol</i> aal5nlpid aal5snap }	<p>(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where:</p> <ul style="list-style-type: none"> aal5mux <i>protocol</i>—AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. aal5nlpid—(IP only) AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. aal5snap—AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default.
	<p>Note Repeat Step 1 through Step 5 for each point-to-point subinterface to be configured on this ATM SPA.</p>	
Step 6	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

**Tip**

To verify the configuration and current status of all PVCs on a particular interface, you can also use the **show atm vc interface atm** command.

Configuring a PVC on a Multipoint Subinterface

Creating a multipoint subinterface allows you to create a point-to-multipoint PVC that can be used as a broadcast PVC for all multicast requests. To create a PVC on a multipoint subinterface, use the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.subinterface multipoint</i>	Creates the specified point-to-multipoint subinterface on the given port on the specified ATM SPA, and enters subinterface configuration mode, where: <ul style="list-style-type: none"> • <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. • <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. • <i>port</i>—Specifies the number of the individual interface port on a SPA. • <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-subif)# ip address <i>address mask</i>	Assigns the specified IP address and subnet mask to this subinterface.
Step 3	Router(config-subif)# no ip directed-broadcast	(Optional) Disables the forwarding of IP directed broadcasts, which are sometimes used in denial of service (DOS) attacks.
Step 4	Router(config-subif)# pvc [<i>name</i>] <i>vpi/vci</i>	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for <i>vpi/vci</i> are: <ul style="list-style-type: none"> • <i>name</i>—(Optional) An arbitrary string that identifies this PVC. • <i>vpi</i>—Specifies the VPI ID. The valid range is 0 to 255. • <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.

Note When using the **pvc** command, remember that the *vpi/vci* combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a *vpi/vci* combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.

	Command or Action	Purpose
Step 5	Router(config-if-atm-vc)# protocol <i>protocol</i> { <i>protocol-address</i> inarp } broadcast	<p>Configures the PVC for a particular protocol and maps it to a specific <i>protocol-address</i>.</p> <ul style="list-style-type: none"> <i>protocol</i>—Typically set to ip or pppoe, but other values are possible. <p>Note PPP is not supported on the Cisco ASR 1000 Series Routers, and PPPoE is supported beginning in Cisco IOS XE Release 2.5.</p> <ul style="list-style-type: none"> <i>protocol-address</i>—Destination address or virtual template interface for this PVC (if appropriate for the <i>protocol</i>). inarp—Specifies that the PVC uses Inverse ARP to determine its address. broadcast— Specifies that this mapping should be used for multicast packets.
Step 6	Router(config-if-atm-vc)# inarp <i>minutes</i>	(Optional) If using Inverse ARP, configures how often the PVC transmits Inverse ARP requests to confirm its address mapping. The valid range is 1 to 60 minutes, with a default of 15 minutes.
Step 7	Router(config-if-atm-vc)# encapsulation { aal5mux <i>protocol</i> aal5nlpid aal5snap }	<p>(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where:</p> <ul style="list-style-type: none"> aal5mux <i>protocol</i>—AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. aal5nlpid—(IP only) AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. aal5snap—AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default.
Note Repeat Step 1 through Step 7 for each multipoint subinterface to be configured on this ATM SPA.		
Step 8	Router(config-if-atm-vc)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying a Multipoint PVC Configuration

To verify the configuration of a particular PVC, use the **show atm pvc** command:

```
Router# show atm pvc 1/120
```

```
ATM3/1/0.120: VCD: 1, VPI: 1, VCI: 120
UBR, PeakRate: 149760
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
```

```
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC status: Not Managed
ILMI VC status: Not Managed
InARP frequency: 15 minutes(s)
Transmit priority 3
InPkts: 1394964, OutPkts: 1395069, InBytes: 1833119, OutBytes: 1838799
InPRoc: 1, OutPRoc: 1, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 94964, OutAS: 95062
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPiErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

**Note**

To verify the configuration and current status of all PVCs on a particular interface, you can also use the **show atm vc interface atm** command.

Configuring a Range of PVCs on a Multipoint Subinterface

Beginning in Cisco IOS XE Release 2.5, you can configure a range of PVCs on an ATM multipoint subinterface.

To create a range of PVCs on a multipoint subinterface, use the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.subinterface</i> multipoint	Creates the specified point-to-multipoint subinterface on the given port on the specified ATM SPA, and enters subinterface configuration mode, where: <ul style="list-style-type: none"> <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. <i>port</i>—Specifies the number of the individual interface port on a SPA. <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-subif)# range [<i>range-name</i>] pvc [<i>start-vpi</i>] <i>start-vci</i> [<i>end-vpi</i>] <i>end-vci</i>	Configures multiple PVCs in the specified range and enters ATM PVC range configuration mode, where: <ul style="list-style-type: none"> <i>range-name</i>—(Optional) Identifies this PVC range with a text string. <i>start-vpi</i>—(Optional) Specifies the beginning VPI ID in the range from 0 to 255. The default is 0. <i>start-vci</i>—Specifies the beginning VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used. <i>end-vpi</i>—(Optional) Specifies the ending VPI ID in the range from 0 to 255. If you don't specify an <i>end-vpi</i> value, the <i>end-vpi</i> value defaults to the <i>start-vpi</i> value. <i>end-vci</i>—Specifies the ending VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used.
Step 3	Once you configure the PVC range, you can configure other commands, such as the protocol command, for all PVCs in the specified range, and you also can go on to define options for individual PVCs using the pvc-in-range	
Step 4	Router(config-if-atm-range-pvc)# pvc-in-range [<i>name</i>] [<i>vpi/vci</i>]	(Optional) Defines an individual PVC within a PVC range, where: <ul style="list-style-type: none"> <i>name</i>—(Optional) Identifies a name for the PVC. The PVC name can have a maximum of 15 characters. <i>vpi/vci</i>—(Optional) VPI for this PVC, from 0 to 255. The default is 0. The VCI value can be in range from 32 to 65535.
Step 5	Once you specify a specific PVC in the range, you can continue to configure options that are specific to that PVC, such as the class-vc command.	
Step 6	Router(config-if-atm-vc-range-pvc)# end	Exits ATM PVC range configuration mode and returns to privileged EXEC mode.

Configuring Traffic Parameters for PVCs

After creating a PVC, you can also configure it for the type of traffic quality of service (QoS) class to be used over the circuit:

- Constant Bit Rate (CBR)—Configures the CBR service class and specifies the average cell rate for the PVC.
- Unspecified Bit Rate (UBR)—Configures the UBR service class and specifies the output peak rate (PCR) for the PVC. This is the default configuration.
- Variable Bit Rate–Non-real Time (VBR-nrt)—Configures the VBR-nrt service class and specifies the output PCR, output sustainable cell rate (SCR), and output maximum burst size (MBS) for the PVC.
- Variable Bit Rate–Real Time (VBR-rt)—Configures the VBR-rt service class and the peak rate and average rate burst for the PVC.

Each service class is assigned a different transmit priority, which the Cisco ASR 1000 Series Router uses to determine which queued cell is chosen to be transmitted out of an interface during any particular cell time slot. This ensures that real-time QoS classes have a higher likelihood of being transmitted during periods of congestion. [Table 7-1](#) lists the ATM QoS classes and their default transmit priorities.

Table 7-1 *ATM Classes of Service and Default Transmit Priorities*

Service Category	Transmit Priority
CBR	0 (highest)
VBR-rt	1
VBR-nrt	2
UBR	3

You can configure a PVC for only one QoS service class. If you enter more than one type, only the most recently configured QoS class takes effect on the circuit.

To configure the traffic parameters for a PVC, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port</i> or Router(config)# interface atm <i>slot/subslot/port.subinterface</i> [multipoint point-to-point]	Enters interface or subinterface configuration mode for the indicated port on the specified ATM SPA, where: <ul style="list-style-type: none"> • <i>slot</i>—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. • <i>subslot</i>—Specifies the secondary slot of the SIP where the SPA is installed. • <i>port</i>—Specifies the number of the individual interface port on a SPA. • <i>subinterface</i>—Specifies the number of the subinterface.
Step 2	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i>	Specifies the PVC to be configured, and enters PVC configuration mode, where: <ul style="list-style-type: none"> • <i>name</i>—(Optional) An arbitrary string that identifies this PVC. • <i>vpi</i>—Specifies the VPI ID. The valid range is 0 to 255. • <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.
	Note When using the pvc command, remember that the <i>vpi/vci</i> combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a <i>vpi/vci</i> combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.	
Step 3	Router(config-if-atm-vc)# cbr <i>rate</i>	Configures constant bit rate (CBR) quality of service (QoS) and average cell rate for the PVC: <ul style="list-style-type: none"> • <i>rate</i>—Average cell rate in kbps. The valid range is 48 to 149760 (OC-3) or 599040 (OC-12).
	or	
	Router(config-if-atm-vc)# ubr <i>output-pcr</i>	Configures unspecified bit rate (UBR) quality of service (QoS) and peak cell rate (PCR) for the PVC: <ul style="list-style-type: none"> • <i>output-pcr</i>—Output PCR in kbps. The valid range is 48 to 149760 (OC-3) or 599040 (OC-12).
	or	

	Command or Action	Purpose
	Router(config-if-atm-vc)# vbr-nrt <i>output-pcr output-scr output-mbs</i>	Configures the variable bit rate–nonreal time (VBR-nrt) QoS, the peak cell rate (PCR), sustainable cell rate (SCR), and maximum burst cell size (MBS) for the PVC: <ul style="list-style-type: none"> <i>output-pcr</i>—Output PCR in kbps. The valid range is 48 to 149760 (OC-3) or 599040 (OC-12). <i>output-scr</i>—Output SCR in kbps. The valid range is 48 to PCR, and typically is less than the PCR value. <i>output-mbs</i>—Output MBS in number of cells. The valid range is 1 to 65535, depending on the PCR and SCR values. If the PCR and SCR are configured to the same value, the only valid value for MBS is 1.
	or	
	Router(config-if-atm-vc)# vbr-rt <i>pcr scr burst</i>	Configures the variable bit rate–real time (VBR-rt) QoS, and the PCR, average cell rate (ACR), and burst cell size (BCS) for the PVC: <ul style="list-style-type: none"> <i>pcr</i>—PCR in kbps. The valid range is 48 to 149760 (OC-3) or 599040 (OC-12). <i>scr</i>—SCR in kbps. The valid range is 48 to PCR, and typically is less than the PCR value. <i>burst</i>—Burst size in number of cells. The valid range is 1 to 65535, depending on the PCR and SCR values. If the PCR and SCR are configured to the same value, the only valid value for <i>burst</i> is 1.
	Note Repeat Step 2 through Step 3 for each PVC to be configured.	
Step 4	Router(config-if-atm-vc)# end	Exits PVC configuration mode and returns to privileged EXEC mode.

Verifying the Traffic Parameter Configuration

Use the **show atm vc** command to verify the configuration of the traffic parameters for a PVC:

```
Router# show atm vc
```

Codes: DN - DOWN, IN - INACTIVE

VCD /							Peak	Av/Min	Burst
Interface	Name	VPI	VCI	Type	Encaps	SC	Kbps	Kbps	Cells St
0/2/2.1	1	2	32	PVC	SNAP	UBR	149760		UP

To verify the configuration of all PVCs on an interface, use the **show atm vc interface atm** command:

```
Router# show atm vc interface atm 0/2/2.1
```

VCD /							Peak	Av/Min	Burst
Interface	Name	VPI	VCI	Type	Encaps	SC	Kbps	Kbps	Cells St
0/2/2.1	1	2	32	PVC	SNAP	UBR	149760		UP

Configuring Virtual Circuit Classes

When multiple PVCs use the same or similar configurations, you can simplify the Cisco ASR 1000 Series Router's configuration file by creating virtual circuit (VC) classes. Each VC class acts as a template, which you can apply to an ATM subinterface, or to individual PVCs.

When you apply a VC class to an ATM subinterface, all PVCs created on that subinterface inherit the VC class configuration. When you apply a VC class to an individual PVC, that particular PVC inherits the class configuration.

You can then customize individual PVCs with further configuration commands. Any commands that you apply to individual PVCs take precedence over those of the VC class that were applied to the interface or to the PVC.

To create and configure a VC class, and then apply it to a subinterface or individual PVC, use the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# vc-class atm <i>vc-class-name</i>	Creates an ATM virtual circuit (VC) class and enters VC-class configuration mode. <ul style="list-style-type: none"> <i>vc-class-name</i>—Arbitrary name to identify this particular VC class.
Step 2	Router(config-vc-class)# <i>configuration-commands</i>	Enter any PVC configuration commands for this VC class.
Step 3	Router(config-vc-class)# interface atm <i>slot/subslot/port</i> or Router(config-vc-class)# interface atm <i>slot/subslot/port.subinterface</i> [multipoint point-to-point]	Enters subinterface configuration mode for the specified ATM subinterface.
Step 4	Router(config-if)# class-int <i>vc-class-name</i> or Router(config-subif)# class-int <i>vc-class-name</i>	(Optional) Applies a VC class on the ATM subinterface. This class then applies to all PVCs that are created on that interface. <ul style="list-style-type: none"> <i>vc-class-name</i>—Name of the VC class that was created in Step 1.
Step 5	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i> or for a subinterface: Router(config-subif)# pvc [<i>name</i>] <i>vpi/vci</i>	Specifies the PVC to be configured, and enters PVC configuration mode, where: <ul style="list-style-type: none"> <i>name</i>—(Optional) An arbitrary string that identifies this PVC. <i>vpi</i>—Specifies the VPI ID. The valid range is 0 to 255. <i>vci</i>—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers.
	Note When using the pvc command, remember that the <i>vpi/vci</i> combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a <i>vpi/vci</i> combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.	

	Command or Action	Purpose
Step 6	Router(config-if-atm-vc)# class-vc <i>vc-class-name</i>	Assigns the specified VC class to this PVC. <ul style="list-style-type: none"> <i>vc-class-name</i>—Name of the VC class that was created in Step 1.
Step 7	Router(config-if-atm-vc)# <i>configuration-commands</i>	Any other VC configuration commands to be applied to this particular PVC. Commands that are applied to the individual PVC supersede any conflicting commands that were specified in the VC class.
Step 8	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Virtual Circuit Class Configuration

To verify the virtual circuit class configuration, use the **show atm vc** command:

```
Router# show atm vc
```

```
Codes: DN - DOWN, IN - INACTIVE
```

Interface	VCD / Name	VPI	VCI	Type	Encaps	SC	Peak Kbps	Av/Min Kbps	Burst Cells	St
0/2/2.1	1	2	32	PVC	SNAP	UBR	149760			UP

Configuring SONET and SDH Framing

The default framing on the ATM OC-3 SPAs is SONET, but the interfaces also support SDH framing.



Note

In ATM environments, the key difference between SONET and SDH framing modes is the type of cell transmitted when no user or data cells are available. The ATM forum specifies the use of idle cells when unassigned cells are not being generated. More specifically, in Synchronous Transport Module-X (STM-X) mode, an ATM interface sends idle cells for cell-rate decoupling. In Synchronous Transport Signal-Xc (STS-Xc) mode, the ATM interface sends unassigned cells for cell-rate decoupling.

To change the framing type and configure optional parameters, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port</i>	Enters interface configuration mode for the indicated port on the specified ATM SPAs.
Step 2	Router(config-if)# atm clock internal	(Optional) Configures the interface to use its own internal (onboard) clock to clock transmitted data. The default (no atm clock internal) configures the interface to use the transmit clock signal that is recovered from the receive data stream, allowing the switch to provide the clocking source.
Step 3	Router(config-if)# atm framing {sdh sonet}	(Optional) Configures the interface for either SDH or SONET framing. The default is SONET.

	Command or Action	Purpose
Step 4	Router(config-if)# [no] atm sonet report {all b1-tca b2-tca b3-tca default lais lrdi pais plop pplm prdi ptim puneq sd-ber sf-ber slof slos}	(Optional) Enables ATM SONET alarm reporting on the interface. The default is for all reports to be disabled. You can enable an individual alarm, or you can enable all alarms with the all keyword. This command also supports a none [ignore] option, which cannot be used with any of the other options. See the “ Configuring AToM VP Cell Mode Relay Support ” section on page 7-23
Step 5	Router(config-if)# [no] atm sonet-threshold {b1-tca value b2-tca value b3-tca value sd-ber value sf-ber value}	(Optional) Configures the BER threshold values on the interface. The value specifies a negative exponent to the power of 10 (10 to the power of minus <i>value</i>) for the threshold value. The default values are the following: <ul style="list-style-type: none"> • b1-tca = 6 (10e-6) • b2-tca = 6 (10e-6) • b3-tca = 6 (10e-6) • sd-ber = 6 (10e-6) • sf-ber = 3 (10e-3)
Step 6	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the SONET and SDH Framing Configuration

To verify the framing configuration, use the **show controllers atm** command:

```
Router# show controllers atm 0/2/2
Interface ATM0/2/2 (SPA-3XOC3-ATM-V2[0/2]) is up
  Framing mode: SONET OC3 STS-3c
  SONET Subblock:
  SECTION
    LOF = 0          LOS      = 1          BIP(B1) = 0
  LINE
    AIS = 0          RDI      = 1          FEBE = 55          BIP(B2) = 0
  PATH
    AIS = 0          RDI      = 1          FEBE = 21          BIP(B3) = 0
    LOP = 1          NEWPTR = 0          PSE  = 0          NSE      = 0

Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

ATM framing errors:
  HCS (correctable):  0
  HCS (uncorrectable): 0

APS
not configured
COAPS = 0          PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = 13
```

```

PATH TRACE BUFFER : STABLE

BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

Clock source:  line

```

Configuring AToM VP Cell Mode Relay Support

To configure Any Transport over MPLS (AToM) Cell Mode Relay, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm <i>slot/subslot/port.subinterface multipoint</i>	Enters interface configuration mode for the indicated port on the specified ATM SPA
Step 2	Router(config-if)# no ip address <i>ip-address mask</i>	Removes the IP address that is assigned to this interface (if one has been configured).
Step 3	Router(config-if)# atm pvp vpi l2transport	Creates a permanent virtual path (PVP) used to multiplex (or bundle) one or more virtual circuits (VCs).
Step 4	Router(config-if)# xconnect <i>peer-ip-address vc-id {encapsulation mpls pw-class pw-class-name}</i>	Routes Layer 2 packets over a specified point-to-point VC by using ATM over multiprotocol label switching (AToM).
Step 5	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

VP Mode Configuration Guidelines

When configuring ATM Cell Relay over MPLS in VP mode, use the following guidelines:

- You do not need to enter the **encapsulation aal0** command in VP mode, but only AAL0 encapsulation is supported with MPLS l2transport.
- One ATM interface can accommodate multiple types of ATM connections. VP cell relay and VC cell relay can coexist on one ATM interface.
- If a VPI is configured for VP cell relay, you cannot configure a PVC using the same VPI.
- VP trunking (mapping multiple VPs to one emulated VC label) is not supported in this release. Each VP is mapped to one emulated VC.
- Each VP is associated with one unique emulated VC ID. The AToM emulated VC type is ATM VP Cell Transport.
- The AToM control word is supported. However, if a peer PE does not support the control word, it is disabled. This negotiation is done by LDP label binding.
- VP mode (and VC mode) drop idle cells.

VP Mode Configuration Example

The following example transports single ATM cells over a virtual path:

```
Router(config)# pseudowire-class vp-cell-relay
```

```

Router(config-pw)# encapsulation mpls
Router(config-pw)# exit
Router(config)# interface atm 1/2/0.1 multipoint
Router(config-if)# atm pvp 1 l2transport
Router(config-if)# xconnect 10.0.0.1 123 pw-class vp-cell-relay

```

Verifying ATM Cell Relay VP Mode

The following **show atm vp** command shows that the interface is configured for VP mode cell relay:

```

Router# show atm vp 1
ATM5/0 VPI: 1, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
VCD    VCI    Type    InPkts    OutPkts    AAL/Encap    Status
6      3      PVC     0         0         F4 OAM       ACTIVE
7      4      PVC     0         0         F4 OAM       ACTIVE
TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0

```

Configuring QoS Features on ATM SPAs

The Cisco ASR1000-SIP10 and the ATM SPAs on the Cisco ASR 1000 Series Routers support the following two areas of QoS:

- ATM SPA QoS—QoS on the ATM SPA is implemented in the segmentation and reassembly (SAR) function using the ATM traffic classes (CBR, VBR-nrt, VBR-rt, and UBR) configured with PCR and SCR values.
- Modular QoS CLI (MQC)—Supports per-VC policy maps with class-based weighted fair queueing (CBWFQ), weighted random early detection (WRED), priority, shaping, bandwidth remaining ratio, bandwidth remaining percent, and policing.

For more information about configuring QoS features in Cisco IOS XE software on the Cisco ASR 1000 Series Routers, refer to the [Cisco IOS XE Quality of Service Solutions Configuration Guide](#), Release 2.

Configuring PPPoEoA on ATM SPAs

Beginning in Cisco IOS XE Release 2.5, you can configure PPP over Ethernet (PPPoE) on ATM (PPPoEoA) to connect a network of hosts over a simple bridging-access device to a remote access concentrator. For more information about this feature, refer to the “PPPoE on ATM” feature from the New Features in Cisco IOS XE Release 2.5 at:

http://www.cisco.com/en/US/products/ps9587/products_feature_guides_list.html

For a sample configuration, see the “PPPoEoA VC Class and PVC Range Configuration Example” section on page 7-30.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

**Note**

To permanently save your configuration changes, you must write them to the nonvolatile RAM (NVRAM) by entering the **copy running-config startup-config** command in privileged EXEC mode.

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For more information about managing configuration files, refer to the [Cisco IOS XE Configuration Fundamentals Configuration Guide](#), Release 2 and [Cisco IOS Configuration Fundamentals Command Reference](#) publications for your specific software.

Shutting Down and Restarting an Interface on a SPA

Shutting down an interface puts it into the administratively down mode and takes it offline, stopping all traffic that is passing through the interface. Shutting down an interface, though, does not change the interface configuration.

As a general rule, you do not need to shut down an interface if you are removing it and replacing it with the same exact model of SPA in an online insertion and removal (OIR) operation. However, we recommend shutting down an interface whenever you are performing one of the following tasks:

- When you do not need to use the interface in the network.
- Preparing for future testing or troubleshooting.
- Changing the interface configuration in a way that would affect the traffic flow, such as changing the encapsulation.
- Changing the interface cables.
- Removing a SPA that you do not expect to replace.
- Replacing an interface card with a different model of card.

Shutting down the interface in these situations prevents anomalies from occurring when you reinstall the new card or cables. It also reduces the number of error messages and system messages that might otherwise appear.

**Note**

If you plan to replace an existing ATM port adapter with an ATM SPA in the Cisco ASR 1000 Series Router and want to use the same configuration, save the slot's configuration before physically replacing the hardware. This is because all slot configuration is lost when you replace one card type with another card type, even if the two cards are functionally equivalent. You can then re-enter the previous configuration after you have inserted the ATM SPA.

To shut down an interface, perform the following procedure beginning in global configuration mode:

	Command or Action	Purpose
Step 1	Router(config)# interface atm slot/subslot/port	Enters interface configuration mode for the indicated port on the specified ATM SPA.
Step 2	Router(config-if)# shutdown	Shuts down the interface.
Step 3	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

**Tip**

When you shut down an interface, the **show interface** command indicates that the interface is administratively down until the SPA is physically removed from the chassis or until the SPA is re-enabled.

The following shows a typical example of shutting down an ATM SPA interface:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 0/2/2
Router(config-if)# shutdown
Router(config-if)# end
Router# show interface atm 0/2/2
```

ATM0/2/2 is administratively down, line protocol is down

```
Hardware is SPA-3XOC3-ATM, address is 000d.2959.d5ca (bia 000d.2959.d5ca)
Internet address is 10.10.10.16/24
MTU 4470 bytes, sub MTU 4470, BW 599040 Kbit, DLY 80 usec,
    reliability 255/255, txload 42/255, rxload 1/255
Encapsulation ATM, loopback not set
Encapsulation(s): AAL0
4095 maximum active VCs, 1 current VCCs
VC idle disconnect time: 300 seconds
0 carrier transitions
Last input 01:01:16, output 01:01:16, output hang never
Last clearing of "show interface" counters 01:10:21
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 702176000 bits/sec, 1415679 packets/sec
1000 packets input, 112000 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
2948203354 packets output, 182788653886 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```


Verifying the Interface Configuration

See the following sections to obtain configuration and operational information about the ATM SPA and its interfaces:

- [Verifying Per-Port Interface Status, page 7-27](#)
- [Monitoring Per-Port Interface Statistics, page 7-28](#)

For additional information on using these and other commands to obtain information about the configuration and operation of the ATM SPAs and interfaces, see [Chapter 8, “Troubleshooting the ATM SPAs”](#).

Verifying Per-Port Interface Status

Use the **show interfaces atm** command to display detailed status information about an interface port in an ATM SPA that is installed in a Cisco ASR 1000 Series Router. The following example provides sample output for interface port 1 (the second port) on the ATM SPA that is located in subslot 2, of the SIP that is installed in slot 0 of a Cisco ASR 1000 Series Router:



Note

The output of the **show interfaces atm** command can display configuration of AAL5 encapsulation, but only AAL0 is supported on the Cisco ASR 1000 Series Routers.

```
Router# show interfaces atm 0/2/2

ATM0/2/2 is up, line protocol is up
  Hardware is SPA-3XOC3-ATM-V2, address is 001a.3044.7522 (bia 001a.3044.7522)
  MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s): AAL5 AAL0
  4095 maximum active VCs, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  4 carrier transitions
  Last input never, output 00:04:11, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 540 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 540 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Monitoring Per-Port Interface Statistics

Use the **show controllers atm** command to display detailed status and statistical information on a per-port basis for an ATM SPA. The following example provides sample output for interface port 2 on the ATM SPA that is located in subslot 2 of the SIP that is installed in slot 0 of a Cisco ASR 1000 Series Router:

```
Router# show controllers atm 0/2/2

Interface ATM0/2/2 (SPA-3XOC3-ATM-V2[0/2]) is up
  Framing mode: SONET OC3 STS-3c
  SONET Subblock:
  SECTION
    LOF = 0          LOS   = 1          BIP(B1) = 0
  LINE
    AIS = 0          RDI   = 1          FEBE = 55          BIP(B2) = 0
  PATH
    AIS = 0          RDI   = 1          FEBE = 21          BIP(B3) = 0
    LOP = 1          NEWPTR = 0          PSE   = 0          NSE    = 0

Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

ATM framing errors:
  HCS (correctable):  0
  HCS (uncorrectable): 0

APS
not configured
COAPS = 0          PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = 13
PATH TRACE BUFFER : STABLE

BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

Clock source:  line
```

Configuration Examples

This section includes the following configuration examples for the ATM SPAs:

- [Basic Interface Configuration Example, page 7-29](#)
- [MTU Configuration Example, page 7-29](#)
- [PVC on a Point-to-Point Subinterface Configuration Example, page 7-29](#)
- [PVC Ranges on a Multipoint Subinterface for PPPoEoA Configuration Example, page 7-30](#)
- [PVC Ranges on a Multipoint Subinterface for PPPoEoA Configuration Example, page 7-30](#)
- [AToM VP Cell Mode Relay Configuration Example, page 7-30](#)
- [PPPoEoA VC Class and PVC Range Configuration Example, page 7-30](#)
- [SONET and SDH Framing Configuration Example, page 7-31](#)

Basic Interface Configuration Example

```
!  
interface ATM5/1/0  
  mtu 9216  
  no ip address  
  atm clock INTERNAL  
!  
interface ATM5/1/0.1 point-to-point  
  mtu 9216  
  ip address 10.1.1.1 255.255.0.0  
  pvc 52/100  
!  
interface ATM5/1/1  
  mtu 9216  
  no ip address  
  atm clock INTERNAL  
!  
interface ATM5/1/1.1 point-to-point  
  mtu 9216  
  ip address 10.2.1.1 255.255.0.0  
  pvc 53/100  
!  
!  
interface ATM5/1/2  
  no ip address  
  atm clock INTERNAL  
!  
interface ATM5/1/3  
  no ip address  
  atm clock INTERNAL  
!
```

MTU Configuration Example

```
!  
interface ATM5/0/0.9 point-to-point  
  mtu 4474  
  bandwidth 7000  
  ip address 192.168.100.13 255.255.255.0  
  ip mtu 4470
```

PVC on a Point-to-Point Subinterface Configuration Example

```
interface ATM5/0/0.9 point-to-point  
  mtu 4474  
  bandwidth 34000  
  ip vrf forwarding vrfexample  
  ip address 192.168.196.18 255.255.255.252  
  ip mtu 4470  
  pvc 11/105  
    ubr 38  
    oam-pvc manage  
    encapsulation aal5snap  
  !  
interface ATM5/0/0.11 point-to-point  
  mtu 4474  
  bandwidth 7000  
  ip address 192.168.252.141 255.255.255.252
```

```

ip mtu 4470
pvc 100/50
  cbr 7000
  encapsulation aal5snap
  service-policy input Leased_Line_Ingress
  max-reserved-bandwidth 100

```

PVC Ranges on a Multipoint Subinterface for PPPoEoA Configuration Example



Note

Multipoint subinterfaces, PVC ranges, and PPPoEoA support is introduced for the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.5.

```

interface atm0/0/0.65000 multipoint
  range pvc 1/32 1/4031
  protocol pppoe group bba_group1
  pvc-in-range 1/32
    class-vc pvcr_bba_vc_class
  !
  pvc-in-range 1/33
    class-vc pvcr_bba_vc_class
  !
  pvc-in-range 1/34
    class-vc pvcr_bba_vc_class
  !
  pvc-in-range 1/35
    class-vc pvcr_bba_vc_class
  !
  pvc-in-range 1/36
    class-vc pvcr_bba_vc_class
  !

```

AToM VP Cell Mode Relay Configuration Example

```

pseudowire-class vp-cell-relay
  encapsulation mpls
  exit
interface atm 1/2/0.1 multipoint
  atm pvp 1 l2transport
  xconnect 10.0.0.1 123 pw-class vp-cell-relay

```

PPPoEoA VC Class and PVC Range Configuration Example

```

bba-group pppoe bba_group1
  virtual-template 1
  !
  vpdn enable
  no vpdn logging
  !
  no virtual-template snmp
  !
bba-group pppoe bba_group1
  virtual-template 1
    sessions per-mac limit 4000
  !
vc-class atm pvcr_bba_vc_class

```

```

protocol pppoe group bba_group1
create on-demand
idle-timeout 30
vbr-nrt 1000 1000 1
!
interface atm0/0/0
atm clock internal
no shutdown
!
interface atm0/0/0.65000 multipoint
range pvc 1/32 1/4031
protocol pppoe group bba_group1
pvc-in-range 1/32
class-vc pvcr_bba_vc_class
!
pvc-in-range 1/33
class-vc pvcr_bba_vc_class
!
pvc-in-range 1/34
class-vc pvcr_bba_vc_class
!
pvc-in-range 1/35
class-vc pvcr_bba_vc_class
!
pvc-in-range 1/36
class-vc pvcr_bba_vc_class
!
interface virtual-template 1
no snmp trap link-status
keepalive 60
ppp ipcp address required
ip unnumbered loopback1
peer default ip address pool local_pool1
ppp mtu adaptive
ppp authentication pap
no logging event link-status

```

SONET and SDH Framing Configuration Example

```

!
interface ATM0/2/2
description Example of SONET framing-"atm framing sonet" is default and doesn't appear
ip address 10.16.2.2 255.255.255.0
logging event link-status
atm sonet report all
atm sonet threshold sd-ber 3
atm sonet threshold sf-ber 6
atm sonet overhead c2 0x00
!

```




CHAPTER 8

Troubleshooting the ATM SPAs

This chapter describes techniques that you can use to troubleshoot the operation of your ATM SPAs.

- [General Troubleshooting Information, page 8-1](#)
- [Performing Basic Interface Troubleshooting, page 8-3](#)
- [Displaying Additional ATM SPA Data, page 8-5](#)
- [Using the Cisco IOS Event Tracer to Troubleshoot Problems, page 8-9](#)
- [Preparing for Online Insertion and Removal of a SPA, page 8-9](#)

For more information about troubleshooting your hardware installation, refer to the *Cisco Aggregation Services Router 1000 Series SIP and SPA Hardware Installation Guide*.

General Troubleshooting Information

This section provides the following general information for troubleshooting ATM SPA cards and their SPA interface processor (SIP) carrier cards:

- [Interpreting Console Error and System Messages, page 8-1](#)
- [Using debug Commands, page 8-2](#)
- [Using show Commands, page 8-2](#)

Interpreting Console Error and System Messages

To view the explanations and recommended actions for Cisco ASR 1000 Series Routers error messages, including messages related to Cisco ASR1000-SIP10 and SPAs, refer to the *System Messages for Cisco IOS XE*.

System error messages are organized in the documentation according to the particular system facility that produces the messages. The SIP and SPA error messages use the following facility names:

- ASR1000_RP_ATM_SPA
- ASR1000_RP_SPA
- ASR1000_SIP
- ASR1000_SIP_SPA
- ATMSPA
- SPA

Using debug Commands

General debug Commands

Along with the other debug commands supported on the Cisco ASR 1000 Series Routers, you can obtain specific debug information for SPAs on the Cisco ASR 1000 Series Routers using the **debug hw-module subslot** privileged exec command.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead can affect system use.

The **debug hw-module subslot** command is intended for use by Cisco Systems technical support personnel. For more information about the debug hw-module subslot command and about other debug commands that can be used on a Cisco ASR 1000 Series Routers, refer to the *Cisco IOS Debug Command Reference* for your specific software.

ATM debug Commands

The following debug commands can be useful when troubleshooting specific ATM problems on an ATM interface or subinterface:

- **debug atm errors**—Displays errors that occur on an ATM interface, such as encapsulation and framing errors, as well as any errors that might occur during configuration of the ATM interfaces.
- **debug atm events**—Displays information about events that occur on the ATM interfaces, such as changes to the ATM SPA and ATM interface configuration, card and interface resets, and PVC creation.

**Note**

The output of **debug atm events** can be extremely verbose and can cause problems if large numbers of ATM VCs are configured. The command should only be used when a few VCs are configured.

- **debug atm oam**—Displays the contents of ATM operation and maintenance (OAM) cells as they arrive from the ATM network.

**Tip**

Use the **no debug all** command to turn off all debugging displays.

For more information about these commands, see the *Cisco IOS Debug Command Reference* for your specific software release.

Using show Commands

There are several **show** commands that you can use to monitor and troubleshoot the SIP and SPA cards on Cisco ASR 1000 Series Routers. For more information on these commands, see the [“Performing Basic Interface Troubleshooting”](#) section on page 8-3 and [“Verifying the Interface Configuration”](#) section on page 7-27 in Chapter 7, “Configuring the ATM SPAs”.

Performing Basic Interface Troubleshooting

You can perform most of the basic interface troubleshooting using the **show interface atm**, **show atm interface atm**, and **show ip interface** commands and examining several areas of the output to determine how the interface is operating.

The following example shows output from the **show atm interface atm** and **show ip interface** commands.

```
Router# show atm interface atm 0/2/2

Interface ATM0/2/2:
AAL enabled: AAL5 , Maximum VCs: 4095, Current VCCs: 1

Max. Datagram Size: 4528
PLIM Type: SONET - 155000Kbps, TX clocking: LINE
Cell-payload scrambling: ON
sts-stream scrambling: ON
5 input, 5 output, 0 IN fast, 0 OUT fast, 0 out drop
Avail bw = 149760
Config. is ACTIVE

Router# show ip interface atm 0/2/2.1

ATM0/2/2.1 is up, line protocol is up
Internet address is 2.4.0.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 4470 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is disabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Distributed switching is disabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
    Topology "base", operation state is UP
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
```

```

WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

```

To verify that your interface is operating properly, complete the steps in [Table 8-1](#):

Table 8-1 Basic Interface Troubleshooting Steps

	Action	Example
Step 1	From global configuration mode, enter the show interface atm , show atm interface atm , or show ip interface command.	<pre> Router# show interfaces atm 0/2/2 Router# show atm interface atm 0/2/2 Router# show ip interface 0/2/2 </pre>
Step 2	Verify that the interface is up.	<pre> Router# show interfaces atm 0/2/2 ATM0/2/2 is up, line protocol is up Router# show atm interface atm 0/2/2 Interface ATM0/2/2: AAL enabled: AAL5 , Maximum VCs: 1023, Current VCCs: 1 Router# show ip interface brief 0/2/2 ATM0/2/2 unassigned YES manual up up </pre>
Step 3	Test the ability of an interface to send and receive packets.	<pre> Router# ping </pre>

Using the Ping Command to Verify Network Connectivity

The **ping** command is a convenient way to test the ability of an interface to send and receive packets over the network. The **ping** command sends ICMP echo request packets to a specified destination address, which should send an equal number of ICMP echo reply packets in reply. By measuring the numbering of packets that are successfully returned, as well as how long each packet takes to be returned, you can quickly obtain a rough idea of the Layer 3 to Layer 3 connectivity between two interfaces.

The IP **ping** command has the following syntax:

ping

or

ping ip-address [repeat count] [data hex] [size datagram-size]

If you enter just **ping**, the command interactively prompts you for all other parameters. Otherwise, you must specify at least a specific IP address as the destination for the ping. You can also optionally specify the following parameters:

- **repeat count**—Number of ICMP echo request packets to send. The default is five packets.
- **data hex**—The data pattern, in hexadecimal, to be sent in the ICMP echo request packets.
- **size datagram-size**—Specifies the size, in bytes, of the ICMP echo request packets to be sent. The range is 40 to 18024 bytes, with a default of 100 bytes.

Displaying Additional ATM SPA Data

The following sections describe additional ATM SPA data that can be displayed:

- [Displaying ATM SPA Hardware Information, page 8-5](#)
- [Displaying Information About PVCs, page 8-5](#)
- [Using Loopback Commands, page 8-6](#)

Displaying ATM SPA Hardware Information

Use the following commands to display different types of hardware and system information:

- **show version**
Displays information about the router, its system hardware and software, and the number of each type of interface that is installed.
- **show hw-module subslot fpd**
Displays information about the hardware revision of the SPA, as well as the version of the field-programmable device (FPD) that is onboard the SPA. Cisco technical engineers might need this information to debug or troubleshoot problems with a SPA installation.
- **show idprom module**
Displays the serial number and board revisions for the ATM SPA.
- **show controllers atm**
Displays information about the controller hardware for an ATM interface, including framing and alarm configuration, as well as port, packet, and channel performance statistics. The syntax is **show controllers atm slot/subslot/port**.
- **show diag**
Displays information about the type of port adapters that are installed in the router. The syntax is **show diag slot**, where *slot* is the slot number that contains the port adapter.

Displaying Information About PVCs

Use the following commands to display information about PVCs, including mapping, traffic, and VLAN configuration information:

- **show atm vp**
Displays information about the virtual paths (VPs) that are configured on the router's ATM interfaces.
- **show atm vc**
If used without any options, displays information about all of the virtual channels that are currently configured on the ATM interfaces. To display detailed information about a specific virtual connection, specify its VC descriptor (VCD) along with the command. You can also display information about the VCs on a specific ATM interface and its subinterfaces, for example:

```
Router# show atm vc interface atm 0/2/2
```

- **show atm pvc**

Displays information about all PVCs that are currently configured on the router's ATM interfaces and subinterfaces. To display detailed information about a particular PVC, specify its VPI/VCI values. To display all PVCs on a particular ATM interface or subinterface, use the **show atm pvc interface atm** command. For example:

```
Router# show atm pvc 1/100
```

- **show atm ilmi-status**

Displays information about Layer 2 and Layer 3 mapping.

- **show atm map**

Displays the mapping between virtual circuits and Layer 3 IP addresses.

- **show atm traffic**

Displays general information about the traffic over the ATM interfaces. To display information about traffic shaping on the ATM interfaces in a particular slot, use the **show atm traffic shaping slot** command. You can also use the **show atm vc traffic** command to display traffic information for a particular VC.

Using Loopback Commands

The **loopback** commands place an interface in loopback mode, which enables you to use the **ping** command to send packets through the local interface and line, so as to test connectivity. These commands are especially useful when an interface is experiencing a high number of cyclic redundancy check (CRC) errors, so that you can pinpoint where the errors are occurring.

The following describes different loopback tests:

- [Using loopback diagnostic to Create a Local Loopback, page 8-6](#)
- [Using loopback line, page 8-8](#)

Using loopback diagnostic to Create a Local Loopback

To perform a local loopback test, in which the transmit data is looped back to the receive data at the physical (PHY) layer, use the **loopback diagnostic** command on an ATM interface. This loopback tests connectivity on the local ATM interface, verifying that the interface's framing circuitry and segmentation and reassembly (SAR) circuitry is operating correctly. This loopback, however, does not test the interface's optics circuitry and ports.



Tip

If an ATM interface is currently connected to another ATM interface and passing traffic, shut down the remote ATM interface before giving the **loopback diagnostic** command on the local ATM interface. Otherwise, the remote interface continues to send traffic to the local interface, and the remote network could also start reporting interface and network errors.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface atm slot/subslot/port	Enters interface configuration mode for the indicated port on the specified ATM SPA card.
Step 3	Router(config-if)# loopback diagnostic	Puts the ATM interface into the local loopback mode, so that data that is transmitted out the interface is internally routed back into the receive data line.
Step 4	Router(config-if)# atm clock internal	Specifies that the AMT interface should derive its clocking from its local oscillator, which is required, because the loopback command isolates the interface from the network and from the clocking signals that are derived from the network line.
Step 5	Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	Router# show interface atm slot/subslot/port	(Optional) Verifies that the interface has been configured for loopback mode. The output should show the words “loopback set” when the interface is operating in loopback mode.
Step 7	Router(config-if)# ping ip-address [repeat count] [data hex] [size datagram-size]	<p>Sends an ICMP echo request packet to the specified IP address.</p> <ul style="list-style-type: none"> • <i>ip-address</i>—Destination IP address for the ICMP echo request packet. Because the interface has been put into loopback mode, the exact IP address does not matter—any valid IP address can be specified. • repeat count—(Optional) Specifies the number of ICMP echo request packets to be sent. The default is 5. • <i>data hex</i>—(Optional) The data pattern, in hexadecimal, to be sent in the ICMP echo request packets. • size datagram-size—(Optional) Specifies the size, in bytes, of the ICMP echo request packets to be sent. The range is 40 to 18024 bytes, with a default of 100 bytes. <p>Note Because the interface is in loopback mode, the ping command will report that it failed. This is to be expected.</p>
Step 8	Router# show interface atm slot/subslot/port	<p>Displays interface statistics, including whether any CRC or other errors occurred during the ping test. For example:</p> <pre>Router# show interface atm 5/0/1 ... Received 0 broadcasts, 0 runs, 0 giants, 0 throttles 5 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort ... Router#</pre>
Step 9	Router(config)# interface atm slot/subslot/port	Enters interface configuration mode for the indicated port on the specified ATM SPA card.

	Command or Action	Purpose
Step 10	Router(config-if)# no loopback diagnostic	Removes the local loopback and return the ATM interface to normal operations.
	Note Also remember to restore the proper clocking on the local ATM interface and to reenble the remote ATM interface.	

Examples

The following sample output shows a local loopback being set with the **loopback diagnostic** command.

```
Router# configure terminal
Router(config)# interface atm 0/2/2
Router(config-if)# loopback diagnostic
Router(config-if)# atm clock internal
Router(config-if)# end
Router# show interface atm 0/2/2

ATM0/2/2 is up, line protocol is up
  Hardware is ATM SPA, address is 000a.f330.2a80 (bia 000a.f330.2a80)
  MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback set
  Encapsulation(s): AAL5
  4095 maximum active VCs, 21 current VCCs
  VC idle disconnect time: 300 seconds
  Signalling vc = 1, vpi = 0, vci = 5
    UNI Version = 4.0, Link Side = user
  6 carrier transitions
  Last input 01:47:05, output 00:00:01, output hang never
  Last clearing of "show interface" counters 01:03:35
  Input queue: 0/75/33439/80 (size/max/drops/flushes); Total output drops: 963306
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    9502306 packets input, 6654982829 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    27827569 packets output, 21072150159 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Using loopback line

If an ATM interface can perform a local loopback successfully, without reporting errors, you can next try a line loopback (**loopback line** command) to determine if packet errors are being generated by the ATM network between the local and remote router. In a line loopback, the interface on the remote router is configured with the loopback line command, so that it reflects every packet that it receives back to the originating router. The local router then generates traffic with the ping command to determine whether the line through the network is generating the packet errors.

Using the Cisco IOS Event Tracer to Troubleshoot Problems

**Note**

This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

For more information about using the Event Tracer feature, refer to the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a0080087164.html

Preparing for Online Insertion and Removal of a SPA

The Cisco ASR 1000 Series Aggregation Services Routers support online insertion and removal (OIR) of the SIP, in addition to each of the SPAs. Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This means that a SIP can remain installed in the router with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see Chapter 5, “Troubleshooting the SIP”.



PART 3

Ethernet Shared Port Adapters



CHAPTER 9

Overview of the Ethernet SPAs

This chapter provides an overview of the release history, and feature and Management Information Base (MIB) support for the Fast Ethernet and Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Aggregation Services Routers.

This chapter includes the following sections:

- [Release History, page 9-2](#)
- [Supported Features, page 9-2](#)
- [SPA Architecture, page 9-7](#)
- [Displaying the SPA Hardware Type, page 9-8](#)

Release History

Release	Modification
Cisco IOS XE Release 3.2	Added support for the 2-Port Gigabit Synchronous Ethernet SPA on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The maximum number of supported 802.1Q VLANs per Ethernet SPA was increased with the hw-module subslot ethernet vlan unlimited global configuration command.
Cisco IOS XE Release 2.1	<p>First release. Support for the following SPAs was introduced on the Cisco ASR1000-SIP10 on the Cisco ASR 1000 Series Routers:</p> <p>Fast Ethernet SPAs</p> <ul style="list-style-type: none"> • 4-Port FastEthernet SPA • 8-Port Fast Ethernet SPA <p>Gigabit Ethernet SPAs</p> <ul style="list-style-type: none"> • 10-Port Gigabit Ethernet SPA, Version 2 • 8-Port Gigabit Ethernet SPA, Version 2 • 5-Port Gigabit Ethernet SPA, Version 2 • 2-Port Gigabit Ethernet SPA, Version 2 • 1-Port 10-Gigabit Ethernet SPA, Version 2

Supported Features

The following is a list of some of the significant hardware and software features supported by Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Routers:

- Autonegotiation
- Auto-MDI/MDIX detection (Fast Ethernet and 2-Port Gigabit Ethernet SPAs only)
- Full-duplex operation
- 802.1Q VLAN termination
- Jumbo frames support (9216 bytes)
- Support for command-line interface (CLI)-controlled OIR
- 802.3x flow control
- The following maximum number of VLANs per SPA:
 - Up to 8100 VLANs per SPA—For all Ethernet SPAs supported on the Cisco ASR 1000 Series Routers in software releases prior to Cisco IOS XE Release 2.5.
 - Up to 4094 VLANs per port per SPA—For all Ethernet SPAs supported on the Cisco ASR 1000 Series Routers beginning in Cisco IOS XE Release 2.5 using the **hw-module subslot ethernet vlan unlimited** command.
- Up to 5000 MAC Accounting Entries per SPA (Source MAC Accounting on the ingress and Destination MAC Accounting on the egress)

- Per-port byte and packet counters for policy drops, oversubscription drops, CRC error drops, packet sizes, unicast, multicast, and broadcast packets
- Per-VLAN byte and packet counters for policy drops, oversubscription drops, unicast, multicast, and broadcast packets
- Per-port byte counters for good bytes and dropped bytes
- Multiprotocol Label Switching (MPLS)
- Quality of Service (QoS)
- Hot Standby Router Protocol (HSRP)

Following are the additional features supported by the 2-Port Gigabit Synchronous Ethernet SPA on the Cisco ASR 1000 Series Routers:

- L1 clock frequency distribution—In this mode, the 2-Port Gigabit Synchronous Ethernet SPA recovers the received clock, synchronizes it to a traceable source, and uses it to transmit data to the next node.
- A Building Integrated Time Source (BITS) interface for an external Synchronization Supply Unit (SSU) or a BITS device can be used as a clock source, or to clean up the accumulated wander on either a system or a recovered clock.
- The GPS timing interface is used for external GPS devices, and can be selected as either an input or an output reference. The GPS timing interface supports connectivity to the GPS clock.
- In order to maintain a communication channel in synchronous network connections, Ethernet relies on a channel called Ethernet Synchronization Messaging Channel (ESMC) based on the IEEE 802.3 Organization-Specific Slow Protocol. ESMC relays the SSM code that represents the quality level of the Ethernet Equipment Clock (EEC) in a physical layer.
- Supports IP Subscriber Awareness over Ethernet.

Restrictions

These restrictions apply to the 2-Port Gigabit Synchronous Ethernet SPA introduced in Cisco IOS XE Release 3.2:

- Synchronous SPA features are compatible with the 2-Port Gigabit Synchronous Ethernet SPA.
- The maximum theoretical bandwidth of the 2-Port Gigabit Synchronous Ethernet SPA is 2 Gbps full duplex. The actual performance is limited by the capability of either the host or the jacket card.
- In a failover scenario, the SPA does not perform any autoswitchover to a secondary clock source, even if the secondary reference is configured on the same SPA. If the primary clock goes down, the platform explicitly sets the secondary clock as source.

Synchronous Ethernet

Synchronous Ethernet (SyncE) is a procedure in which a physical layer interface is used to pass timing from node to node in the same way that timing is passed in SONET or SDH. SyncE, defined by ITU-T standards, such as G.8261, G.8262, G.8264, and G.781, leverages the PHY layer of Ethernet to transmit frequency to remote sites. SyncE over Ethernet provides a cost-effective alternative to the networks. For SyncE to work, each network element must, along with the synchronization path, support SyncE.

The 2-Port Gigabit Synchronous Ethernet SPA has a dedicated external interface known as the BITS interface to recover the clock from a SSU. The Cisco ASR 1000 Series Routers use this clock for SyncE. The BITS interface supports E1 (European SSUs) and T1 (American BITS) framing. [Table 9-1](#) lists the framing modes for the BITS interface on a 2-Port Gigabit Synchronous Ethernet SPA.

Table 9-1 Framing Modes for BITS Interface

BITS or SSU Interface Support Matrix	Framing Modes Supported	SSM or QL support	Tx Port	Rx Port
T1	T1 ESF	Yes	Yes	Yes
T1	T1 SF	No	Yes	Yes
E1	E1 CRC4	Yes	Yes	Yes
E1	E1 FAS	No	Yes	Yes
E1	E1 CAS	No	No	Yes
E1	E1 CAS CRC4	Yes	No	Yes
2048kHz	2048kHz	No	Yes	Yes

You can implement SyncE on the 2-Port Gigabit Synchronous Ethernet SPA, with four different configurations:

- **Clock Recovery from SyncE:** The system clock is recovered from the SyncE clocking source (Gigabit and Tenggigabit interfaces only). The router uses this clock as the Tx clock for other SyncE interfaces or ATM or CEoP interfaces.
- **Clock Recovery from External Interface:** The system clock is recovered from a BITS clocking source or a GPS interface.
- **Line to External:** The system clock received from an Ethernet is forwarded to an external Synchronization Supply Unit (SSU). During a synchronization chain, the received clock may have unacceptable wander and jitter. The router recovers the clock from the SyncE interface, converts it to the format required for the BITS interface, and sends it to an SSU through the BITS port. The SSU cleans the clock and sends it back to the BITS interface. This clock is used as the Tx clock for the SyncE ports.
- **System to External:** The system clock is used as the Tx clock for an external interface. By default, the system clock is not transmitted on an external interface.

Squelching

Squelching is a process in which, an alarm indication signal (AIS) is sent to the Tx interfaces whenever the clock source goes down. The squelching functionality is implemented in two scenarios:

- **Line to external:** If the line source goes down, an AIS is transmitted on the external interface to the SSU.
- **System to external:** If the router loses all the clock sources, an AIS is transmitted on the external interface to the SSU.

Squelching is performed only on an external device such as an SSU or a Primary Reference Clock (PRC).

SSM and ESMC

Network clocking uses these mechanisms to exchange the quality level of the clock between the network elements :

- Synchronization Status Message
- Ethernet Synchronization Messaging Channel

Synchronization Status Message

Network elements use Synchronization Status Messages (SSM) to inform the neighboring elements about the Quality Level (QL) of the clock. Non-Ethernet interfaces, such as optical interfaces and SONET/T1/E1 SPA framers, use SSM. The key benefits of the SSM are:

- Prevents timing loops.
- Provides quick recovery when a part of the network fails.
- Ensures that a node derives timing from the most reliable clock source.

Ethernet Synchronization Messaging Channel

In order to maintain a logical communication channel in synchronous network connections, Ethernet relies on a channel called Ethernet Synchronization Messaging Channel (ESMC) based on IEEE 802.3 Organization-Specific Slow Protocol standards. ESMC relays the SSM code that represents the quality level of the Ethernet Equipment Clock (EEC) in a physical layer.

The ESMC packets are received only for those ports configured as clock sources, and transmitted on all the SyncE interfaces in the system. These packets are then processed by the clock selection algorithm on RP, and are used to select the best clock. The Tx frame is generated based on the QL value of the selected clock source, and sent to all the enabled SyncE ports.

Clock Selection Algorithm

The clock selection algorithm selects the best available synchronization source from the nominated sources. The algorithm has a nonrevertive behavior among clock sources with the same QL value, and always selects the signal with the best QL value. For clock option 1, the default is revertive, and for clock option 2, the default is nonrevertive.

The clock selection process works in the QL-enabled and QL-disabled modes. When multiple selection processes are present in a network element, all processes work in the same mode.

QL-Enabled Mode

In QL-enabled mode, the following parameters contribute to the selection process:

- Quality level
- Signal fail via QL-FAILED
- Priority
- External commands.

**Note**

- If no external commands are active, the algorithm selects the reference (for clock selection) with the highest quality level that does not experience a signal fail condition. If multiple inputs have the same highest quality level, the input with the highest priority is selected. For multiple inputs having the

same highest priority and quality level, the existing reference is maintained (if it belongs to this group), otherwise an arbitrary reference from this group is selected.

QL-Disabled Mode

In QL-Disabled mode, the following parameters contribute to the selection process:

- Signal failure
- Priority
- IP Subscriber Awareness over Ethernet
- External commands



Note

- If no external commands are active, the algorithm selects the reference (for clock selection) with the highest priority that does not experience a signal fail condition. For multiple inputs having the same highest priority, the existing reference is maintained (if it belongs to this group). Otherwise an arbitrary reference from this group is selected.

Supported MIBs

The following MIBs are supported by the Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Routers:

- ENTITY-MIB (RFC 4133)
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-ALARM-MIB
- ENTITY-SENSOR-MIB (RFC 3433)
- CISCO-ENTITY-SENSOR-MIB
- IF-MIB
- ETHERLIKE-MIB (RFC 3635)
- Remote Monitoring (RMON)-MIB (RFC 1757)
- CISCO-CLASS-BASED-QOS-MIB
- MPLS-related MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<https://tools.cisco.com/RPF/register/register.do>

Supported Ethernet SPAs

This section lists and describes the Ethernet SPAs supported by the Cisco ASR 1000 Series Routers and the SIP line cards supporting these Ethernet SPAs.

2-Port Gigabit Synchronous Ethernet SPA

The 2-Port Gigabit Synchronous Ethernet SPA provides time and frequency distribution across Ethernet networks. Synchronization is not traditionally present in the all-packet networks. Synchronization is cost-effective, and especially important to service providers that migrated late to packet networks, and use an external time-division multiplexing (TDM) circuit to provide timing to remote networks. These remote networks constantly require synchronization for crucial voice services.

SPA-2X1GE-SYNCE also has the ability to interface with either an external SSU or BITS interface or a GPS timing interface. The 2-Port Gigabit Synchronous Ethernet SPA comprises these clock interfaces:

- BITS In
- BITS Out
- GPS In
- GPS Out

The 2-Port Gigabit Synchronous Ethernet SPA (SPA-2X1GE-SYNCE) is compatible with the 2-Port GigE SPA-v2, and provides additional services, such as clock frequency and time-of-day synchronization, using the following technologies:

- Synchronous Ethernet (SyncE)
- ESMC

SyncE defined by ITU-T standards, such as G.8261, G.8262, G.8264, and G.781, and leverages the PHY layer of Ethernet to transmit frequency to remote sites. SyncE provides a cost-effective alternative to the SONET networks. For SyncE to work, each network element must along with the synchronization path, support SyncE.

SPA Architecture

This section provides an overview of the architecture of the Gigabit Ethernet SPAs and describes the path of a packet in the ingress and egress directions. Some of these areas of the architecture are referenced in the SPA software and can be helpful to understand when troubleshooting or interpreting some of the SPA CLI and **show** command output.

Every incoming and outgoing packet on the Gigabit Ethernet SPAs goes through the physical (PHY) SFP optics, the Media Access Controller (MAC), and a Layer 2 Filtering/Accounting ASIC.

Path of a Packet in the Ingress Direction

The following steps describe the path of an ingress packet through the Gigabit Ethernet SPAs:

1. For one-Gigabit Ethernet SPAs, the SFP optics receive incoming frames on a per-port basis from one of the optical fiber interface connectors.

2. For ten-Gigabit Ethernet SPAs, the XFP PHY device processes the frame and sends it over a serial interface to the MAC device.
3. The MAC device receives the frame, strips the CRCs, and sends the packet via the SPI 4.2 bus to the ASIC.
4. The ASIC takes the packet from the MAC devices and classifies the Ethernet information. CAM lookups based on Ethertype, port, VLAN, and source and destination address information determine whether the packet is dropped or forwarded to the SPA interface.

Path of a Packet in the Egress Direction

The following steps describe the path of an egress packet from the SIP through the Gigabit Ethernet SPAs:

1. The packet is sent to the ASIC using the SPI 4.2 bus. The packets are received with Layer 2 and Layer 3 headers in addition to the packet data.
2. The ASIC uses port number, destination MAC address, destination address type, and VLAN ID to perform parallel CAM lookups. If the packet is forwarded, it is forwarded via the SPI 4.2 bus to the MAC device.
3. For Gigabit Ethernet SPAs, the MAC device forwards the packets to the PHY laser-optic interface, which transmits the packet.

Displaying the SPA Hardware Type

To verify the SPA hardware type that is installed in your Cisco ASR 1000 Series Routers, you can use the **show platform** command.

Table 9-2 shows the hardware description that appears in the **show interfaces** command output for each Gigabit Ethernet SPA that is supported on the Cisco ASR 1000 Series Routers.

Table 9-2 SPA Hardware Descriptions in show Commands

SPA	Description in show interfaces Command
4-Port Fast Ethernet SPA	Hardware is SPA-4X1FE-TX-V2
8-Port Fast Ethernet SPA	Hardware is SPA-8X1FE-TX-V2
10-Port Gigabit Ethernet SPA	Hardware is SPA-10X1GE-V2
8-Port Gigabit Ethernet SPA	Hardware is SPA-8X1GE-v2
5-Port Gigabit Ethernet SPA	Hardware is SPA-5X1GE-V2
2-Port Gigabit Ethernet SPA	Hardware is SPA-2X1GE-V2
1-Port 10-Gigabit Ethernet SPA	Hardware is SPA-1X10GE-L-V2

Example of the show interfaces Command

The following example shows output from the **show interfaces tengigabitethernet** command on a Cisco ASR 1000 Series Routers with a 1-Port 10-Gigabit Ethernet SPA installed in slot 7:

```
Router# show interfaces tengigabitethernet7/0/0
TenGigabitEthernet0/0/0 is up, line protocol is up (connected)
```

```

Hardware is SPA-1X10GE-L-V2, address is 0000.0c00.0102 (bia 000f.342f.c340)
Internet address is 15.1.1.2/24
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full-duplex, 10Gb/s
input flow-control is on, output flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:10, output hang never
Last clearing of "show interface" counters 20:24:30
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
237450882 packets input, 15340005588 bytes, 0 no buffer
Received 25 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
1676 packets output, 198290 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out

```

The following example shows a sample output of the **show interfaces gigabitethernet** command on a Cisco ASR 1000 Series Router with a 2-Port Gigabit Synchronous Ethernet SPA installed in slot 2:

```

Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
Hardware is GigEther SPA, address is 000a.f330.2e40 (bia 000a.f330.2e40)
Internet address is 2.2.2.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 1000Mb/s, link type is force-up, media type is SX
output flow-control is on, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:19:34, output 03:19:29, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1703 packets input, 638959 bytes, 0 no buffer
Received 23 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1670 multicast, 0 pause input
1715 packets output, 656528 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out

```




CHAPTER 10

Configuring the Ethernet SPAs

This chapter provides information about configuring the Fast Ethernet and Gigabit Ethernet SPAs and on the Cisco ASR 1000 Series Router. It includes the following sections:

- [Configuration Tasks, page 10-1](#)
- [Verifying the Interface Configuration, page 10-15](#)
- [Using show Commands to Check SFP Module and XFP Module Status, page 10-16](#)
- [Configuring the Network Clock for the 2-Port Gigabit Synchronous Ethernet SPA on a Cisco ASR 1000 Series Router, page 10-19](#)

For more information about the commands used in this chapter, refer to the related Cisco IOS software command reference and master index publications and the publication that corresponds to your Cisco IOS XE software release. For more information about accessing these publications, see the [“Related Documentation” section on page xxvi](#).

For information about managing your system images and configuration files, refer to the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*, the *Cisco IOS Configuration Fundamentals Configuration Guide*, and the *Cisco IOS Configuration Fundamentals Command Reference* publications that correspond to your Cisco IOS software release.

Configuration Tasks

This section describes how to configure the Gigabit Ethernet and Fast Ethernet SPAs and includes information about verifying the configuration.

This section includes the following topics:

- [Required Configuration Tasks, page 10-2](#)
- [Specifying the Interface Address on a SPA, page 10-4](#)
- [Modifying the MAC Address on an Interface, page 10-4](#)
- [Gathering MAC Address Accounting Statistics, page 10-5](#)
- [Configuring the Hot Standby Router Protocol, page 10-5](#)
- [Modifying the Interface MTU Size, page 10-6](#)
- [QoS Classification, page 10-7](#)
- [Configuring the Encapsulation Type, page 10-10](#)
- [Configuring the Autonegotiation on an Interface, page 10-10](#)

- [Configuring a Subinterface on a VLAN, page 10-12](#)
- [VLAN Classification, page 10-13](#)
- [Saving the Configuration, page 10-15](#)
- [Shutting Down and Restarting an Interface on a SPA, page 10-15](#)

Required Configuration Tasks

This section lists the required configuration steps to configure the Gigabit Ethernet SPAs. Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command. These commands are indicated by “(As Required)” in the Purpose column.

To configure the Fast Ethernet or Gigabit Ethernet SPAs, complete the following steps:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface gigabitethernet <i>slot/subslot/port</i> [<i>.subinterface-number</i>] or Router(config)# interface tengigabitethernet <i>slot/subslot/port</i> [<i>.subinterface-number</i>] or Router(config)# interface fastethernet <i>slot/subslot/port</i> [<i>.subinterface-number</i>]	Specifies the Gigabit Ethernet, Ten Gigabit Ethernet, or Fast Ethernet interface to configure, where: <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 10-4. • <i>.subinterface-number</i>—(Optional) Specifies a secondary interface (subinterface) number.
Step 3	Router(config-if)# ip address [<i>ip-address mask</i> { secondary } dhcp { client-id <i>interface-name</i> } { hostname <i>host-name</i> }]	Sets a primary or secondary IP address for an interface that is using IPv4, where: <ul style="list-style-type: none"> • <i>ip-address</i>—Specifies the IP address for the interface. • <i>mask</i>—Specifies the mask for the associated IP subnet. • secondary—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. • dhcp—Specifies that IP addresses will be assigned dynamically using DHCP. • client-id <i>interface-name</i>—Specifies the client identifier. The <i>interface-name</i> sets the client identifier to the hexadecimal MAC address of the named interface. • hostname <i>host-name</i>—Specifies the hostname for the DHCP purposes. The <i>host-name</i> is the name of the host to be placed in the DHCP option 12 field.

	Command	Purpose
Step 4	Router(config-if)# ip accounting mac-address {input output}	<p>(Optional) Enables MAC address accounting. MAC address accounting provides accounting information for IP traffic based on the source and destination MAC addresses of the LAN interfaces, where:</p> <ul style="list-style-type: none"> • input—Specifies MAC address accounting for traffic entering the interface. • output—Specifies MAC address accounting for traffic leaving the interface.
Step 5	Router(config-if)# mtu bytes	<p>(As Required) Specifies the maximum packet size for an interface, where:</p> <ul style="list-style-type: none"> • <i>bytes</i>—Specifies the maximum number of bytes for a packet. <p>The default is 1500 bytes; the range is 1500 to 9216.</p>
Step 6	Router(config-if)# standby [group-number] ip [ip-address [secondary]]	<p>(Required for HSRP Configuration Only) Creates (or enables) the HSRP group using its number and virtual IP address, where:</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—Specifies the group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface if configuring HSRP) <i>ip-address</i>—Specifies the virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) secondary—Specifies the IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router. <p>This command enables HSRP but does not configure it further. For additional information on configuring HSRP, refer to the HSRP section of the <i>Cisco IP Configuration Guide</i> publication that corresponds to your Cisco IOS software release.</p>
Step 7	Router(config-if)# no shutdown	Enables the interface.

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Aggregation Services Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 0:

```
Router(config)# interface GigabitEthernet 0/0/0
interface GigabitEthernet0/0/0
no ip address
shutdown
negotiation auto
no cdp enable
```

Modifying the MAC Address on an Interface

The Gigabit Ethernet SPAs use a default MAC address for each port that is derived from the base address that is stored in the electrically erasable programmable read-only memory (EEPROM) on the backplane of the Cisco ASR 1000 Series Routers.

To modify the default MAC address of an interface to some user-defined address, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# mac-address <i>ieee-address</i>	Modifies the default MAC address of an interface to some user-defined address, where: <ul style="list-style-type: none">• <i>ieee-address</i>—Specifies the 48-bit Institute of Electrical and Electronics Engineers (IEEE) MAC address written as a dotted triple of four-digit hexadecimal numbers (<i>xxxx.yyyy.zzzz</i>).

To return to the default MAC address on the interface, use the **no** form of the command.

Verifying a MAC Address

To verify the MAC address of an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the “address is” field.

The following example shows that the MAC address is 000a.f330.2e40 for interface 1 on the SPA installed in subslot 0 of the SIP installed in slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is up, line protocol is up
  Hardware is SPA-1X10GE-L-V2, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```



```

    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive not supported
    Full-duplex, 1000Mb/s, link type is force-up, media type is SX
    output flow-control is on, input flow-control is on
    (Additional output removed for readability)

```

Gathering MAC Address Accounting Statistics

The **ip accounting mac-address [input | output]** command can be entered to enable MAC Address Accounting on an interface. After enabling MAC Address Accounting, MAC address statistics can be displayed by entering the **show interfaces mac-accounting** command.

Configuring the Hot Standby Router Protocol

The Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. HSRP is used in a group of routers for selecting an active router and a standby router. (An *active router* is the router of choice for routing packets; a *standby router* is a router that takes over the routing duties when an active router fails, or when preset conditions are met).

HSRP is enabled on an interface by entering the **standby [group-number] ip [ip-address [secondary]]** command. The **standby** command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, refer to the HSRP section of the *Cisco IP Configuration Guide* publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 2/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

```

Router(config)# interface GigabitEthernet 2/1/0
Router(config-if)# standby 2 ip 120.12.1.200
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt

```

Verifying HSRP

To verify the HSRP information, use the **show standby** command in EXEC mode:

```

Router# show standby
Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1

```

Modifying the Interface MTU Size

The Cisco IOS software supports three different types of configurable maximum transmission unit (MTU) options at different levels of the protocol stack:

- **Interface MTU**—Checked by the SPA on traffic coming in from the network. Different interface types support different interface MTU sizes and defaults. The interface MTU defines the maximum packet size allowable (in bytes) for an interface before drops occur. If the frame is smaller than the interface MTU size, but is not smaller than the minimum frame size for the interface type (such as 64 bytes for Ethernet), then the frame continues to process.
- **IP MTU**—Can be configured on an interface or subinterface. If an IP packet exceeds the IP MTU size, then the packet is fragmented.
- **Tag or Multiprotocol Label Switching (MPLS) MTU**—Can be configured on an interface or subinterface and allows up to six different labels, or tag headers, to be attached to a packet. The maximum number of labels is dependent on your Cisco IOS software release.

Different encapsulation methods and the number of MPLS MTU labels add additional overhead to a packet. For example, Subnetwork Access Protocol (SNAP) encapsulation adds an 8-byte header, dot1q encapsulation adds a 2-byte header, and each MPLS label adds a 4-byte header (n labels \times 4 bytes).

For Gigabit Ethernet SPAs on the Cisco ASR 1000 Series Aggregation Services Routers, the default MTU size is 1500 bytes. The maximum configurable MTU is 9216 bytes. The SPA automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.

Interface MTU Configuration Guidelines

When configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco ASR 1000 Series Router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following additional overhead:
 - Layer 2 header—14 bytes
 - Dot1q header—4 bytes
 - CRC—4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU.
- If you are using MPLS labels, then you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Interface MTU Configuration Task

To modify the MTU size on an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# mtu <i>bytes</i>	Configures the maximum packet size for an interface, where: <ul style="list-style-type: none"><i>bytes</i>—Specifies the maximum number of bytes for a packet. The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.

To return to the default MTU size, use the **no** form of the command.

Verifying the MTU Size

To verify the MTU size for an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the “MTU” field.

The following example shows an MTU size of 1500 bytes for interface port 1 (the second port) on the Gigabit Ethernet SPA installed in the top subslot (0) of the SIP that is located in slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is up, line protocol is up
  Hardware is SPA-1X10GE-L-V2, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
```

QoS Classification

The physical level interface module (PLIM) is the hardware component in the data path between the media interface and the forwarding engine.

Use the following commands in interface configuration mode to configure QoS:

Command	Purpose
Router(config-if)# plim qos input map ip { precedence-based precedence <i>precedence-value</i> queue low-latency }	<p>Classifies incoming IP traffic according to the value of the IP precedence bits and places the traffic into the appropriate queue.</p> <ul style="list-style-type: none"> <i>precedence-value</i>—Specifies the value of the IP precedence bits (0 to 7). You can specify a range of values separated by a dash or a list of values. By default, the Gigabit Ethernet SPA classifies IP precedence range 6-7 as high priority. low-latency—Specifies the high priority queue. Enter 0 for low priority. <p>Use the no form of the command to remove the configured values.</p>
Router(config-if)# plim qos input map ipv6 all queue low-latency 0	<p>Classifies all IPv6 packets as high or low priority.</p> <ul style="list-style-type: none"> low-latency—Specifies high priority traffic. Enter 0 for low priority. <p>The no form of this command disables all IPv6 classification. By default, without using this command, the command is disabled.</p>
Router(config-if)# plim qos input map ipv6 tc [<i>tc-value</i> <i>tc-range</i>] queue low-latency 0	<p>Classifies ingress IPv6 traffic based on the value of the traffic-class bits and places the traffic into the appropriate queue.</p> <ul style="list-style-type: none"> <i>tc-value</i> <i>tc-range</i>—Specifies the value of the traffic class bits. You can specify a range of values separated by a dash or a list of values. low-latency—Specifies the high priority queue. Enter 0 for the low priority queue. <p>The no form of this command sets the classification according to default DSCP EF.</p> <p>By default, IPv6 traffic with a traffic-class value equal to ef uses the high-priority queue and all other traffic uses the low-priority queue. Only the most significant six bits of the traffic-class octet is used for the classification.</p>
Router(config-if)# plim qos input map mpls all queue low-latency 0	<p>Classifies all MPLS packets as high or low priority.</p> <ul style="list-style-type: none"> low-latency—Specifies high priority packets. Enter 0 for low priority packets. <p>The no form of this command disables MPLS classification. By default, without using this command, the command is disabled.</p>

Command	Purpose
Router(config-if)# plim qos input map mpls exp <i>exp-value exp-range</i> queue low-latency 0	<p>Classifies incoming MPLS traffic according to the value of the exp bits and places the traffic into the appropriate queue.</p> <ul style="list-style-type: none"> <i>exp-value exp-range</i>—Specifies which MPLS exp value or range to use. low-latency—Specifies high priority MPLS traffic. Enter 0 for low priority. <p>By default, without using this command, the Gigabit Ethernet SPA classifies MPLS EXP range 6-7 as high priority.</p> <p>The no form of this command sets the classification according to default exp range 6-7.</p>
Router(config-if)# plim qos input queue low-latency 0 pause [enable threshold percent]	<p>Enables Ethernet pause frame generation due to flow control status.</p> <ul style="list-style-type: none"> low latency—Specifies high priority queue. Enter 0 for a low priority queue. pause—Sets up the queue threshold to send a pause frame, which is a percentage of queue limit for packet drop. The default threshold is 90 percent. <p>By default, without using the command, pause frame generation is enabled for low latency queue.</p> <p>The no form of this command disables pause generation for a queue.</p>
Router(config-if)# plim qos input [bandwidth value_in_Kbps [low-latency]] [weight weight]	<p>Specifies the whole port, regardless of priority, or specifies priority only (low-latency) to receive minimum bandwidth guarantee, what minimum bandwidth is demanded, and what weight value is assigned for the excess scheduling.</p> <p>The default mode (without using this command) is that minimum scheduling is <i>off</i> and only excess scheduling is in service, which uses default weight proportional to the interface bandwidth.</p> <p>The no form of this command sets the interface to the default minimum bandwidth and weight.</p>

Port-Level or Physical-Level QoS Classification

Use the following commands for port or physical level classification:

Command	Purpose
Router(config-if)# plim qos input map ip all queue low-latency 0	<p>Allows user to specify all IPv4 packets as high or low priority.</p> <ul style="list-style-type: none"> low latency—Specifies high priority packets. Enter 0 for a low priority packets <p>The no form of this command disables all IPv4 classification. By default, without using this command, the command is disabled.</p>
Router(config-if)# plim qos input map ip dscp-based	<p>Enables IP DSCP-based classification.</p> <p>By default, without using this command, the Gigabit Ethernet SPA enables IP precedence-based classification for the Cisco ASR 1000 Series Routers.</p> <p>]The no form of this command totally disables the IP DSCP-based classification.</p>
Router(config-if)# plim qos input map ip dscp dscp-value <i>dscp-range</i> queue low-latency 0	<p>Allows the user to specify an IP DSCP value or range.</p> <ul style="list-style-type: none"> low-latency—Specifies high priority IP DSCP value. Enter 0 for low priority. <p>By default, without this command, the Gigabit Ethernet SPA classifies DSCP cs6-cs7 as high priority.</p> <p>The no form of this command removes the IP DSCP value or range.</p>

Configuring the Encapsulation Type

By default, the interfaces on the Gigabit Ethernet SPAs support Advanced Research Projects Agency (ARPA) encapsulation. They do not support configuration of service access point or SNAP encapsulation for transmission of frames; however, the interfaces will properly receive frames that use service access point and SNAP encapsulation.

The only other encapsulation supported by the SPA interfaces is IEEE 802.1Q encapsulation for virtual LANs (VLANs).

Configuring the Autonegotiation on an Interface

Fast Ethernet and Gigabit Ethernet interfaces use a connection-setup algorithm called *autonegotiation*. Autonegotiation allows the local and remote devices to configure compatible settings for communication over the link. Using autonegotiation, each device advertises its transmission capabilities and then agrees upon the settings to be used for the link.

For the Gigabit Ethernet interfaces on the Cisco ASR 1000 Series Aggregation Services Routers, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

The following guidelines should be followed regarding autonegotiation:

- If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled while the other end of the link does not, the link will not come up properly on both ends.
- Autonegotiation is not supported on the 10-Port Gigabit Ethernet SPA on the Cisco ASR1000-SIP10.
- Flow control is enabled by default.
- Flow control will be on if autonegotiation is disabled on both ends of the link.

Disabling Autonegotiation

Autonegotiation is automatically enabled and can be disabled on the Fast Ethernet and Gigabit Ethernet interfaces on the Cisco ASR1000-SIP10. During autonegotiation, advertisement for flow control, speed, and duplex occurs, depending on the media (fiber or copper) in use. If the interface is connected to a link that has autonegotiation disabled, autonegotiation should either be re-enabled on the other end of the link or disabled on the Fast Ethernet or Gigabit Ethernet SPA, if possible. Both ends of the link will not come up properly if only one end of the link has disabled autonegotiation.

Speed and duplex configurations can be advertised using autonegotiation. However, the only values that are negotiated are:

- For Fast Ethernet SPAs—100 Mbps for speed and full-duplex mode.
- For Gigabit Ethernet SPAs using RJ-45 copper interfaces—1000 Mbps for speed and full-duplex mode. Link speed is not negotiated when using fiber interfaces.

From a user's perspective, these settings are not really negotiated, but rather are enabled using autonegotiation. The SFPs for Gigabit Ethernet SPAs support 1000Base-X, and the IEEE 1000Base-X standard for fiber does not support negotiation of link speed.

To disable autonegotiation, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# no negotiation auto	Disables autonegotiation on Fast Ethernet or Gigabit Ethernet SPA interfaces on the Cisco ASR1000-SIP10. No advertisement of flow control occurs.

Configuring Speed and Duplex

When autonegotiation is turned off on Fast Ethernet or the RJ-45 interface in the 2-Port Gigabit Ethernet SPA, you can manually specify the speed and duplex configuration.



Note

When using the SFP-GE-T, you must configure both the speed and duplex modes.

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in interface configuration mode. To return to the default setting, use the **no** form of this command:

Command	Purpose
Router(config-if)# speed {10 100 1000}	Configures the interface to transmit at 10 Mbps, 100 Mbps, or 1000 Mbps. (The 1000 keyword is only valid for Gigabit Ethernet.)

To configure duplex operation on an interface, use the **duplex** command in interface configuration mode. Use the **no** form of this command to return to the default value.

Command	Purpose
Router(config-if)# duplex {full half}	Specifies full- or half-duplex operation.

Configuring the Media Type

The 2-Port Gigabit Ethernet SPA supports RJ-45 and fiber ports. Use the **media-type** configuration command to select either the RJ-45 or fiber media for a given port.

Command	Purpose
Router(config-if)# media-type {10baset 100baset rj45 gbic}	Specifies the physical connection on an interface.

Enabling Autonegotiation

To re-enable autonegotiation on a Fast Ethernet or Gigabit Ethernet interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# negotiation auto	Enables autonegotiation on a Fast Ethernet SPA interface on a Cisco ASR1000-SIP10 or a Gigabit Ethernet SPA interface on the Cisco ASR1000-SIP10. Advertisement of flow control occurs.

Configuring a Subinterface on a VLAN



Note

You can configure no more than 8100 802.1Q VLAN subinterfaces per Ethernet SPA in software releases prior to Cisco IOS XE Release 2.5. Beginning in Cisco IOS XE Release 2.5, you can use the **hw-module subslot ethernet vlan unlimited** command to increase the system default and enable support for configuration of up to 4094 dot1q VLANs per port per SPA. The default is 8100 VLANs.

You can configure subinterfaces on the Fast Ethernet SPA interfaces and Gigabit Ethernet SPA interfaces on a VLAN using IEEE 802.1Q encapsulation. Cisco Discovery Protocol (CDP) is disabled by default on the 2-Port Gigabit Ethernet SPA interfaces and subinterfaces on the Cisco ASR1000-SIP10.

To configure a SPA subinterface on a VLAN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# hw-module subslot <i>slot/subslot ethernet vlan unlimited</i>	(Optional) Enables configuration of up to 4094 dot1q VLANs per port per Ethernet SPA, where: <ul style="list-style-type: none"> <i>slot</i>—Specifies the chassis slot number where the SIP is installed. <i>subslot</i>—Specifies the slot of the SIP where the SPA is installed.
Step 2	Router(config)# interface gigabitethernet <i>slot/subslot/port.subinterface-number</i> or Router(config)# interface tengigabitethernet <i>slot/subslot/port.subinterface-number</i>	Specifies the Gigabit Ethernet interface to configure, where: <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 10-4. <i>.subinterface-number</i>—Specifies a secondary interface (subinterface) number.
Step 3	Router(config-subif)# encapsulation dot1q <i>vlan-id</i>	Defines the encapsulation format as IEEE 802.1Q (“dot1q”), where <i>vlan-id</i> is the number of the VLAN (1–4094).
Step 4	Router(config-if)# ip address <i>ip-address</i> <i>mask</i> [secondary]	Sets a primary or secondary IP address for an interface, where: <ul style="list-style-type: none"> <i>ip-address</i>—Specifies the IP address for the interface. <i>mask</i>—Specifies the mask for the associated IP subnet. secondary—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

VLAN Classification



Note

When the **hw-module subslot ethernet vlan unlimited** command is configured, the default classification of CoS bits 6-7 as high priority is still supported. However, other user-defined CoS values for high and low priority classification using the **plim qos input map cos queue** command are not supported.

To specify VLAN classification, use the following commands in subinterface configuration mode:

Command	Purpose
Router(config-subif)# plim qos input map cos enable	<p>Enables packet classification based on 802.1q VLAN COS bits.</p> <p>By default, this command is enabled on the Gigabit Ethernet SPA.</p> <p>The no form of this command totally disables the COS classification.</p> <p>The command is used in the dot1q subinterface configuration mode which can be either under the main physical interface or the Gigabit EtherChannel (GEC) link bundle.</p>
Router(config-subif)# plim qos input map cos cos-value cos-range queue low-latency 0	<p>Allows the user to specify which COS value or range for high priority (low-latency) or low priority (0).</p> <p>By default, without this command, COS value 6-7 is classified as high priority. Only the default behavior is supported when the hw-module subslot ethernet vlan unlimited command is configured.</p> <p>The no form of this command sets the classification according to the default value (COS priority value 6-7).</p> <p>This command is in the VLAN subinterface configuration mode under either the main physical interface or the GEC link bundle.</p>

Verifying Subinterface Configuration on a VLAN

To verify the configuration of a subinterface and its status on the VLAN, use the **show vlans** privileged EXEC command.

The following example shows the status of subinterface number 1 on port 0 on the SPA in VLAN number 200:

```
Router# show vlans
VLAN ID:200 (IEEE 802.1Q Encapsulation)

Protocols Configured:      Received:      Transmitted:
        IP                0                2

VLAN trunk interfaces for VLAN ID 200:

GigabitEthernet4/1/0.1 (200)

        IP:12.200.21.21

        Total 0 packets, 0 bytes input
        Total 2 packets, 120 bytes output
```

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For information about managing your system image and configuration files, refer to the [Cisco IOS Configuration Fundamentals Configuration Guide](#) and [Cisco IOS Configuration Fundamentals Command Reference](#) publications that correspond to your Cisco IOS software release.

Shutting Down and Restarting an Interface on a SPA

You can shut down and restart any of the interface ports on a SPA independently of each other. Shutting down an interface stops traffic and enters the interface into an “administratively down” state.

There are no restrictions for online insertion and removal (OIR) on Gigabit Ethernet SPAs. Gigabit Ethernet SPAs can be removed from a SIP at any time. SIPs populated with any type of SPAs can be removed from the router at any time.

If you are preparing for an OIR of a SPA, it is not necessary to independently shut down each of the interfaces prior to deactivation of the SPA. The **hw-module subslot stop** command automatically stops traffic on the interfaces and deactivates them along with the SPA in preparation for OIR.

In similar fashion, you do not need to independently restart any interfaces on a SPA after OIR of a SPA or SIP.

To shut down an interface on a SPA, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# shutdown	Disables an interface.

To restart an interface on a SPA, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# no shutdown	Restarts a disabled interface.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Router configuration settings, you can use the **show interfaces gigabitethernet** command to get detailed information on a per-port basis for your Gigabit Ethernet SPAs.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the Gigabit Ethernet SPAs, use the **show interfaces gigabitethernet** command.

The following example provides sample output for interface port 1 on the SPA located in the top subslot (0) of the SIP that is installed in slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is up, line protocol is up
  Hardware is SPA-1X10GE-L-V2, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 1000Mb/s, link type is force-up, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:18:49, output 03:18:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1703 packets input, 638959 bytes, 0 no buffer
    Received 23 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 1670 multicast, 0 pause input
    1715 packets output, 656528 bytes, 0 underruns
    0 output errors, 0 collisions, 4 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

Using show Commands to Check SFP Module and XFP Module Status

You can use various **show** commands to view information specific to SFP, XFP, CWDM, and DWDM optical transceiver modules.

To check or verify the status of an SFP Module or XFP Module, use the following **show** commands:

- **show hw-module *slot/subslot* transceiver *port idprom* detail**
- **show hw-module *slot/subslot* transceiver *port idprom* brief**
- **show hw-module *slot/subslot* transceiver *port idprom* dump**
- **show hw-module *slot/subslot* transceiver *port idprom* status**

Following are sample output of several **show** commands for SFP Modules and XFP Modules.

The following **show hw-module subslot** command sample output is for SFP-GE-S:

```
Router# show hw-module subslot 2/0 transceiver 0 idprom
```

```
IDPRM for transceiver GigabitEthernet2/0/0:
Description = SFP optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = FTRJ8519P1BNL-C6
Vendor Revision = A
Serial Number (SN) = FNS1037R8DH
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = IPUIALJRAA
Cisco part number = 10-2143-01
Device State = Enabled.
Date code (yy/mm/dd) = 06/09/14
Connector type = LC.
Encoding = 8B10B
NRZ
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

The following **show hw-module subslot** command sample output is for CWDM 1490:

```
Router# show hw-module subslot 2/0 transceiver 2 idprom
IDPRM for transceiver GigabitEthernet2/0/2:
Description = SFP optics (type 3)
Transceiver Type: = GE CWDM 1490 (28)
Product Identifier (PID) = FWDM-16217D49CSC
Vendor Revision = C
Serial Number (SN) = FNS10500HA9
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = CNTRVX0FAA
Cisco part number = 10-1884-01
Device State = Enabled.
Date code (yy/mm/dd) = 06/12/12
Connector type = LC.
Encoding = 8B10B
NRZ
Nominal bitrate = (2700 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

The following **show hw-module subslot** command sample output is for an XFP module:

```
Router# show hw-module subslot 2/2 transceiver 0 idprom brief
IDPRM for transceiver TenGigabitEthernet2/2/0:
Description = XFP optics (type 6)
Transceiver Type: = OC192 + 10GBASE-L (97)
Product Identifier (PID) = TRF5011AN-LF004
Vendor Revision = 05
Serial Number (SN) = ONT11061053
Vendor Name = CISCO-OPNEXT
Vendor OUI (IEEE company ID) = 00.0B.40 (2880)
CLEI code = WMOTBEVAAB
Cisco part number = 10-1989-02
Device State = Enabled.
Date code (yy/mm/dd) = 07/02/06
Connector type = LC.
Encoding = 64B/66B
SONET Scrambled
NRZ
```

Minimum bit rate = 9900 Mbits/s
Maximum bit rate = 10500 Mbits/s

The following sample output is for SFP-GE-SX:

```
Router# show hw-module subslot 2/0 transceiver 0 idprom dump
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = FTRJ8519P1BNL-C6
Vendor Revision = A
Serial Number (SN) = FNS1037R8DH
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = IPUIALJRAA
Cisco part number = 10-2143-01
Device State = Enabled.
SFP IDPROM Page 0xA0:
000: 03 04 07 00 00 00 01 00 00 00
010: 00 01 0D 00 00 00 37 1B 00 00
020: 43 49 53 43 4F 2D 46 49 4E 49
030: 53 41 52 20 20 20 00 00 90 65
040: 46 54 52 4A 38 35 31 39 50 31
050: 42 4E 4C 2D 43 36 41 20 20 20
060: 03 52 00 74 00 1A 00 00 46 4E
070: 53 31 30 33 37 52 38 44 48 20
080: 20 20 20 20 30 36 30 39 31 34
090: 20 20 58 80 01
SFP IDPROM Page 0xA2:
000: 6D 00 E3 00 67 00 F3 00 98 58
010: 69 78 90 88 71 48 1D 4C 01 F4
020: 17 70 03 E8 25 19 02 F5 25 19
030: 04 A9 E3 EE 01 DF 8F C5 02 EC
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 3E 5D
070: 01 79 C0 5B AC 86 01 00 00 00
080: 00 AA FF FD 01 00 00 00 01 00
090: 00 00 00 00 00 3A 1B 70 80 D8
100: 00 62 00 28 00 22 00 00 00 00
110: 82 F8 05 40 00 00 05 40 00 00
120: 00 00 00 00 00 00 00 01 49 50
130: 55 49 41 4C 4A 52 41 41 31 30
140: 2D 32 31 34 33 2D 30 31 56 30
150: 31 20 89 FB 55 00 00 00 00 78
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: AA AA 53 46 50 2D 47 45 2D 53
200: 20 20 20 20 20 20 20 20 20 20
210: 20 20 00 00 00 00 00 00 00 00
220: 00 00 00 A2 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 00 40
250: 00 40 00 00 00 00
Router#
```

Configuring the Network Clock for the 2-Port Gigabit Synchronous Ethernet SPA on a Cisco ASR 1000 Series Router

The 2-Port Gigabit Synchronous Ethernet SPA supports time, phase, and frequency awareness through Ethernet networks. The 2-Port Gigabit Synchronous Ethernet SPA on the Cisco SIP-40 enables clock selection and translation between the various clock frequencies. If the 2-Port Gigabit Synchronous Ethernet SPA interoperates with devices that do not support synchronization, synchronization features can be disabled or partially enabled to maintain backward compatibility.



Note

For additional details to understand how SyncE feature is implemented on Cisco ASR 1000 Series Router using 4 different configuration, please refer the chapter ‘Synchronous Ethernet Support On Cisco ASR 1000 Series Routers’ in the *Cisco ASR 1000 Series Software Configuration Guide*.

The network clock can be configured in global configuration mode and interface configuration mode:

- [Configuring the Network Clock in Global Configuration Mode, page 10-19](#)
- [Configuring the Network Clock in Interface Configuration Mode, page 10-23](#)

Configuring the Network Clock in Global Configuration Mode

Use the following commands to configure the network clock in global configuration mode on the Cisco SIP-40:

Command	Purpose
Router(config)# [no] network-clock synchronization automatic	Enables G.781 based automatic clock selection process. G.781 is the ITU-T Recommendation that specifies the synchronization layer functions.
Router(config)# [no] network-clock eec { 1 2 } <i>Example</i> Router(config)# network-clock eec 1	Configures the clocking system hardware with the desired parameters. These are the options: <ul style="list-style-type: none"> • For option 1, the default value is EEC-Option 1 (2048). • For option 2, the default value is EEC-Option 2 (1544).

Command	Purpose
<p>Router(config)#[no] network-clock synchronization ssm option {1 2 {GEN1 GEN2}}</p> <p><i>Example</i></p> <pre>Router(config)#network-clock synchronization ssm option 2 GEN1</pre>	<p>Configures the router to work in a synchronized network mode as described in G.781. The following are the options:</p> <ul style="list-style-type: none"> Option 1: refers to synchronization networks designed for Europe (SDH/ E1 framings are compatible with this option). Option 2: refers to synchronization networks designed for the US (SONET/T1 framings are compatible with this option). The default option is 1 and while choosing option 2, you need to specify the second generation message (GEN2) or first generation message (GEN1). <p>Note Network-clock configurations that are not common between options need to be configured again.</p>
<p>Router(config)#[no] network-clock synchronization mode QL-enabled</p>	<p>Configures the automatic selection process for quality level QL-enabled mode.</p> <p>Note QL-enabled mode succeeds only if there are any synchronization interfaces that are capable of sending SSM.</p>
<p>Router(config)#[no] esmc process</p>	<p>Enables or disables the ESMC process at system level.</p> <p>Note This command fails if there is no SyncE capable interface installed in the platform.</p>
<p>Router(config)#network-clock hold-off {0 <50-10000>} global</p> <p><i>Example</i></p> <pre>Router(config)#network-clock hold-off 75 global</pre>	<p>Configures general hold-off timer in milliseconds. The default value is 300 milliseconds.</p> <p>Note Displays a warning message for values below 300 ms and above 1800 ms.</p>
<p>Router(config)#network-clock external <slot/card/port> hold-off {0 <50-10000>}</p> <p><i>Example</i></p> <pre>Router(config)#network-clock external 3/1/1 hold-off 300</pre>	<p>Overrides hold-off timer value for external interface.</p> <p>Note Displays a warning message for values above 1800 ms, as waiting longer causes the clock to go into the holdover mode.</p>
<p>Router(config)#network-clock wait-to-restore <0-86400> global</p> <p><i>Example</i></p> <pre>Router(config)#network-clock external wait-to-restore 1000 global</pre>	<p>Sets the value for the wait-to-restore timer globally. The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds.</p> <p> Caution Ensure that you set the wait-to-restore values above 50 seconds to avoid a timing flap.</p>


Command	Purpose
<p>Router(config)# [no] network-clock input-source <priority> {interface <interface_name> <slot/card/port> top <slot/card/port/session> {external <slot/card/port> [t1 {sf efs d4} e1 [crc4 fas cas [crc4] 2m 10m]]}}</p> <p><i>Example</i></p> <pre>Router(config)# network-clock input-source 23 top 2/0/1/3</pre> <p><i>Example for GPS interface</i></p> <pre>Router(config)# network-clock input-source 1 external 3/0/0 10m</pre>	<p>Configures a clock source line interface, an external timing input interface, GPS interface, or a packet-based timing recovered clock as the input clock for the system and defines its priority. Priority is a number between 1 and 250.</p> <p>This command also configures the type of signal for an external timing input interface. These signals are:</p> <ul style="list-style-type: none"> • T1 with Standard Frame format or Extended Standard Frame format. • E1 with or without CRC4 • 2 MHz signal • Default for Europe or Option I is e1 crc4 if the signal type is not specified. • Default for North America or Option II is t1 esf if signal type is not specified. <p>Note The no version of the command reverses the command configuration, implying that the priority has changed to undefined and the state machine is informed.</p>
<p>Router(config)#[no] network-clock revertive</p>	<p>Specifies whether or not the clock source is revertive. Clock sources with the same priority are always non-revertive. The default value is non-revertive.</p> <p>In non-revertive switching, a switch to an alternate reference is maintained even after the original reference recovers from the failure that caused the switch. In revertive switching, the clock switches back to the original reference after that reference recovers from the failure, independent of the condition of the alternate reference.</p>

Command	Purpose
<p>Router(config)#network-clock quality-level {tx rx} <value> {interface <interface name> <slot/card/port> external <slot/card/port> controller <slot/card/port>}</p> <p><i>Example</i></p> <pre>Router(config)# network-clock quality-level rx QL-PRC external 4/0/0 e1 crc4</pre>	<p>Specifies the QL value for line or external timing input or output. The value is based on a global interworking Option.</p> <ul style="list-style-type: none"> If Option 1 is configured, the available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. If Option 2 is configured with GEN 2, the available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4 and QL-DUS. If option 2 is configured with GEN1, the available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4 and QL-DUS <p>Note This command is not supported for synchronous ethernet interfaces.</p>
<p>Router(config)#network-clock output-source line <priority> {interface <interface_name> controller {t1 e1} <slot/card/port>} {external <slot/card/port> [t1 {sf efs d4} e1 [crc4] fas cas [crc4] 2m 10m]}</p> <p><i>Example</i></p> <pre>Router(config)# network-clock output-source line 1 interface GigabitEthernet3/0/0</pre>	<p>Transmits the line clock sources to external timing output interfaces.</p> <p>Note A line can be configured to be the output source for only one external interface.</p> <p>This command provides the station clock output as per G.781. We recommend that you use the interface level command instead of global commands. Global command should preferably be used for interfaces that do not have an interface sub mode. For more information on configuring network clock in interface level mode, see Configuring the Network Clock in Interface Configuration Mode, page 10-23.</p>
<p>Router(config)#network-clock output-source system <priority> {external <slot/card/port> [t1 {sf efs d4} e1 [crc4] fas cas [crc4] 2m 10m]}</p> <p><i>Example</i></p> <pre>Router(config)#network-clock output-source system 55 external 3/0/1 t1 efs</pre>	<p>Allows transmitting the system clock to external timing output interfaces.</p> <p>This command provides station clock output as per G.781. We recommend that you use the interface level command instead of global commands. Global command should preferably be used for interfaces that do not have an interface sub mode. For more information on configuring network clock in interface level mode, see Configuring the Network Clock in Interface Configuration Mode, page 10-23.</p>
<p>Router(config)#[no] network-clock synchronization participate <slot number></p> <p><i>Example</i></p> <pre>Router(config)#[no] network-clock synchronization participate 2</pre>	<p>Enables or disables a slot from participating in network-clock algorithm.</p> <p>By default all slots are participating slots.</p> <p>Note A slot cannot be disabled from participation if it's primary source, secondary source, or system to external is valid.</p>

Configuring the Network Clock in Interface Configuration Mode

Use the following commands in the interface configuration mode to configure the network clock and timers on the Cisco ASR 1000 Series Router SIP-40.

Command	Purpose
Router(config-if)#synchronous mode	Configures the ethernet interface to synchronous mode and this automatically enables the ESMC and Quality Level process on the interface. Note This command is applicable to Synchronous Ethernet capable interfaces. The default value is asynchronous mode.
Router(config-if)#esmc mode [tx rx <cr>] <i>Example:</i> Router(config-if)#esmc mode tx	Enables or disables ESMC process on the interface. Note If the interface is configured as line source but does not receive ESMC message from peer node on the interface, then the interface is removed from selectable clock source list. By default this is enabled for synchronous mode and disabled for asynchronous mode. Note This command is not supported for non-synchronous ethernet interfaces.
Router(config-if)#network-clock source quality-level <value> {tx rx} <i>Example:</i> Router(config-if)#network-clock source quality-level QL-PRC	The command forces QL value to local clock selection process and it is considered by the clock selection process as a value from network. The value is based on global interworking Option. <ul style="list-style-type: none"> • If Option 1 is configured, the available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. • If Option 2 is configured with GEN 2, the available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4 and QL-DUS. • If option 2 is configured with GEN1, the available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4 and QL-DUS Note This command is applicable to Synchronous Ethernet capable interfaces.
Router(config-if)#network-clock hold-off <0 50-10000> <i>Example:</i> Router(config-if)#network-clock hold-off 1000	Configures hold-off timer for interface. The default value is 300 milliseconds. Note Displays a warning for values below 300 ms and above 1800 ms.

Command	Purpose
Router(config-if)#[no] network-clock wait-to-restore <0-86400> <i>Example:</i> Router(config-if)#network-clock wait-to-restore 1000	Configures the wait-to-restore timer on the SyncE interface.  Caution Ensure that you set the wait-to-restore values above 50 seconds to avoid timing flap.
Router(config-if)# [no] esmc mode ql-disabled	Disables the quality level mode. The default mode for synchronous ethernet is ql-enabled. Note This command is not supported for non-synchronous ethernet interfaces.

Managing Synchronization

You can manage the synchronization using the following management commands:

Command	Purpose
Router# network-clock set lockout {interface interface_name slot/card/port external slot/card/port} <i>Example:</i> Router#network-clock set lockout interface GigabitEthernet 0/0/0 Router#network-clock clear lockout interface GigabitEthernet 0/0/0	Locks out a clock source. A clock source flagged as lock-out is not selected for SyncE. To clear the lock-out on a source, use network-clock clear lockout {interface interface_name slot/card/port external slot/card/port} command. Note Lockout takes precedence over force switch and force switch overrides the manual switch.
Router# network-clock switch force {interface interface_name slot/card/port external slot/card/port internal T0} <i>Example:</i> Router#network-clock switch force interface GigabitEthernet 0/0/0 external 0/2/0	Forcefully selects a synchronization source irrespective of whether the source is available and is within the range.

Command	Purpose
Router# network-clock switch manual {interface interface_name slot/card/port external slot/card/port internal T0} <i>Example:</i> Router#network-clock switch manual interface GigabitEthernet 0/0/0 T0	Manually selects a synchronization source, provided the source is available and is within the range.
Router#network-clock clear switch {t0 external <slot/card/port> [10m 2m]} <i>Example:</i> Router#network-clock clear switch t0	Clears the forced switch and manual switch commands.

Sample Configuration

Example 10-1 Configuration for QL-Enabled Mode Clock Selection.

```

network-clock synchronization automatic
network-clock synchronization mode QL-enabled
network-clock input-source 1 interface GigabitEthernet0/2/0
network-clock input-source 1 interface ATM6/0/0
!
interface GigabitEthernet0/2/1
 no ip address
 clock source line
 synchronous mode
end
!
interface ATM6/0/0
 no ip address
 atm framing sdh
 no atm enable-ilmi-trap
end

```

Example 10-2 Configuration for Line to External

```

network-clock synchronization automatic
network-clock synchronization mode QL-enabled
network-clock input-source 1 External 3/0/0
network-clock output-source line 1 interface GigabitEthernet3/0/0 External 3/0/0 e1 crc4

interface GigabitEthernet3/0/0
 no ip address
 no negotiation auto
 synchronous mode

```

Example 10-3 GPS Configuration

```

10MHz signal
network-clock input-source 1 External 3/0/0 10m

2M signal

```

```
network-clock input-source 1 External 3/0/0 10m
```

Verifying Synchronous Ethernet Configuration

Use the **show network-clocks synchronization** command to display the sample output as shown here:

```
Router#show network-clocks synchronization
Router# show network-clocks synchronization
Symbols:      En - Enable, Dis - Disable, Adis - Admin Disable
              NA - Not Applicable
              *  - Synchronization source selected
              #  - Synchronization source force selected
              &  - Synchronization source manually switched
```

```
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet1/1/0
Hold-off (global) : 300 ms
Wait-to-restore (global) : 30 sec
Tsm Delay : 180 ms
Revertive : No
```

Nominated Interfaces

Interface	SigType	Mode/QL	Prio	QL_IN	ESMC Tx	ESMC Rx
Internal	NA	NA/Dis	251	QL-SEC	NA	NA
*Gi1/1/0	NA	Sync/En	1	QL-PRC	-	-

Use the **show network-clocks synchronization detail** command to display all the details of the network clock synchronization parameters at the global and interface levels, as shown here:

```
Router# show network-clocks synchronization detail
Symbols:      En - Enable, Dis - Disable, Adis - Admin Disable
              NA - Not Applicable
              *  - Synchronization source selected
              #  - Synchronization source force selected
              &  - Synchronization source manually switched
```

```
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet1/1/0
Hold-off (global) : 300 ms
Wait-to-restore (global) : 30 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 2
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (ql_mode_enable)-> 1A (begin)-> 1A (sf_change)-> 1A
(sf_change)-> 1A (ql_change)-> 1A (ql_change)-> 1A (ql_change)-> 1A (ql_change)-> 1A
```

Nominated Interfaces

Interface	SigType	Mode/QL	Prio	QL_IN	ESMC Tx	ESMC Rx
-----------	---------	---------	------	-------	---------	---------

Internal	NA	NA/Dis	251	QL-SEC	NA	NA
*Gi1/1/0	NA	Sync/En	1	QL-PRC	-	-
External 1/3/0	E1 CRC4	NA/En	2	QL-FAILED	NA	NA

Interface:

Local Interface: Internal

Signal Type: NA

Mode: NA(ql-enabled)

SSM Tx: DISABLED

SSM Rx: DISABLED

Priority: 251

QL Receive: QL-SEC

QL Receive Configured: -

QL Receive Overridden: -

QL Transmit: -

QL Transmit Configured: -

Hold-off: 0

Wait-to-restore: 30

Lock Out: FALSE

Signal Fail: FALSE

Alarms: FALSE

Slot Disabled: FALSE

Local Interface: Gi1/1/0

Signal Type: NA

Mode: Synchronous(ql-enabled)

ESMC Tx: ENABLED

ESMC Rx: ENABLED

Priority: 1

QL Receive: QL-PRC

QL Receive Configured: -

QL Receive Overridden: -

QL Transmit: QL-DNU

QL Transmit Configured: -

Hold-off: 300

Wait-to-restore: 30

Lock Out: FALSE

Signal Fail: FALSE

Alarms: FALSE

Slot Disabled: FALSE

Use the **show interface accounting** command to display packets accounting statistics, as shown here:

Router#**show interfaces GigabitEthernet 0/2/0 accounting**

GigabitEthernet0/2/0

Protocol	Pkts In	Chars In	Pkts Out	Chars Out
DEC MOP	14	1134	14	1806
ARP	0	0	2	224
CDP	145	55970	145	63049
ESMC	3246	194760	7099	823484

Use the **show esmc** command to display the sample output, as shown here:

Router#**show esmc**

SYNCE-2RU#show esmc

Interface: GigabitEthernet0/2/0

Administrative configurations:

Mode: Synchronous

ESMC TX: Enable

ESMC RX: Enable

QL TX: -

QL RX: -

Operational status:

```

Port status: UP
QL Receive: QL-DNU
QL Transmit: QL-SEC
QL rx overridden: QL-DNU
ESMC Information rate: 1 packet/second
ESMC Expiry: 5 second

Interface: GigabitEthernet0/2/1
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-SEC
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second

Interface: GigabitEthernet0/3/0
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-SEC
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second

Interface: GigabitEthernet0/3/1
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: DOWN
  QL Receive: QL-DNU
  QL Transmit: -
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second

```

Use the **show esmc detail** command to display all the details of the ESMC parameters at the global and interface levels, as shown here:

```

Router#show esmc detail
Interface: GigabitEthernet0/2/0
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -

```



```
QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-SEC
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 0
  ESMC INFO pkts out: 629451
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 0

Interface: GigabitEthernet0/2/1
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-SEC
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 0
  ESMC INFO pkts out: 629451
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 0

Interface: GigabitEthernet0/3/0
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX: Enable
  QL TX: -
  QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: QL-SEC
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 0
  ESMC INFO pkts out: 624901
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 0

Interface: GigabitEthernet0/3/1
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
```

```
ESMC RX: Enable
QL TX: -
QL RX: -
Operational status:
  Port status: DOWN
  QL Receive: QL-DNU
  QL Transmit: -
  QL rx overridden: QL-DNU
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Running
  ESMC Rx Timer: Running
  ESMC Tx interval count: 0
  ESMC INFO pkts in: 0
  ESMC INFO pkts out: 0
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 0
```

Troubleshooting the Synchronous Ethernet Configuration

The following debug commands are available for troubleshooting the synchronous Ethernet configuration on the Cisco ASR 1000 Series Router:

Table 10-1 *Debug Commands for Troubleshooting*

Debug Command	Purpose
<code>debug platform network-clock</code>	Debugs issues related to the network clock such as alarms, OOR, active-standby sources not selected correctly, and so on.
<code>debug esmc error</code> <code>debug esmc event</code> <code>debug esmc packet [interface</code> <interface name>] <code>debug esmc packet rx [interface</code> <interface name>] <code>debug esmc packet tx [interface</code> <interface name>]	Verifies whether the ESMC packets are transmitted and received with the correct quality-level values.

Troubleshooting Scenarios



Note

Before you troubleshoot, ensure that all the network clock synchronization configurations are complete.

Table 10-2 provides the troubleshooting scenarios encountered while configuring the synchronous ethernet.

Table 10-2 *Troubleshooting scenarios*

Problem	Solution
Clock selection	<ul style="list-style-type: none"> Verify that there are no alarms on the interfaces. Use the show network-clock synchronization detail command to check this. Ensure that the nonrevertive configurations are in place. Reproduce the issue and collate the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact the Cisco technical support if the issue persists.

Problem	Solution
Incorrect QL values	<ul style="list-style-type: none">• Ensure that there is no framing mismatch with the SSM option.• Reproduce the issue using the debug network-clock errors, debug network-clock event, and debug platform ssm commands. Also, enable the debug hw-module subslot command.
Alarms	<ul style="list-style-type: none">• Reproduce the issue using the debug platform network-clock command enabled in the route processor. Alternatively, enable the debug network-clock event and debug network-clock errors commands.

Configuration Examples

This section includes the following configuration examples:

- [Basic Interface Configuration Example, page 10-33](#)
- [MAC Address Configuration Example, page 10-33](#)
- [MAC Address Accounting Configuration Example, page 10-34](#)
- [MTU Configuration Example, page 10-34](#)
- [VLAN Configuration Example, page 10-35](#)

Basic Interface Configuration Example

The following example shows how to enter global configuration mode to specify the interface that you want to configure, configure an IP address for the interface, and save the configuration. This example configures interface port 1 on the SPA that is located in subslot 0 of the SIP that is installed in slot 0 of the Cisco ASR 1000 Series Router:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address.
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure an IP address.
!
Router(config-if)# ip address 192.168.50.1 255.255.255.0
!
! Start the interface.
!
Router(config-if)# no shut
!
! Save the configuration to NVRAM.
!
Router(config-if)# exit
Router# copy running-config startup-config
```

MAC Address Configuration Example

The following example changes the default MAC address on the interface to 1111.2222.3333:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Modify the MAC address.
!
Router(config-if)# mac-address 1111.2222.3333
```

MAC Address Accounting Configuration Example

The following example enables MAC Address Accounting:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Enable MAC address accounting
Router(config)# ip accounting mac-address {input | output}
Router(config-if)# ip accounting ?
access-violations Account for IP packets violating access lists on this interface
mac-address Account for MAC addresses seen on this interface
output-packets Account for IP packets output on this interface
precedence Count packets by IP precedence on this interface
<cr>
Router(config-if)# ip accounting mac-address ?
input Source MAC address on received packets
output Destination MAC address on transmitted packets
Router(config-if)# ip accounting mac-address input ?
<cr>
! Specify MAC address accounting for traffic entering the interface.
!
Router(config-if)# ip accounting mac-address input
! Specify MAC address accounting for traffic leaving the interface.
!
Router(config-if)# ip accounting mac-address output
Router(config-if)# end
! Verify the MAC Address on the interface.
!
Router# show interfaces GigabitEthernet 4/0/2 mac-accounting
GigabitEthernet4/0/2
Input (511 free)
000f.f7b0.5200(26 ): 124174 packets, 7450440 bytes, last: 1884ms ago
Total: 124174 packets, 7450440 bytes
Output (511 free)
000f.f7b0.5200(26 ): 135157 packets, 8109420 bytes, last: 1884ms ago
Total: 135157 packets, 8109420 bytes
```

MTU Configuration Example

The following example sets the interface MTU to 9216 bytes:



Note

The SPA automatically adds an additional 38 bytes to the configured interface MTU size.

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
Router(config-if)# mtu 9216
```

VLAN Configuration Example

The following example creates subinterface number 268 on SPA interface port 2 (the third port), and configures the subinterface on the VLAN with ID number 268, using IEEE 802.1Q encapsulation:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 2/0/1.268
!
! Configure dot1q encapsulation and specify the VLAN ID.
!
Router(config-subif)# encapsulation dot1q 268
```




CHAPTER 11

Troubleshooting the Gigabit Ethernet SPAs

This chapter describes techniques that you can use to troubleshoot the operation of your Gigabit Ethernet SPAs.

It includes the following sections:

- [General Troubleshooting Information, page 11-1](#)
- [Performing Basic Interface Troubleshooting, page 11-2](#)
- [Understanding SPA Automatic Recovery, page 11-6](#)
- [Using the Cisco IOS Event Tracer to Troubleshoot Problems, page 11-6](#)
- [Preparing for Online Insertion and Removal of a SPA, page 11-7](#)

The first section provides information about basic interface troubleshooting. If you are having a problem with your SPA, use the steps in the “[Performing Basic Interface Troubleshooting](#)” section on [page 11-2](#) to begin your investigation of a possible interface configuration problem.

To perform more advanced troubleshooting, see the other sections in this chapter.

General Troubleshooting Information

This section describes general information for troubleshooting SIPs and SPAs. It includes the following sections:

- [Using debug Commands, page 11-2](#)
- [Using show Commands, page 11-2](#)

Using debug Commands



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Along with the other **debug** commands supported on the Cisco ASR 1000 Series Aggregation Services Routers, you can obtain specific debug information for SPAs on the Cisco ASR 1000 Series Routers using the **debug hw-module subslot** privileged EXEC command.

The **debug hw-module subslot** command is intended for use by Cisco technical support personnel.

For information about other **debug** commands supported on the Cisco ASR 1000 Series Routers, refer to the *Cisco IOS Debug Command Reference* and any related feature documents for the applicable Cisco IOS release.

Using show Commands

There are several **show** commands that you can use to monitor and troubleshoot the SIPs and SPAs on the Cisco ASR 1000 Series Aggregation Services Routers. This chapter describes using the **show interfaces** command to perform troubleshooting of your SPA.

For more information about **show** commands to verify and monitor SIPs and SPAs, see [Chapter 5, “Troubleshooting the SIP”](#), [Chapter 10, “Configuring the Ethernet SPAs”](#), and the Cisco IOS technology area command reference books.

Performing Basic Interface Troubleshooting

You can perform most of the basic interface troubleshooting using the **show interfaces fastethernet**, **show interfaces gigabitethernet**, or **show interfaces tengigabitethernet** command and examining several areas of the output to determine how the interface is operating.

The following example shows output from both the **show interfaces gigabitethernet** and **show interfaces tengigabitethernet** commands with some of the significant areas of the output to observe shown in bold:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
  Hardware is SPA-1X10GE-L-V2, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 1000Mb/s, link type is force-up, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:18:49, output 03:18:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```

Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1703 packets input, 638959 bytes, 0 no buffer
    Received 23 broadcasts (0 IP multicasts)
      0 runs, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 1670 multicast, 0 pause input
    1715 packets output, 656528 bytes, 0 underruns
      0 output errors, 0 collisions, 4 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out

```

```

Router# show interfaces tengigabitethernet 0/0/0
TenGigabitEthernet7/0/0 is up, line protocol is up (connected)
  Hardware is TenGigEther SPA, address is 0000.0c00.0102 (bia 000f.342f.c340)
  Internet address is 15.1.1.2/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
  Last clearing of "show interface" counters 20:24:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
  237450882 packets input, 15340005588 bytes, 0 no buffer
    Received 25 broadcasts (0 IP multicasts)
      0 runs, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 0 multicast, 0 pause input
      0 input packets with dribble condition detected
    1676 packets output, 198290 bytes, 0 underruns
      0 output errors, 0 collisions, 4 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 PAUSE output
      0 output buffer failures, 0 output buffers swapped out

```

To verify that your interface is operating properly, complete the steps in [Table 11-1](#):

Table 11-1 *Basic Interface Troubleshooting Steps*

	Action	Example
Step 1	From global configuration mode, enter the show interfaces gigabitethernet , show interfaces tengigabitethernet , or show interfaces fastethernet command.	Router# show interfaces gigabitethernet 2/0/1 Router# show interfaces tengigabitethernet 7/0/0 Router# show interfaces fastethernet 3/0/0
Step 2	Verify that the interface is up.	Router# show interfaces gigabitethernet 2/0/1 GigabitEthernet2/0/1 is up , line protocol is up Router# show interfaces tengigabitethernet 7/0/0 TenGigabitEthernet7/0/0 is up , line protocol is up (connected) Router# show interfaces fastethernet 3/0/0 FastEthernet3/0/0 is up , line protocol is up
Step 3	Verify that the line protocol is up.	Router# show interfaces gigabitethernet 2/0/1 GigabitEthernet2/0/1 is up, line protocol is up Router# show interfaces tengigabitethernet 7/0/0 TenGigabitEthernet7/0/0 is up, line protocol is up (connected) Router# show interfaces fastethernet 3/0/0 FastEthernet3/0/0 is up, line protocol is up
Step 4	Observe the CRC counter.	0 input errors, 0 CRC, 0 frame, 130043940 overrun, 0 ignored
Step 5	Observe the carrier signal counters.	0 lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped out

For more information about the verification steps and possible responses to correct detected problems, see the following sections:

- [Verifying the Interface Is Up](#), page 11-4
- [Verifying the Line Protocol Is Up](#), page 11-5
- [Verifying the CRC Counter](#), page 11-5
- [Verifying the Carrier Signal](#), page 11-5

Verifying the Interface Is Up

In the output from the **show interfaces gigabitethernet**, **show interfaces tengigabitethernet**, or **show interfaces fastethernet** command, verify that the interface is up. If the interface is down, perform the following corrective actions:

- If the interface is *administratively down*, use the **no shutdown** interface configuration command to enable the interface.
- Be sure that the cable is fully connected.
- Verify that the cable is not bent or damaged. If the cable is bent or damaged, the signal will be degraded.

- Verify that a hardware failure has not occurred. Observe the LEDs to confirm the failure. See the other troubleshooting sections of this chapter, and refer to the *Cisco ASR 1000 Series Aggregation Services Router Hardware Installation Guide*. If the hardware has failed, replace the SPA as necessary.
- Check the autonegotiation status.

Verifying the Line Protocol Is Up

In the output from the **show interfaces gigabitethernet**, **show interfaces tengigabitethernet**, or **show interfaces fastethernet** command, verify that the line protocol is up. If the line protocol is down, the line protocol software processes have determined that the line is unusable.

Perform the following corrective actions:

- Replace the cable.
- Check the local and remote interface for misconfiguration.
- Verify that a hardware failure has not occurred. Observe the LEDs to confirm the failure. See the other troubleshooting sections of this chapter, and refer to the *Cisco ASR 1000 Series Aggregation Services Router Hardware Installation Guide*. If the hardware has failed, replace the SPA as necessary.

Verifying the CRC Counter

In the output from the **show interfaces gigabitethernet**, **show interfaces tengigabitethernet**, or **show interfaces fastethernet** command, observe the value of the CRC counter. Excessive noise will cause high CRC errors accompanied by a low number of collisions.

Perform the following corrective actions if you encounter high CRC errors:

- Check the cables for damage.
- Verify that the correct cables are being used for the SPA interface.

Verifying the Carrier Signal

In the output from the **show interfaces gigabitethernet**, **show interfaces tengigabitethernet**, or **show interfaces fastethernet** command, observe the value of the carrier signal counters. The lost carrier counter shows the number of times that the carrier was lost during transmission. The no carrier counter shows the number of times that the carrier was not present during transmission.

Carrier signal resets can occur when an interface is in loopback mode or shut down.

Perform the following corrective actions if you observe the carrier signal counter incrementing outside of these conditions:

- Check the interface for a malfunction.
- Check for a cable problem.

Understanding SPA Automatic Recovery

When Gigabit Ethernet SPAs encounter thresholds for certain types of errors and identify a fatal error, the SPAs initiate an automatic recovery process.

You do not need to take any action unless the error counters reach a certain threshold, and multiple attempts for automatic recovery by the SPA fail.

The Gigabit Ethernet SPAs might perform automatic recovery for the following types of errors:

- SPI4 TX/RX out of frame
- SPI4 TX train valid
- SPI4 TX DIP4
- SPI4 RX DIP2

When Automatic Recovery Occurs

If the SPI4 errors occur more than 25 times within 10 milliseconds, the SPA automatically deactivates and reactivates itself. Error messages are logged on the console indicating the source of the error and the status of the recovery.

If Automatic Recovery Fails

If the SPA attempts automatic recovery more than five times in an hour, then the SPA deactivates itself and remains deactivated.

To troubleshoot automatic recovery failure for a SPA, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Use the show hw-module subslot slot/subslot oir command to verify the status of the SPA. The status is shown as “failed” if the SPA has been powered off due to five consecutive failures. |
| Step 2 | If you verify that automatic recovery has failed, perform OIR of the SPA. For information about performing OIR, see the “Preparing for Online Insertion and Removal of a SPA” section on page 11-7 . |
| Step 3 | If reseating the SPA after OIR does not resolve the problem, replace the SPA hardware. |
-

Using the Cisco IOS Event Tracer to Troubleshoot Problems

This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, Route Processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

For more information about using the Event Tracer feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/evnttrcr.html

Preparing for Online Insertion and Removal of a SPA

The Cisco ASR 1000 Series Routers support online insertion and removal (OIR) of the SIP, in addition to each of the SPAs. Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This means that a SIP can remain installed in the router with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see [Chapter 5, “Troubleshooting the SIP.”](#)



PART 4

Packet over SONET Shared Port Adapters



CHAPTER 12

Overview of the POS SPAs

This chapter provides an overview of the release history, and feature and Management Information Base (MIB) support for the Packet over SONET (POS) SPAs on the Cisco ASR 1000 Series Aggregation Services Routers.

This chapter includes the following sections:

- [Release History, page 12-2](#)
- [POS Technology Overview, page 12-2](#)
- [Supported Features, page 12-3](#)
- [Restrictions, page 12-5](#)
- [Supported MIBs, page 12-5](#)
- [SPA Architecture, page 12-6](#)
- [Displaying the SPA Hardware Type, page 12-9](#)

Release History

Release	Modification
Cisco IOS XE Release 2.4	Support for the following SPAs was introduced on the Cisco ASR 1000 Series Routers: <ul style="list-style-type: none"> • 2-Port, 4-Port, and 8-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA • 1-Port OC-48c/STM-16 POS SPA • 8-Port OC-3c/STM-1 POS SPA • 1-Port OC-192c/STM-64 POS XFP SPA
Cisco IOS XE Release 2.2	Support for the following SPAs was introduced on the Cisco ASR 1000 Series Routers: <ul style="list-style-type: none"> • 2-Port OC-48c/STM-16 POS/RPR SPA • 4-Port OC-48c/STM-16 POS/RPR SPA
Cisco IOS XE Release 2.1	Support for the following SPAs was introduced on the Cisco ASR 1000 Series Routers: <ul style="list-style-type: none"> • 2-Port OC-3c/STM-1 POS SPA • 4-Port OC-3c/STM-1 POS SPA • 1-Port OC-12c/STM-4 POS SPA

POS Technology Overview

Packet-over-SONET is a high-speed method of transporting IP traffic between two points. This technology combines the Point-to-Point Protocol (PPP), High-level Data Link Control (HDLC), or Frame Relay with Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) interfaces.

SONET is an octet-synchronous multiplex scheme defined by the American National Standards Institute (ANSI) standard (T1.1051988) for optical digital transmission at hierarchical rates from 51.840 Mbps to 9.95 Gbps (Synchronous Transport Signal, STS-1 to STS-48) and greater. SDH is an equivalent international standard for optical digital transmission at hierarchical rates from 155.520 Mbps (Synchronous Transfer Mode-1 [STM-1]) to 9.95 Gbps (STM-16) and greater.

SONET specifications have been defined for single-mode fiber and multimode fiber. The POS SPAs allow transmission over single-mode and multimode optical fiber at Optical Carrier 3, 12, 48, and 192 (OC-3, OC-12, OC-48, and OC-192) rates.

SONET/SDH transmission rates are integral multiples of 51.840 Mbps. The following transmission multiples are currently specified and used on the POS SPAs on the Cisco ASR 1000 Series Routers:

- OC-3c/STM-1—155.520 Mbps
- OC-12c/STM-4—622.080 Mbps
- OC-48c/STM-16—2.488 Gbps
- OC-192/STM-64 XFP—9.95 Gbps

Supported Features

- Small form-factor pluggable (SFP) and XFP optics module OIR
- Field-programmable gate array (FPGA) upgrade support
- IPv4 and IPv6 addressing

SONET/SDH Compliance Features

- American National Standards Institute (ANSI) T1.105
- ITU-T G.707, G.783, G.957, G.958
- Telcordia GR-253-CORE: SONET Transport Systems: Common Generic Criteria
- Telcordia GR-1244: Clocks for the Synchronized Network: Common Generic Criteria

SONET/SDH Error, Alarm, and Performance Monitoring Features

- Signal failure bit error rate (SF-BER)
- Signal degrade bit error rate (SD-BER)
- Signal label payload construction (C2)
- Path trace byte (J1)
- Section:
 - Loss of signal (LOS)
 - Loss of frame (LOF)
 - Error counts for B1
 - Threshold crossing alarms (TCA) for B1
- Line:
 - Line alarm indication signal (LAIS)
 - Line remote defect indication (LRDI)
 - Line remote error indication (LREI)
 - Error counts for B2
 - Threshold crossing alarms (TCA) for B2
- Path:
 - Path alarm indication signal (PAIS)
 - Path remote defect indication (PRDI)
 - Path remote error indication (PREI)
 - Error counts for B3
 - Threshold crossing alarms (TCA) for B3
 - Loss of pointer (LOP)
 - New pointer events (NEWPTR)

- Positive stuffing event (PSE)
- Negative stuffing event (NSE)

SONET/SDH Synchronization Features

- Local (internal) timing (for inter-router connections over dark fiber or Wavelength Division Multiplex [WDM] equipment)
- Loop (line) timing (for connecting to SONET/SDH equipment)
- +/- 20 ppm clock accuracy over full operating temperature

WAN Protocol Features

- HDLC and Frame Relay IETF encapsulation
- Multiprotocol Label Switching (MPLS)
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC framing*
- RFC 2615, *PPP over SONET/SDH* (with 1+x43 self-synchronous payload scrambling)

Network Management Features

- Simple Network Management Protocol (SNMP) Management Information Base (MIB) counters
- Local (diagnostic) loopback
- Network loopback
- NetFlow Data Export
- RFC 3592 performance statistics for timed intervals (current, 15-minute, multiple 15-minute, and 1-day intervals):
 - Section CV (code violations)
 - Section ES (error seconds)
 - Section SES (severely errored seconds)
 - Near end & Far end Line CV
 - Near end & Far end Line ES
 - Near end & Far end Line SES
 - Near end & Far end Line UAS (unavailable seconds)
 - Near end & Far end Path CV
 - Near end & Far end Path ES
 - Near end & Far end Path SES
 - Near end & Far end Path UAS

Restrictions



Note

For other SIP-specific features and restrictions see also [Chapter 3, “Overview of the SIP”](#).

[Table 12-1](#) provides information about POS feature compatibility and restrictions by SIP and SPA combination.

Table 12-1 *POS Feature Compatibility and Restrictions by SIP and SPA Combination*

Feature	Cisco ASR1000-SIP10
Bridge Control Protocol (BCP)	Not supported on any POS SPAs.
Dynamic Packet Transport (DPT), which includes RPR/SRP	Not supported on any POS SPAs.
Frame Relay	Supported on all POS SPAs.

Supported MIBs

The following MIBs are supported for the POS SPAs on the Cisco ASR 1000 Series Routers:

- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENVMON-MIB (For NPEs, NSEs, line cards, and MSCs only)
- CISCO-EXTENDED-ENTITY-MIB
- CISCO-OPTICAL-MIB
- ENTITY-MIB
- OLD-CISCO-CHASSIS-MIB
- IF-MIB
- SONET-MIB (RFC 2558, *Definitions of Managed Objects for SONET/SDH Interface Type*)
- MIB II

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

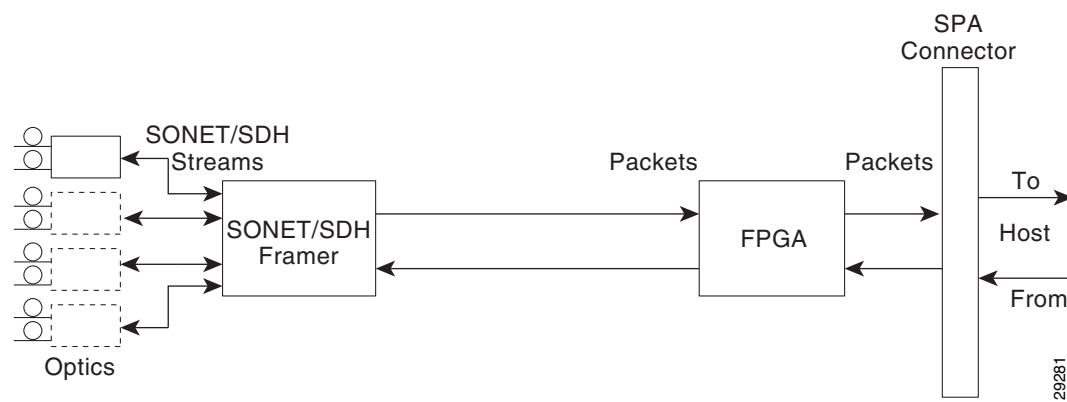
SPA Architecture

This section provides an overview of the architecture of the POS SPAs and describes the path of a packet in the ingress and egress directions. Some of these areas of the architecture are referenced in the SPA software and can be helpful to understand when troubleshooting or interpreting some of the SPA CLI and **show** command output.

4-Port OC-3c/STM-1 POS SPA Architecture

Figure 12-1 identifies some of the hardware devices that are part of the POS SPA architecture. The figure shows the four ports that are supported by the 4-Port OC-3c/STM-1 POS SPA only.

Figure 12-1 4-Port OC-3c/STM-1 POS SPA Architecture



Every incoming and outgoing packet on the 4-Port OC-3c/STM-1 POS SPA goes through the SONET/SDH framer and field-programmable gate array (FPGA) devices.

Path of a Packet in the Ingress Direction

The following steps describe the path of an ingress packet through the 4-Port OC-3c/STM-1 POS SPA:

1. The framer receives SONET/SDH streams from the SFP optics, extracts clocking and data, and processes the section, line, and path overhead.
2. The framer extracts the POS frame payload and verifies the frame size and frame check sequence (FCS).
3. The framer passes valid frames to the field-programmable gate array (FPGA) on the SPA.
4. The FPGA on the SPA transfers frames to the host through the SPI4.2 bus for further processing and switching.

Path of a Packet in the Egress Direction

The following steps describe the path of an egress packet through the 4-Port OC-3c/STM-1 POS SPA:

1. The host sends packets to the FPGA on the SPA using the SPI4.2 bus.
2. The FPGA on the SPA stores the data in the appropriate channel first-in first-out (FIFO) queue.
3. The FPGA on the SPA passes the packet to the framer.

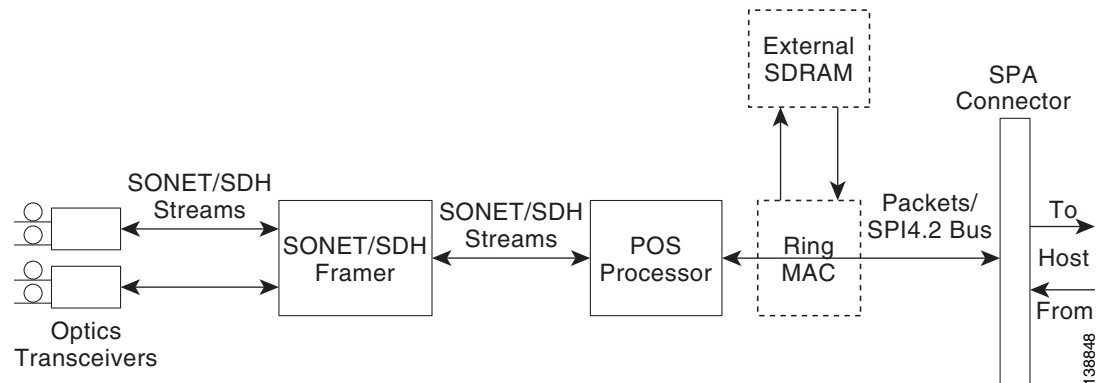
4. The framer accepts the data and stores it in the appropriate channel queue.
5. The framer adds the FCS and SONET/SDH overhead.

The framer sends the data to the SFP optics for transmission onto the network.

2-Port OC-48c/STM-16 POS SPA Architecture

Figure 2 identifies the primary hardware devices that are part of the 2-Port OC-48c/STM-16 POS SPA architecture.

Figure 2 2-Port OC-48c/STM-16 POS SPA Architecture



Path of a Packet in the Ingress Direction

The following steps describe the path of an ingress packet through the 2-Port OC-48c/STM-16 POS SPA:

1. The framer receives SONET/SDH streams from the SFP optics, extracts clocking and data, and processes the section, line, and path overhead.
2. The framer detects Loss of Signal (LOS), Loss of Frame (LOF), Severely Errored Frame (SEF), Line Alarm Indication Signal (AIS-L), Loss of Pointer (LOP), Line Remote Defect Indication Signal (Enhanced RDI-L), Path Alarm Indication Signal (AIS-P), Standard and Enhanced Path Remote Defect Indication Signal (RDI-P), Path Remote Error Indication (Enhanced REI-P). The framer extracts or inserts DCC bytes.
3. The framer processes the S1 synchronization status byte, the pointer action bytes (per Telcordia GR-253-CORE), and extracts or inserts DCC bytes.
4. The POS processor extracts the POS frame payload and verifies the frame size and frame check sequence (FCS).
5. The POS processor supports PPP, Frame Relay, or HDLC modes and optionally performs payload scrambling.
6. The POS processor passes valid frames to the System Packet Level Interface 4.2 (SPI4.2) interface on the SPA.
7. The SPI4.2 interface transfers frames to the host through the SPI4.2 bus for further processing and switching.

Path of a Packet in the Egress Direction

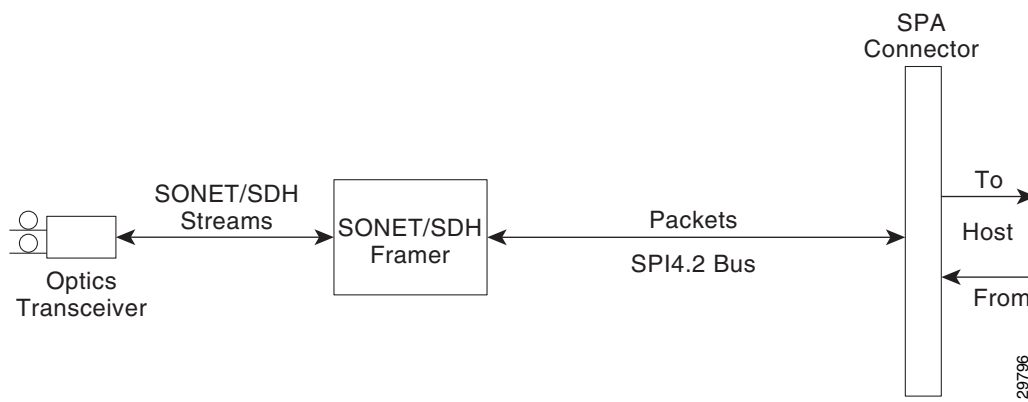
The following steps describe the path of an egress packet through the 2-Port OC-48c/STM-16 POS SPA:

1. The host sends packets to the SPA using the SPI4.2 bus.
2. The SPA stores the data in the appropriate SPI4 channel's first-in first-out (FIFO) queue.
3. The SPA passes the packet from the SPI4 interface to the POS processor where it is encapsulated in a POS frame and FCS is added.
4. The POS frame is sent to the SONET/SDH framer where it is placed into the SONET payload.
5. The framer adds the FCS and SONET/SDH overhead.
6. The framer sends the data to the SFP optics for transmission onto the network.

1-Port OC-192c/STM-64 POS XFP SPA Architecture

Figure 3 identifies the primary hardware devices that are part of the POS SPA architecture. The figure shows a single optics transceiver. The 1-Port OC-192c/STM-64 POS XFP SPA supports XFP optics.

Figure 3 1-Port OC-192c/STM-64 POS XFP SPA Architecture



In POS mode, every incoming and outgoing packet on the OC-192 POS SPAs goes through the SONET/SDH framer and SPI4.2 interface.

Path of a Packet in the Ingress Direction

The following steps describe the path of an ingress packet through the 1-Port OC-192c/STM-64 POS XFP SPA:

1. The framer receives SONET/SDH streams from the XFP optics, extracts clocking and data, and processes the section, line, and path overhead.
2. The framer extracts the POS frame payload and verifies the frame size and frame check sequence (FCS).
3. The framer passes valid frames to the System Packet Level Interface 4.2 (SPI4.2) interface on the SPA.
4. The SPI4.2 interface transfers frames to the host through the SPI4.2 bus for further processing and switching.

Path of a Packet in the Egress Direction

The following steps describe the path of an egress packet through the 1-Port OC-192c/STM-64 POS XFP SPA:

1. The host sends packets to the SPA using the SPI4.2 bus.
2. The SPA stores the data in the appropriate channel's first-in first-out (FIFO) queue.
3. The SPA passes the packet to the framer.
4. The framer accepts the data and stores it in the appropriate channel queue.
5. The framer adds the FCS and SONET/SDH overhead.
6. The framer sends the data to the XFP optics for transmission onto the network.

Displaying the SPA Hardware Type

To verify information about the SPA hardware that is installed in your Cisco ASR 1000 Series Routers, you can use the **show interfaces** command or the **show controllers** command. There are several other commands on the Cisco ASR 1000 Series Routers that also provide SPA hardware information.

[Table 12-2](#) shows the hardware description that appears in the **show** command output for each POS SPA that is supported on the Cisco ASR 1000 Series Routers.

Table 12-2 SPA Hardware Descriptions in show Commands

SPA	Description in show interfaces command
2-Port OC-3c/STM-1 POS SPA	Hardware is Packet over Sonet
4-Port OC-3c/STM-1 POS SPA	Hardware is Packet over Sonet
8-Port OC-3c/STM-1 POS SPA	Hardware is Packet over Sonet
1-Port OC-12c/STM-4 POS SPA	Hardware is Packet over Sonet
2-Port OC-12c/STM-4 POS SPA	Hardware is Packet over Sonet
4-Port OC-12c/STM-4 POS SPA	Hardware is Packet over Sonet
8-Port OC-12c/STM-4 POS SPA	Hardware is Packet over Sonet
1-Port OC-48c/STM-16 POS SPA	Hardware is Packet over Sonet
2-Port OC-48c/STM-16 POS/RPR SPA	Hardware is Packet over Sonet
4-Port OC-48c/STM-16 POS/RPR SPA	Hardware is Packet over Sonet
1-Port OC-192 POS-XFP SPA	SPA-OC192POS-XFP

Example of the show interfaces Command

The following example shows output from the **show interfaces pos** command on a Cisco ASR 1000 Series Router with a 1-Port OC-192c/STM-64 POS XFP SPA installed in slot 1:

```
Router# show interfaces POS1/0/0
POS1/0/0 is up, line protocol is up
  Hardware is SPA-OC192POS-XFP
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
```

```

Keepalive set (10 sec)
Scramble disabled
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of 'show interface' counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  138525 packets input, 3324600 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    1 runts, 6 giants, 0 throttles
    0 parity
  3951 input errors, 3944 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  138522 packets output, 3324528 bytes, 0 underruns
    0 output errors, 0 applique, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions

```

Example of the show controllers Command

The following example shows output from the **show controllers pos** command on Cisco ASR 1000 Series Routers with a 4-Port OC-3c/STM-1 POS SPA installed in slot 1:

```

Router# show controllers pos 1/0/1
POS5/0/1
SECTION
  LOF = 0 LOS = 0 BIP(B1) = 0
LINE
  AIS = 0 RDI = 0 FEBE = 0 BIP(B2) = 0
PATH
  AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 0
  LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

BER thresholds: SF = 10e-3, SD = 10e-6
TCA thresholds: B1 = 10e-6, B2 = 10e-6, B3 = 10e-6
APS
  COAPS = 0 PSBF = 0
  State: PSBF_state = False
  Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
  S1S0 = 00, C2 = CF
CLOCK RECOVERY
  RDOOL = 0
  State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
  Remote hostname : c7600-1
  Remote interface: POS7/1/3
  Remote IP addr  : 10.5.5.4
  Remote Rx(K1/K2): 00/00 Tx(K1/K2): 00/00

BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Clock source: internal

```



CHAPTER 13

Configuring the POS SPAs

This chapter provides information about configuring the Packet over SONET (POS) shared port adapters (SPAs) on the Cisco ASR 1000 Series Aggregation Services Routers. This chapter includes the following sections:

- [Configuration Tasks, page 13-1](#)
- [Verifying the Interface Configuration, page 13-11](#)
- [Configuration Examples, page 13-12](#)

For information about managing your system images and configuration files, refer to the *Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2 and *Cisco IOS Configuration Fundamentals Command Reference* publications that correspond to your Cisco IOS XE software release.

Configuration Tasks

This section describes how to configure POS SPAs and includes information about verifying the configuration.

It includes the following topics:

- [Specifying the Interface Address on a SPA, page 13-1](#)
- [Modifying the Interface MTU Size, page 13-2](#)
- [Modifying the POS Framing, page 13-3](#)
- [Modifying the Keepalive Interval, page 13-5](#)
- [Modifying the CRC Size, page 13-6](#)
- [Modifying the Clock Source, page 13-6](#)
- [Modifying SONET Payload Scrambling, page 13-8](#)
- [Configuring the Encapsulation Type, page 13-8](#)
- [Configuring POS Alarm Trigger Delays, page 13-9](#)

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 2:

```
Router(config)# interface serial 2/0/0
```

This command shows a serial SPA as a representative example, however the same *slot/subslot/port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Modifying the Interface MTU Size

The Cisco IOS software supports three different types of configurable maximum transmission unit (MTU) options at different levels of the protocol stack:

- Interface MTU—Checked by the SPA on traffic coming in from the network. Different interface types support different interface MTU sizes and defaults. The interface MTU defines the maximum packet size allowable (in bytes) for an interface before drops occur. If the frame is smaller than the interface MTU size, but is not smaller than three bytes of payload size, then the frame continues to process.
- IP MTU—Can be configured on a subinterface and is used by the Cisco IOS software to determine whether fragmentation of a packet takes place. If an IP packet exceeds the IP MTU size, then the packet is fragmented.
- Tag or Multiprotocol Label Switching (MPLS) MTU—Can be configured on a subinterface and allows up to six different labels, or tag headers, to be attached to a packet. The maximum number of labels is dependent on your Cisco IOS software release.

Different encapsulation methods and the number of MPLS MTU labels add additional overhead to a packet. For example, for an Ethernet packet, SNAP encapsulation adds an 8-byte header, dot1q encapsulation adds a 2-byte header, and each MPLS label adds a 4-byte header (n labels \times 4 bytes).

Interface MTU Configuration Guidelines

When configuring the interface MTU size on the POS SPAs, consider the following guidelines:

- If you are also using MPLS, be sure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU.
- If you change the interface MTU size, the giant counter increments when the interface receives a packet that exceeds the MTU size that you configured, plus an additional 24 bytes for overhead, and an additional 2 or 4 bytes for the configured cyclic redundancy check (CRC).

For example, with a maximum MTU size of 9216 bytes, the giant counter increments:

- For a 16-bit CRC (or FCS), when receiving packets larger than 9306 bytes ($9216 + 24 + 2$).
- For a 32-bit CRC, when receiving packets larger than 9308 bytes ($9216 + 24 + 4$).

- The Frame Relay Local Management Interface (LMI) protocol requires that all permanent virtual circuit (PVC) status reports fit into a single packet. Using the default MTU of 4470 bytes, this limits the number of data-link connection identifiers (DLCIs) to 890. The following formula demonstrates how to determine the maximum DLCIs for a configured interface MTU:
 - Maximum DLCIs = (MTU bytes – 20)/(5 bytes per DLCI)
 - Maximum DLCIs for the default MTU = (4470 – 20)/5 = 890 DLCIs per interface

Interface MTU Configuration Task

To modify the MTU size on an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# mtu <i>bytes</i>	Configures the maximum packet size for an interface, where: <ul style="list-style-type: none"> • <i>bytes</i>—Specifies the maximum number of bytes for a packet. The default is 4470 bytes.

To return to the default MTU size, use the **no** form of the command.

Verifying the MTU Size

To verify the MTU size for an interface, use the **show interfaces pos** privileged EXEC command and observe the value shown in the “MTU” field.

The following example shows an MTU size of 4470 bytes for interface port 0 (the first port) on the SPA installed in subslot 1 of the SIP that is located in slot 2 of the Cisco ASR 1000 Series Routers:

```
Router# show interfaces pos 2/1/0
POS2/1/0 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.1.1/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255.
```

Modifying the POS Framing

POS framing can be specified as SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy). SONET and SDH are a set of related standards for synchronous data transmission over fiber-optic networks. SONET is the United States version of the standard published by the American National Standards Institute (ANSI). SDH is the international version of the standard published by the International Telecommunications Union (ITU).

To modify the POS framing, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# pos framing {sonet sdh}	<p>Specifies the POS framing type, where:</p> <ul style="list-style-type: none"> sonet—Enables Synchronous Optical Network framing for optical carrier (OC) rates. This is the default. sdh—Enables Synchronous Digital Hierarchy framing for synchronous transfer mode (STM) rates. <p>The POS framing type must be configured to be the same on both ends of the POS link.</p>

To return to the default, use the **no** form of the command.

Verifying the POS Framing

To verify the POS framing, use the **show controllers pos** privileged EXEC command and observe the value shown in the “Framing” field. The following example shows that POS framing mode is set to SONET for the first interface (0) on the POS SPA installed in subslot 2 of a SIP installed in chassis slot 3:

```
Router# show controllers pos 3/2/0
POS3/2/0
SECTION
LOF = 0 LOS = 0 BIP(B1) = 0
LINE
AIS = 0 RDI = 0 FEBE = 0 BIP(B2) = 0
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 0
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0
Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA
```

Framing: SONET

```
APS
COAPS = 0 PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = CF
Remote aps status (none); Reflected local aps status (none)
CLOCK RECOVERY
RDOOL = 0
State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
Remote hostname : sip-sw-7600-2
Remote interface: POS3/2/1
Remote IP addr : 0.0.0.0
Remote Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6
Clock source: internal
```


Modifying the Keepalive Interval

When the keepalive feature is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. The keepalive interval *must* be configured to be the same on both ends of the POS link.

To modify the keepalive interval, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# keepalive [<i>period</i> [<i>retries</i>]]	Specifies the frequency at which the Cisco IOS software sends messages to the other end of the link, to ensure that a network interface is alive, where: <ul style="list-style-type: none"> <i>period</i>—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds. <i>retries</i>—Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. The default is 5 retries.

To disable keepalive packets, use the **no** form of this command.



Note

If keepalives are enabled and you are trying to configure line loopback on a POS interface, the keepalive protocol will fail and periodically reset the interface based on the keepalive timeout and cause Layer 1 errors on the other end of the link that is trying to do the loopbacks.

You can avoid this by using the **no keepalive** command on the POS interface that is configured for line loopback. The side that is not in line loopback detects that its keepalive is being looped back and functions properly. An interface configured for internal loopback also functions properly with keepalives enabled.

Verifying the Keepalive Interval

To verify the keepalive interval, use the **show interfaces pos** privileged EXEC command and observe the value shown in the “Keepalive” field.

The following example shows that keepalive is enabled for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in chassis slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces pos 2/0/0
  POS2/0/0 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.1.1.2
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255,
  rxload 1/255
  Keepalive set (10 sec)
```

Modifying the CRC Size

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The CRC size indicates the length in bits of the FCS.

The CRC size *must* be configured to be the same on both ends of the POS link.

To modify the CRC size, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# crc [16 32]	(As Required) Specifies the length of the cyclic redundancy check (CRC), where: <ul style="list-style-type: none">• 16—Specifies a 16-bit length CRC. This is the default.• 32—Specifies a 32-bit length CRC. The CRC size must be configured to be the same on both ends of the POS link.

To return to the default CRC size, use the **no** form of the command.

Verifying the CRC Size

To verify the CRC size, use the **show interfaces pos** privileged EXEC command and observe the value shown in the “CRC” field.

The following example shows that the CRC size is 16 for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in chassis slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.1.1.2.1
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
```

Modifying the Clock Source

A clock source of **internal** specifies that the interface clocks its transmitted data from its internal clock. A clock source of **line** specifies that the interface clocks its transmitted data from a clock recovered from the line’s receive data stream.

For information about the recommended clock source settings for POS router interfaces, refer to *Configuring Clock Settings on POS Router Interfaces* at the following URL:

http://www.cisco.com/en/US/tech/tk482/tk607/technologies_tech_note09186a0080094bb9.shtml

To modify the clock source, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# clock source {line internal}	Specifies the clock source for the POS link, where: <ul style="list-style-type: none"> line—The link uses the recovered clock from the line. This is the default. internal—The link uses the internal clock source.

To return to the default clock source, use the **no** form of this command.

Verifying the Clock Source

To verify the clock source, use the **show controllers pos** privileged EXEC command and observe the value shown in the “Clock source” field.

The following example shows that the clock source is internal for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Cisco ASR 1000 Series Routers:

```
Router# show controllers pos 2/0/0
POS2/0/0
SECTION
LOF = 0 LOS = 1 BIP(B1) = 7
LINE
AIS = 0 RDI = 1 FEBE = 20 BIP(B2) = 9
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 5
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None

Alarm reporting enabled for: SF SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PLOP PRDI PUNEQ
B3-TCA RDOOL

APS

COAPS = 2 PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 02, C2 = CF
CLOCK RECOVERY
RDOOL = 0
State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
Remote hostname : RouterTester. Port 102/1
Remote interface:
Remote IP addr :
Remote Rx(K1/K2): / Tx(K1/K2): /

BER thresholds: SF = 10e-5 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Clock source: internal
```

Modifying SONET Payload Scrambling

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density.

The default configuration is SONET payload scrambling disabled.

SONET payload scrambling *must* be configured to be the same on both ends of the POS link.

To modify SONET payload scrambling, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# pos scramble-atm	Enables SONET payload scrambling.

To disable SONET payload scrambling, use the **no** form of this command.

Verifying SONET Payload Scrambling

To verify SONET payload scrambling, use the **show interfaces pos** privileged EXEC command and observe the value shown in the “Scramble” field.

The following example shows that SONET payload scrambling is disabled for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Cisco ASR 1000 Series Routers:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.0.0.1/24
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
```

Configuring the Encapsulation Type

By default, the POS interfaces support High-Level Data Link Control (HDLC) encapsulation. The encapsulation method can be specified as HDLC, Point-to-Point Protocol (PPP), or Frame Relay. The encapsulation type *must* be configured to be the same on both ends of the POS link.

To modify the encapsulation method, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# encapsulation encapsulation-type	Specifies the encapsulation method used by the interface, where: <ul style="list-style-type: none"><i>encapsulation-type</i>—Can be HDLC, PPP, or Frame Relay. The default is HDLC.

Verifying the Encapsulation Type

To verify the encapsulation type, use the **show interfaces pos** privileged EXEC command and observe the value shown in the “Encapsulation” field.

The following example shows the encapsulation type is HDLC for port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show interfaces pos 2/0/0
Hardware is Packet over Sonet
Internet address is 10.0.0.1/24
MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive not set
Scramble disabled
```

Configuring POS Alarm Trigger Delays

A trigger is an alarm that, when activated, causes the line protocol to go down. The POS alarm trigger delay helps to ensure uptime of a POS interface by preventing intermittent problems from disabling the line protocol. The POS alarm trigger delay feature delays the setting of the line protocol to down when trigger alarms are received. If the trigger alarm was sent because of an intermittent problem, the POS alarm trigger delay can prevent the line protocol from going down when the line protocol is functional.

Path-Level Triggers

You can issue the **pos delay triggers path** command to configure various path alarms as triggers and to specify an activation delay between 0 and 10000 milliseconds. The default delay value is 100 milliseconds. The following path alarms are not triggers by default. You can configure these path alarms as triggers and also specify a delay:

- Path alarm indication signal (PAIS)
- Path remote defect indication (PRDI)
- Path loss of pointer (PLOP)

The **pos delay triggers path** command can also bring down the line protocol when the higher of the B2 and B3 error rates is compared with the signal failure (SF) threshold. If the SF threshold is crossed, the line protocol of the interface goes down.

To configure POS path-level triggers, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# pos delay triggers path <i>ms</i>	Specifies that path-level alarms should act as triggers and specifies a delay for setting the line protocol to down when a path-level trigger alarm is received, where: <ul style="list-style-type: none"> • <i>ms</i>—Specifies the delay in milliseconds. The default delay is 100 milliseconds.

To disable path-level triggers, use the **no** form of this command.

Verifying POS Alarm Trigger Delays

To verify POS alarm trigger delays, use the **show controllers pos** privileged EXEC command and observe the values shown in the “Line alarm trigger delay” and “Path alarm trigger delay” fields.

The following example shows the POS alarm trigger delays for interface port 0 on the POS SPA installed in the SIP that is located in slot 2 of the Cisco ASR 1000 Series Router:

```
Router# show controllers pos 2/0/0 details
POS2/0/0
SECTION
LOF = 0 LOS = 1 BIP(B1) = 5
LINE
AIS = 0 RDI = 1 FEBE = 5790 BIP(B2) = 945
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 5
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 1 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Line alarm trigger delay = 100 ms
Path alarm trigger delay = 100 ms
```

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For more information about managing your system image and configuration files, refer to the [Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2](#) and [Cisco IOS Configuration Fundamentals Command Reference](#) publications that correspond to your Cisco IOS XE software release.

Shutting Down and Restarting an Interface on a SPA

You can shut down and restart any of the interface ports on a SPA independently of each other. Shutting down an interface stops traffic and then enters the interface into an “administratively down” state.

If you are preparing for an OIR of a SPA, it is not necessary to independently shut down each of the interfaces prior to deactivation of the SPA. You do not need to independently restart any interfaces on a SPA after OIR of a SPA or SIP. For more information about performing an OIR for a SPA, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

To shut down an interface on a SPA, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# shutdown	Disables an interface.

To restart an interface on a SPA, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# no shutdown	Restarts a disabled interface.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Routers configuration settings, you can use the **show interfaces pos** and **show controllers pos** commands to get detailed information on a per-port basis for your POS SPAs.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the POS SPAs, use the **show interfaces pos** command. For an example of the command output for a POS SPA at location 0/3/0, see the following:

```
router#show interfaces POS 0/3/0
POS0/3/0 is administratively down, line protocol is down
  Hardware is Packet over Sonet
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Scramble disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
      0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

Monitoring Per-Port Interface Statistics

To find detailed alarm and error information on a per-port basis for the POS SPAs, use the **show controllers pos** command. For an example of the command output for a POS SPA at location 0/3/0, see the following:

```
router#show controllers pos
POS0/3/0
SECTION
  LOF = 0          LOS    = 0          BIP(B1) = 0
LINE
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
  PLM = 0          UNEQ   = 0          TIM    = 0          TIU    = 0
```

```

LOP = 0          NEWPTR = 0          PSE = 0          NSE = 0

Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Framing: SONET
APS

COAPS = 0          PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = 00
Remote aps status (none); Reflected local aps status (none)
--More--          CLOCK RECOVERY
RDOOL = 0
State: RDOOL_state = False
PATH TRACE BUFFER: UNSTABLE
Remote hostname :
Remote interface:
Remote IP addr  :
Remote Rx(K1/K2): / Tx(K1/K2): /

BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Clock source: line

```

Configuration Examples

This section includes the following examples for configuring a POS SPA installed in a Cisco ASR 1000 Series Router:

- [Basic Interface Configuration Example, page 13-13](#)
- [MTU Configuration Example, page 13-13](#)
- [POS Framing Configuration Example, page 13-14](#)
- [Keepalive Configuration Example, page 13-14](#)
- [CRC Configuration Example, page 13-14](#)
- [Clock Source Configuration Example, page 13-15](#)
- [SONET Payload Scrambling Configuration Example, page 13-15](#)
- [Encapsulation Configuration Example, page 13-15](#)
- [POS Alarm Trigger Delays Configuration Example, page 13-16](#)

Basic Interface Configuration Example

The following example shows how to enter global configuration mode to specify the interface that you want to configure, configure an IP address for the interface, enable the interface, and save the configuration. This example configures interface port 0 (the first port) of the SPA located in subslot 0 of the SIP that is installed in slot 2 of the Cisco ASR 1000 Series Router:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/0/0
!
! Configure an IP address
!
Router(config-if)# ip address 192.168.50.1 192.255.255.0
!
! Enable the interface
!
Router(config-if)# no shutdown
!
! Save the configuration to NVRAM
!
Router(config-if)# exit
Router# copy running-config startup-config
```

MTU Configuration Example

The following example sets the MTU to 4470 bytes on interface port 1 (the second port) of the SPA located in the bottom subslot (1) of the SIP that is installed in slot 2 of the Cisco ASR 1000 Series Router:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure MTU
!
Router(config-if)# mtu 4470
```

POS Framing Configuration Example

The following example shows how to change from the default POS framing of SONET to SDH:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
! (The default pos framing is sonet)
!
!Modify the framing type
!
Router(config-if)# pos framing sdh
```

Keepalive Configuration Example

The following example shows how to change from the default keepalive period of 10 seconds to 20 seconds:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure keepalive 20
!
Router(config-if)# keepalive 20
```

CRC Configuration Example

The following example shows how to change the CRC size from 32 bits to the default 16 bits for POS SPAs:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure crc 16
!
Router(config-if)# crc 16
```

Clock Source Configuration Example

The following example shows how to change from the default clock source of internal to line:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure the clock source
!
Router(config-if)# clock source line
```

SONET Payload Scrambling Configuration Example

The following example shows how to change from a default SONET payload scrambling of disabled to enabled:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure the SONET payload scrambling
!
Router(config-if)# pos scramble-atm
```

Encapsulation Configuration Example

The following example shows how to change from the default encapsulation method of HDLC to PPP:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure ppp
!
Router(config-if)# encapsulation ppp
```

POS Alarm Trigger Delays Configuration Example

The following example shows how to change POS line-level and path-level alarm trigger delays from the default of 100 milliseconds to 200 milliseconds:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
Router(config-if)# pos delay triggers line 200
Router(config-if)# pos delay triggers path 200
```



PART 5

Serial Shared Port Adapters



CHAPTER 14

Overview of the Serial SPAs

This chapter provides an overview of the release history, supported features, restrictions, and Management Information Base (MIB) support for the serial SPAs on the Cisco ASR 1000 Series Aggregation Services Routers.

This chapter includes the following sections:

- [Release History, page 14-1](#)
- [Supported Features, page 14-2](#)
- [Restrictions, page 14-4](#)
- [Supported MIBs, page 14-5](#)
- [Displaying the SPA Hardware Type, page 14-7](#)

Release History

Release	Modification
Cisco IOS XE Release 2.6	Support for the following SPA was introduced on the Cisco ASR 1000 Series SIP: <ul style="list-style-type: none">• 1-Port Channelized OC-12/STM-4 SPA
Cisco IOS XE Release 2.2	Support for the following SPA was introduced on the Cisco ASR 1000 Series SIP: <ul style="list-style-type: none">• 1-Port Channelized OC-3/STM-1 SPA
Cisco IOS XE Release 2.1	Support for the following SPAs was introduced on the Cisco ASR 1000 Series SIP: <ul style="list-style-type: none">• 2-Port Clear Channel T3/E3 SPA (SPA-2XT3/E3)• 4-Port Clear Channel T3/E3 SPA (SPA-4XT3/E3)• 8-Port Channelized T1/E1 SPA (SPA-8XCHT1/E1)• 2-Port Channelized T3 SPA (SPA-2XCT3/DS0)• 4-Port Channelized T3 SPA (SPA-4XCT3/DS0)• 4-Port Serial SPA (SPA-4TX-Serial)

Supported Features

**Note**

There are some variations in support by SPA model and software release. These differences are identified here, in the [“Restrictions” section on page 14-4](#), and in the corresponding configuration chapter for that SPA.

The following is a list of some of the significant software features supported by the serial SPAs on the Cisco ASR 1000 Series Routers:

- Software selectable between T1, E1, T3, or E3 framing on each card (ports are configured as all T1, E1, T3, or E3). Applies to the 2-Port and 4-Port Clear Channel T3/E3 SPA and 8-Port Channelized T1/E1 SPA.
- Layer 2 encapsulation support:
 - Point-to-Point Protocol (PPP)
 - High-level Data Link Control (HDLC)
 - Frame Relay
- Internal or network clock (selectable per port).
- Online insertion and removal (OIR).
- Hot Standby Router Protocol (HSRP).
- Alarm reporting: 24-hour history maintained, 15-minute intervals on all errors.
- 16- and 32-bit cyclic redundancy checks (CRC) supported (16-bit default).
- Local and remote loopback.
- Bit error rate testing (BERT) pattern generation and detection per port.
- Programmable BERT patterns enhancements.

**Note**

The programmable BERT patterns enhancements are not supported on the 2- and 4-Port T3/E3 SPAs or the 8-Port Channelized T1/E1 SPA.

- Dynamic provisioning—Allows for the addition of new customer circuits within a channelized interface without affecting other customers.
- Field-programmable device (FPD) upgrades.
- End-to-end FRF.12 fragmentation support (Quantum Flow Processor [QFP] based).
- QFP-based Multilink PPP (MLPPP) and Link Fragmentation and Interleaving (LFI).
- Support for MLPPP across all SPAs.
- Support for MLPPP using any combination of E1, T1, and NxDS0 member links.
- Compressed Real-Time Protocol (cRTP)—8-Port Channelized T1/E1 SPA and 2-Port and 4-Port Channelized T3 SPAs only.
- T1 features
 - All ports can be fully channelized down to DS0.
 - Data rates in multiples of 56 Kbps or 64 Kbps per channel.
 - Maximum 1.536 Mbps for each T1 port.

- D4 Superframe (SF) and Extended Superframe (ESF) support for each T1 port.
- ANSI T1.403 and AT&T TR54016 CI FDL support.
- Internal and receiver recovered clocking modes.
- Short haul and long haul channel service unit (CSU) support.
- Bipolar eight zero substitution (B8ZS) and alternate mark inversion (AMI) line encoding.



Note B8ZS and AMI line encoding are not configurable for TW on the 2-Port and 4-Port Channelized T3 SPA.

- E1 features



Note E1 is not supported on the 1-Port Channelized OC-12/STM-4 SPA in Cisco IOS XE Release 2.6.

- Maximum 1.984 Mbps for each E1 port in framed mode and a 2.048 Mbps in unframed E1 mode.
- All ports can be fully channelized down to DS0.
- Compliant with ITU G7.03, G.704, ETSI and ETS300156.
- Internal and receiver recovered clocking modes.
- Hi-density bipolar with three zones (HDB3) and AMI line encoding.

- E3 features



Note E3 is not supported on the 1-Port Channelized OC-12/STM-4 SPA in Cisco IOS XE Release 2.6.

- Full duplex connectivity at E3 rate (34.368 MHz).
 - Supports ITU-T G.751 or G.832 framing (software selectable).
 - HD3B line coding.
 - Compliant with E3 pulse mask.
 - Line build-out: configured for up to 450 feet (135 m) of type 728A or equivalent coaxial cable.
 - Loopback modes: data terminal equipment (DTE), local, dual, and network.
 - E3 alarm/event detection (once per second polling):
 - Alarm indication signal (AIS)
 - Loss of frame (LOF)
 - Remote alarm indication (RAI)
 - Subrate and scrambling features for these data service unit (DSU) vendors:
 - Digital Link
 - ADC Kentrox
- T3 features
 - Binary 3-zero substitution (B3ZS) line coding.
 - Compliant with DS3 pulse mask per ANSI T1.102-1993.

- DS3 far-end alarm and control (FEAC) channel support.
- Full duplex connectivity at DS3 rate (44.736 MHz).
- 672 DS0s per T3.
- Loopback modes: DTE, local, remote, dual, and network.
- C-bit or M23 framing (software selectable).
- Line build-out: configured for up to 450 feet (135 m) of type 734A or equivalent coaxial cable.
- DS3 alarm/event detection (once per second polling):
 - AIS
 - Out of frame (OOF)
 - Far-end receive failure (FERF)
- Generation and termination of DS3 Maintenance Data Link (MDL) in C-bit framing.
- Full FDL support and FDL performance monitoring.



Note FDL support is not supported on the 2-Port and 4-Port Clear Channel T3/E3 SPAs. It applies to the 2-Port and 4-Port Channelized T3 SPAs, the 1-Port Channelized OC-3/STM-1 SPA, and the 1-Port Channelized OC-12/STM-4 SPA.

- Subrate and scrambling features for these DSU vendors:
 - Cisco
 - Digital Link
 - ADC Kentrox
 - Adtran
 - Verilink
 - Larscom

Restrictions

Consider the following restrictions when configuring the serial SPAs on the Cisco ASR 1000 Series Routers:



Note

For additional information, see also the configuration chapters for the corresponding SPA model. For other SIP-specific features and restrictions see also [Chapter 3, “Overview of the SIP”](#).

- FRF.16—Multilink Frame Relay (MLFR) is not supported.
- MLPPP is only supported on serial PPP interfaces. MLPPP is not supported over Frame Relay, ATM, or PPPoE interfaces.
- Virtual-template interfaces are not supported with MLPPP.
- On a 2-Port and 4-Port Channelized T3 SPA, when one of the T3 ports is configured as a DS3 clear channel interface and the other T3s are configured with a large number (greater than or equal to 400) of low bandwidth channels (N×DS0, N=1, 2, 3, or 4), the DS3 clear channel interface is not able to

run at 100 percent DS3 line rate when those low bandwidth channels are idle (that is, not transmitting or receiving packets). This issue does not occur if those low bandwidth channels are not idle.

- The maximum number of channels supported on the channelized SPAs are:
 - 1023 channels per SPA—On a 2-Port and 4-Port Channelized T3 SPA or 1-Port Channelized OC-3/STM-1 SPA.
 - 2000 NxDS0 per SPA—On a 1-Port Channelized OC-12/STM-4 SPA.
- On a 2-Port and 4-Port Channelized T3 SPA or 1-Port Channelized OC-3/STM-1 SPA, the maximum number of FIFO buffers is 4096. The FIFO buffers are shared among the interfaces; how they are shared is determined by speed. If all the FIFO buffers have been assigned to existing interfaces, a new interface cannot be created, and the “%Insufficient FIFOs to create channel group” error message is seen.

To find the number of available FIFO buffers, use the **show controller t3** command:

```
Router# show controller t3 1/0/0

T3 1/0/0 is up.
Hardware is SPA-4XCT3/DS0
IO FPGA version: 2.6, HDLC Framers version: 0
T3/T1 Framers(1) version: 2, T3/T1 Framers(2) version: 2
SUBRATE FPGA version: 1.4
HDLC controller available FIFO buffers 3112
```

FIFO allocation information is provided in [Table 14-1](#).

Table 14-1 *FIFO Allocation*

Number of Time Slots	Number of FIFO Buffers
1–6 DS0	4
7–8 DS0	6
9 DS0	6
10–12 DS0	8
13–23 DS0	12
1–6 E1 TS	4
7–9 E1 TS	6
11–16 E1 TS	8
17–31 E1 TS	16
T1	12
E1	16
DS3	336

Supported MIBs

The following MIBs are supported for the serial SPAs on the Cisco ASR 1000 Series Routers.

Serial SPAs

- CISCO-ENTITY-ALARM-MIB

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- ENTITY-MIB
- IF-MIB
- RMON-MIB
- MPLS-LDP-STD-MIB
- MPLS-LSR-STD-MIB
- MPLS-TE-MIB
- MPLS-VPN-MIB

2-Port and 4-Port Clear Channel T3/E3 SPAs

- DS3-MIB

8-Port Channelized T1/E1 SPA

- DS1-MIB

2-Port and 4-Port Channelized T3 SPA

- DS1-MIB
- DS3-MIB
- CISCO-FRAME-RELAY-MIB
- IANAifType-MIB -- not in MIB doc
- RFC1381-MIB -- not in MIB doc

1-Port Channelized STM-1/OC-3 SPA

- DS1-MIB
- DS3-MIB
- SONET-MIB

1-Port Channelized OC-12/STM-4 SPA

- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-SONET-MIB
- DS1-MIB
- DS-3-MIB
- ENTITY-MIB
- ENTITY-SENSOR-MIB

- IF-MIB
- SONET-MIB

To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Displaying the SPA Hardware Type

To verify the SPA hardware type that is installed in your Cisco ASR 1000 Series Routers, you can use the **show platform** command or the **show interface** command (once the interface has been configured). There are several other commands on the Cisco ASR 1000 Series Routers that also provide SPA hardware information.

Table 14-2 shows the hardware description that appears in the **show** command output for each type of SPA that is supported on the Cisco ASR 1000 Series Routers.

Table 14-2 SPA Hardware Descriptions in show Commands

SPA	Description in show interfaces and show controllers Commands
2-Port Clear Channel T3/E3 SPA	“Hardware is SPA-4XT3/E3”
4-Port Clear Channel T3/E3 SPA	“Hardware is SPA-2XT3/E3”
8-Port Channelized T1/E1 SPA	“Hardware is SPA-8XCHT1/E1”
2-Port Channelized T3 SPA	“Hardware is SPA-2XCT3/DS0”
4-Port Channelized T3 SPA	“Hardware is SPA-4XCT3/DS0”
4-Port Serial Interface SPA	“Hardware is SPA-4XT-SERIAL”
1-Port Channelized OC-3/STM-1 SPA	“Hardware is SPA-1XCHSTM1/OC3”
1-Port Channelized OC-12/STM-4 SPA	“Hardware is SPA-1XCHOC12/DS0”

Examples of the show interfaces Command

The following example shows output from the **show interfaces serial** command on a Cisco ASR 1000 Series Router with a 4-Port Clear Channel T3/E3 SPA installed in slot 2:

```
router#: show interfaces serial 2/0/0
Serial2/0/0 is up, line protocol is up
Hardware is SPA-4XT3/E3[3/0]
```

```

MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
reliability 248/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Last input 00:00:06, output 00:00:07, output hang never
Last clearing of 'show interface' counters 00:00:01
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 applique, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions

```

The following example shows output from the **show interfaces serial** command on a Cisco ASR 1000 Series Router with an 8-Port Channelized T1/E1 SPA installed in slot 0:

```

router#show interfaces serial 0/3/0:0
Serial0/3/0:0 is up, line protocol is up
  Hardware is SPA-8XCHT1/E1
  Internet address is 79.1.1.2/16
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
    reliability 255/255, txload 240/255, rxload 224/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 3d21h, output 3d21h, output hang never
  Last clearing of 'show interface' counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2998712
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1744000 bits/sec, 644 packets/sec
  5 minute output rate 1874000 bits/sec, 690 packets/sec
    180817311 packets input, 61438815508 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
    180845200 packets output, 61438125092 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags 2

```

Examples of the show controllers Command

The following example shows output from the **show controllers serial** command on a Cisco ASR 1000 Series Router with a 2-Port Clear Channel T3/E3 SPA installed in slot 2:

```

Router# show controllers serial 2/2/0
Serial2/2/0 - (SPA-2XT3/E3) is up
  Current mode is T3

  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10 feet
  rx FEBE since last clear counter 0, since reset 0
  Data in current interval (820 seconds elapsed):

```

```

0 Line Code Violations, 0 P-bit Coding Violation
0 C-bit Coding Violation
0 P-bit Err Secs, 0 P-bit Sev Err Secs
0 Sev Err Framing Secs, 0 Unavailable Secs
0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
0 Severely Errored Line Secs
0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
0 CP-bit Far-end Unavailable Secs
0 Near-end path failures, 0 Far-end path failures
0 Far-end code violations, 0 FERF Defect Secs
0 AIS Defect Secs, 0 LOS Defect Secs
Data in Interval 1:
0 Line Code Violations, 0 P-bit Coding Violation
0 C-bit Coding Violation
0 P-bit Err Secs, 0 P-bit Sev Err Secs
0 Sev Err Framing Secs, 0 Unavailable Secs

```

The following example shows output from the **show controllers** command on a Cisco ASR 1000 Series Router with an 8-Port Channelized T1/E1 SPA installed in slot 0:

```

Router# show controllers e1 0/3/0 brief
E1 0/3/0 is up.
  Applique type is SPA-8XCHT1/E1
  No alarms detected.
  alarm-trigger is not set
  Framing is crc4, Line Code is HDB3, Clock Source is Line.
  Data in current interval (571 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
    0 Line Code Violations, 0 Path Code Violations,
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

```

The following example shows output from the **show controllers** command on a Cisco ASR 1000 Series Router with a 4-Port Channelized T3 SPA installed in slot 2:

```
Router# show controllers t3
T3 2/0/0 is up.
  Hardware is SPA-2XCT3/DS0
  IO FPGA version: 2.7, HDLC Framers version: 0
  T3/T1 Framers(1) version: 2
  SUBRATE FPGA version: 1.4
  HDLC controller available FIFO buffers 4084
  Applique type is Channelized T3/T1
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Cablelength is 224
  Clock Source is Internal
  Equipment customer loopback
  Data in current interval (204 seconds elapsed):
    2 Line Code Violations, 6 P-bit Coding Violation
    0 C-bit Coding Violation, 1 P-bit Err Secs
    1 P-bit Severely Err Secs, 1 Severely Err Framing Secs
    0 Unavailable Secs, 1 Line Errored Secs
    1 C-bit Errored Secs, 1 C-bit Severely Errored Secs
    0 Severely Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
    11 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 1 Far-end path failures
    0 Far-end code violations, 10 FERF Defect Secs
    0 AIS Defect Secs, 0 LOS Defect Secs

  T1 1 is down
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  Transmitter is sending LOF Indication.
  Receiver is getting AIS.
  Framing is ESF, Clock Source is Internal
  Data in current interval (202 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    9 Unavail Secs, 0 Stuffed Secs
    5 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs

  T1 2
    Not configured.

  T1 3
    Not configured.
```

The following example shows output from the **show controllers sonet** command on a Cisco ASR 1000 Series Router with a 1-Port Channelized STM-1/OC-3 SPA installed in slot 1:

```
Router#show controllers sonet 1/0/0

SONET 1/0/0 is up.
  Hardware is SPA-1XCHSTM1/OC3
  IO FPGA version: 1.7, HDLC Framers version: 0
  T3/T1 Framers(1) version: 1
  Sonet/SDH Framers version: 0
  SUBRATE FPGA version: 1.4
  HDLC controller available FIFO buffers 3760
  Applique type is Channelized Sonet/SDH
```



```
Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
SECTION:
  LOS = 0          LOF = 0          BIP(B1) = 85

SONET/SDH Section Tables
  INTERVAL      CV      ES      SES      SEFS
  23:15-23:20    0       0       0       0
  23:00-23:15    0       0       0       0
  22:45-23:00    85      1       1       0
Total of Data in Current and Previous Intervals
  22:45-23:20    85      1       1       0

(remaining text not shown)
```




CHAPTER 15

Configuring the 8-Port Channelized T1/E1 SPA

This chapter provides information about configuring the 8-Port Channelized T1/E1 SPA on the Cisco ASR 1000 Series Routers. It includes the following sections:

- [Configuration Tasks, page 15-1](#)
- [Verifying the Interface Configuration, page 15-13](#)
- [Configuration Examples, page 15-14](#)

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications.

For more information about the commands used in this chapter, refer to the Cisco IOS Command Reference publication for your Cisco IOS software release.

For more information, see the [“Related Documentation” section on page xxvi](#).

Configuration Tasks

This section describes how to configure the 8-Port Channelized T1/E1 SPA for the Cisco ASR 1000 Series Routers and includes information about verifying the configuration.

It includes the following topics:

- [Required Configuration Tasks, page 15-1](#)
- [Specifying the Interface Address on a SPA, page 15-6](#)
- [Optional Configurations, page 15-7](#)
- [Saving the Configuration, page 15-13](#)

Required Configuration Tasks

This section lists the required configuration steps to configure the 8-Port Channelized T1/E1 SPA. Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command.

- [Setting the Card Type, page 15-2](#)
- [Enabling the Interfaces on the Controller, page 15-4](#)
- [Verifying Controller Configuration, page 15-5](#)

- [Setting the IP Address, page 15-6](#)
- [Verifying Interface Configuration, page 15-6](#)

**Note**

To better understand the address format used to specify the physical location of the SIP, SPA, and interfaces, see the [“Specifying the Interface Address on a SPA” section on page 15-6](#).

Setting the Card Type

The SPA is not functional until the card type is set. Information about the SPA is not indicated in the output of any **show** commands until the card type has been set. There is no default card type.

**Note**

Mixing of interface types is not supported. All ports on a SPA must be of the same type.

To set the card type for the 8-Port Channelized T1/E1 SPA, complete these steps:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.

	Command	Purpose
Step 2	Router(config)# card type {e1 t1} slot subslot	<p>Sets the serial mode for the SPA:</p> <ul style="list-style-type: none"> • t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default line code for T1. • e1—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 1.984 Mbps in framed mode and 2.048 Mbps in unframed E1 mode. • <i>slot subslot</i>—Specifies the location of the SPA. See the “Specifying the Interface Address on a SPA” section on page 15-6. <p>Note To change the current card type for a SPA-8XCHT1/E1, you must either:</p> <ul style="list-style-type: none"> – Remove the SPA-8XCHT1/E1 from current slot and reinsert the SPA to another slot. The slot in which the SPA-8XCHT1/E1 is being reinserted must not have previously been installed with a SPA-8XCHT1/E1. This is because the CLI configuration is stored for a slot or subslot and not for a SPA. <p>OR</p> <ul style="list-style-type: none"> – Reload the router without saving the configuration. <p>Note The SPA module must be reset after configurations are done to ensure that the SPA passes diagnostics.</p>
Step 3	Router(config)# exit	Exits configuration mode and returns to the EXEC command interpreter prompt.

Enabling the Interfaces on the Controller

To create the interfaces for the 8-Port Channelized T1/E1 SPA, complete these steps:

	Command	Purpose
Step 1	Router(config)# controller { t1 e1 } <i>slot/subslot/port</i>	<p>Selects the controller to configure and enters controller configuration mode.</p> <ul style="list-style-type: none"> t1—Specifies the T1 controller. e1—Specifies the E1 controller. <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 15-6.
Step 2	Router(config-controller)# clock source { internal line }	<p>Sets the clock source.</p> <p>Note The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal.</p> <ul style="list-style-type: none"> internal—Specifies that the internal clock source is used. line—Specifies that the network clock source is used. This is the default for T1 and E1.
Step 3	Router(config-controller)# linecode { ami b8zs hdb3 }	<p>Selects the linecode type.</p> <ul style="list-style-type: none"> ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers. <p>Note After configuring the linecode as Alternate Mark Inversion (AMI), you need to configure invert-data by executing the invert-data command from interface configuration mode. For additional details, please refer http://www.ciscosystems.com/en/US/docs/ios/12_2t/inter/command/reference/irftint.html.</p> <ul style="list-style-type: none"> b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines. hdb3—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.
Step 4	<p>For T1 controllers</p> <p>Router(config-controller)# framing {sf esf}</p> <p>For E1 controllers</p> <p>Router(config-controller)# framing {crc4 no-crc4}</p>	<p>Selects the framing type.</p> <ul style="list-style-type: none"> sf—Specifies Super Frame as the T1 frame type. esf—Specifies Extended Super Frame as the T1 frame type. This is the default for E1. crc4—Specifies CRC4 as the E1 frame type. This is the default for E1. no-crc4—Specifies no CRC4 as the E1 frame type.

	Command	Purpose
Step 5	Router(config-controller)# channel-group <i>t1 t1-number</i> { timeslots range unframed } [speed { 56 64 }]	<p>Defines the time slots that belong to each T1 or E1 circuit.</p> <ul style="list-style-type: none"> • <i>t1 t1-number</i>— Channel-group number. When configuring a T1 data line, channel-group numbers can be values from 1 to 28. When configuring an E1 data line, channel-group numbers can be values from 0 to 30. • timeslots range— One or more time slots or ranges of time slots belonging to the channel group. The first time slot is numbered 1. For a T1 controller, the time slot range is from 1 to 24. For an E1 controller, the time slot range is from 1 to 31. • unframed—Unframed mode (G.703) uses all 32 time slots for data. None of the 32 time slots are used for framing signals. • speed—(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64. <p>Note The default is 64. Speed is not mentioned in the configuration.</p> <p>Note Each channel group is presented to the system as a serial interface that can be configured individually.</p> <p>Note Once a channel group has been created with the channel-group command, the channel group cannot be changed without removing the channel group. To remove a channel group, see the “Changing a Channel Group Configuration” section on page 15-12.</p>
Step 6	Router(config)# exit	Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Controller Configuration

Use the **show controllers** command to verify the controller configuration:

```
Router(config)# show controllers e1 0/3/0 brief
E1 0/3/0 is up.
  Applique type is SPA-8XCHT1/E1
  No alarms detected.
  alarm-trigger is not set
  Framing is crc4, Line Code is HDB3, Clock Source is Line.
  Data in current interval (571 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
    0 Line Code Violations, 0 Path Code Violations,
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
```

```
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Setting the IP Address

To set the IP address for the 8-Port Channelized T1/E1 SPA, complete these steps:

	Command	Purpose
Step 1	Router(config)# interface serial slot/subslot/port:channel-group	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port:channel-group</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 15-6.
Step 2	Router(config-if)# ip address address mask	Sets the IP address and subnet mask. <ul style="list-style-type: none"> <i>address</i>—IP address. <i>mask</i>—Subnet mask.
Step 3	Router(config)# exit	Exits interface configuration mode and returns to the EXEC command interpreter prompt.

Verifying Interface Configuration

Use the **show interfaces** command to verify the interface configuration:

```
Router(config)# show interfaces
Serial6/0/1:0 is up, line protocol is up
Hardware is SPA-8XCHT1/E1
  MTU 1500 bytes, BW 1536 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  LCP Open, multilink Open
  Last input 00:00:03, output 00:00:03, output hang never
  Last clearing of "show interface" counters 5d17h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 3194905708
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    74223 packets input, 1187584 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    74227 packets output, 1187751 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    4 carrier transitions no alarm present
  Timeslot(s) Used:1-24, subrate: 64Kb/s, transmit delay is 0 flags
```

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 3:

```
Router(config)# interface serial 3/0/0
```

This command shows a serial SPA as a representative example, however the same *slot/subslot/port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

For the 8-Port Channelized T1/E1 SPA, the interface address format is *slot/subslot/port:channel-group*, where:

- *channel-group*—Specifies the logical channel group assigned to the time slots within the T1 link.

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your serial SPA.

- [Configuring Framing, page 15-8](#)
- [Configuring Encapsulation, page 15-9](#)
- [Configuring the CRC Size for T1, page 15-10](#)
- [Configuring FDL, page 15-11](#)
- [Invert Data on the T1/E1 Interface, page 15-11](#)
- [Changing a Channel Group Configuration, page 15-12](#)
- [Configuring QoS Features on Serial SPAs, page 15-12](#)

Configuring Framing

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. To configure framing, use the following commands.

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# controller {t1 e1} <i>slot/subslot/port</i>	Selects the controller to configure. <ul style="list-style-type: none"> t1—Specifies the T1 controller. e1—Specifies the E1 controller. <i>slot/subslot/port</i>—Specifies the location of the controller. See the “Specifying the Interface Address on a SPA” section on page 15-6.
For T1 controllers Router(config-controller)# framing {sf esf} For E1 controllers Router(config-controller)# framing {crc4 no-crc4}	Set the framing on the interface. <ul style="list-style-type: none"> sf—Specifies Super Frame as the T1 frame type. esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1. crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1. no-crc4—Specifies no CRC4 as the E1 frame type.

Verifying Framing Configuration

Use the **show controllers** command to verify the framing configuration:

```
Router(config)# show controllers e1 0/3/0 brief
E1 0/3/0 is up.
  Applique type is SPA-8XCHT1/E1
  No alarms detected.
  alarm-trigger is not set
  Framing is crc4, Line Code is HDB3, Clock Source is Line.
  Data in current interval (571 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
    0 Line Code Violations, 0 Path Code Violations,
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port:channel-group</i>	Selects the interface to configure. <ul style="list-style-type: none"> <i>slot/subslot/port:channel-group</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 15-6
Router(config-if)# encapsulation <i>encapsulation-type {hdlc ppp frame-relay}</i>	Sets an encapsulation type on the interface: <ul style="list-style-type: none"> hdlc—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. ppp—PPP (for serial interface). frame-relay—Frame Relay (for serial interface).

Verifying Encapsulation

Use the **show interfaces serial** command to verify encapsulation on the interface:

```
Router# show interfaces serial 2/0/0:0
Serial2/0/0:0 is down, line protocol is down
  Hardware is SPA-8XCHT1/E1
  MTU 1500 bytes, BW 1536 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, crc 32, loopback not set
  Keepalive set (10 sec)
  LCP Closed, multilink Closed
  Last input 1w0d, output 1w0d, output hang never
  Last clearing of "show interface" counters 6d23h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1152 kilobits/sec
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions alarm present
```

Timeslot(s) Used:1-24, subrate: 64Kb/s, transmit delay is 0 flags

Configuring the CRC Size for T1

All 8-Port Channelized T1/E1 SPA interfaces use a 16-bit cyclic redundancy check (CRC) by default, but also support a 32-bit CRC. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used CRC throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

To set the length of the cyclic redundancy check (CRC) on a T1 interface, use the following:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port:channel-group</i>	Selects the interface to configure. <ul style="list-style-type: none"> <i>slot/subslot/port:channel-group</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 15-6.
Router(config-if)# crc {16 32}	Selects the CRC size in bits. <ul style="list-style-type: none"> 16—16-bit CRC. This is the default 32—32-bit CRC.

Verifying the CRC Size

Use the **show interfaces serial** command to verify the CRC size set on the interface:

```
Router# show interfaces serial 6/0/0:0
Serial6/0/0:0 is up, line protocol is up
  Hardware is SPA-T1E1
  MTU 1500 bytes, BW 1536 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, crc 32, loopback not set
  Keepalive set (10 sec)
  LCP Open, multilink Open
  Last input 00:00:38, output 00:00:00, output hang never
  Last clearing of "show interface" counters 01:46:16
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    1272 packets input, 20396 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    6 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 3 abort
    1276 packets output, 20460 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions no alarm present
  Timeslot(s) Used:1-24, subrate: 64Kb/s, transmit delay is 0 flags
```

Configuring FDL

Facility Data Link (FDL) is a 4-kbps channel provided by the Extended Super Frame (ESF) T1 framing format. The FDL performs outside the payload capacity and allows you to check error statistics on terminating equipment without intrusion.

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# controller t1 <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. See the “Specifying the Interface Address on a SPA” section on page 15-6.
Router(config-controller)# fdl [ansi att both]	If the framing format was configured for esf , configures the format used for Facility Data Link (FDL). <ul style="list-style-type: none"> ansi—Specifies the ANSI T1.403 standard. att—Specifies the AT&T TR54016 standard. both—Specifies support for both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.

Verifying FDL

Use the **show controllers t1** command to verify the FDL setting:

```
Router# show controllers t1 0/2/0
T1 0/2/0 is up.
  Applique type is SPA-8XCHT1/E1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (750 seconds elapsed):
    4000 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
    0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Invert Data on the T1/E1 Interface

If the interface on the 8-Port Channelized T1/E1 SPA is used to drive a dedicated T1 line that does not have B8ZS encoding, you must invert the data stream on the connecting CSU/DSU or on the interface. Be careful not to invert data on both the CSU/DSU and the interface, as two data inversions will cancel each other out. To invert data on a T1/E1 interface, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port:channel-group</i>	Selects the serial interface and enters interface configuration mode. <ul style="list-style-type: none"> <i>channel-group</i>—The channel group number for channel-associated signaling or robbed-bit signaling.
Router(config-if)# invert data	Inverts the data stream.

Verifying Invert Data on the T1/E1 Interface

Use the show running configuration command to verify that invert data has been set:

```
Router# show running configuration
interface Serial6/0/0:0
  no ip address
  encapsulation ppp
  logging event link-status
  load-interval 30
  invert data
  no cdp enable
  ppp chap hostname group1
  ppp multilink
  multilink-group 1
```

Changing a Channel Group Configuration

To alter the configuration of an existing channel group, the channel group needs to be removed first. To remove an existing channel group, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# controller {t1 e1} <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 15-6.
Router(config-controller)# no channel-group t1 <i>t1-number</i>	Selects the channel group you want to remove. <ul style="list-style-type: none"> <i>t1 t1-number</i>—Channel-group number.
Follow the steps in the “Enabling the Interfaces on the Controller” section on page 15-4.	Creates a new channel group with the new configuration.

Configuring QoS Features on Serial SPAs

The SIPs and SPAs support many QoS features using modular QoS CLI (MQC) configuration. Since there are no serial SPA-specific QoS features, refer to your network processor documentation for QoS configuration information.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Routers configuration settings, you can use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your 8-Port Channelized T1/E1 SPA.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the 8-Port Channelized T1/E1 SPA, use the **show interfaces serial** command.

```
Router# show interfaces serial 3/0/1:0
Serial0/3/0:0 is up, line protocol is up
  Hardware is SPA-8XCHT1/E1
  Internet address is 79.1.1.2/16
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
    reliability 255/255, txload 240/255, rxload 224/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 3d21h, output 3d21h, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2998712
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1744000 bits/sec, 644 packets/sec
  5 minute output rate 1874000 bits/sec, 690 packets/sec
    180817311 packets input, 61438815508 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
    180845200 packets output, 61438125092 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions no alarm present
Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags 2
```

Configuration Examples

This section includes the following configuration examples:

- [Framing and Encapsulation Configuration Example, page 15-14](#)
- [CRC Configuration Example, page 15-14](#)
- [Facility Data Link Configuration Example, page 15-15](#)
- [Invert Data on the T1/E1 Interface Example, page 15-15](#)

Framing and Encapsulation Configuration Example

The following example sets the framing and encapsulation for the controller and interface:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the framing method
!
Router(config-controller)# framing esf
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
!
! Specify the encapsulation protocol
!
Router(config-if)# encapsulation ppp
!
! Exit interface configuratin mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

CRC Configuration Example

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
!
! Specify the CRC size
!
Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
```



```
! Exit global configuration mode
!
Router(config)# exit
```

Facility Data Link Configuration Example

The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the FDL specification
!
Router(config-controller)# fdl ansi
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Invert Data on the T1/E1 Interface Example

The following example inverts the data on the serial interface:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3:0
!
! Configure invert data
!
Router(config-if)# invert data
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```




CHAPTER 16

Configuring the 2-Port and 4-Port Channelized T3 SPAs

This chapter provides information about configuring the 2-Port and 4-Port Channelized T3 SPAs on the Cisco ASR 1000 Series Routers. It includes the following sections:

- [Configuration Tasks, page 16-1](#)
- [Verifying the Interface Configuration, page 16-16](#)
- [Configuration Examples, page 16-17](#)

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications that corresponds to your Cisco IOS software release.

For more information about the commands used in this chapter, refer to the *Cisco IOS Software Releases Command Reference* for your Cisco IOS release. For more information, see the [“Related Documentation” section on page -xxvi](#).

Configuration Tasks

This section describes how to configure the 2-Port and 4-Port Channelized T3 SPA for the Cisco ASR 1000 Series Routers and includes information about verifying the configuration.

It includes the following topics:

- [Required Configuration Tasks, page 16-2](#)
- [Specifying the Interface Address on a SPA, page 16-7](#)
- [Optional Configurations, page 16-8](#)
- [Saving the Configuration, page 16-16](#)

Required Configuration Tasks

This section lists the required configuration steps to configure the 2-Port and 4-Port Channelized T3 SPA. Some of the required configuration commands implement default values that might be appropriate for your network.

- [Configuring the T3 Controller, page 16-2](#)
- [Configuring the Logical T1 Interfaces, page 16-3](#)
- [Verifying T3 Controller Configuration, page 16-5](#)
- [Verifying Interface Configuration, page 16-6](#)



Note

To better understand the address format used to specify the physical location of the SIP, SPA, and interfaces, see the [“Specifying the Interface Address on a SPA” section on page 16-7](#).

Configuring the T3 Controller

To configure the T3 controller for the 2-Port and 4-Port Channelized T3 SPA, complete the following steps:


	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# controller t3 <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the Channelized T3 SPA port. See the “Specifying the Interface Address on a SPA” section on page 16-7.
Step 3	Router(config-controller)# [no] channelized	(Optional) Specifies the channelization mode. <ul style="list-style-type: none"> • channelized—In channelized mode, the T3 link can be channelized into 28 T1s, and each T1 can be further channelized into 24 DS0s. This is the default. • no channelized—In the unchannelized mode, the T3 link provides a single high-speed data channel of 44210 kbps.

	Command	Purpose
Step 4	Router(config-controller)# framing { auto-detect c-bit m23 }	(Optional) Specifies the framing type in channelized mode. <ul style="list-style-type: none"> • auto-detect—Detects the framing type at the device at the end of the line and switches to that framing type. If both devices are set to auto-detect, c-bit framing is used. • c-bit—Specifies c-bit parity framing. This is the default. • m23—Specifies M23 framing. Note To set the framing type for an unchannelized T3, see the “Configuring T3 Framing” section on page 16-13.
Step 5	Router(config-controller)# clock source { internal line }	(Optional) Specifies the clock source. <ul style="list-style-type: none"> • internal—Specifies that the internal clock source is used. Default for channelized mode. • line—Specifies that the network clock source is used. Default for unchannelized mode.
Step 6	Router(config-controller)# cablelength { <i>0 - 450</i> }	(Optional) Specifies the cable length. <ul style="list-style-type: none"> • <i>0-450</i>—Cable length in feet. The default is 224 ft.

Configuring the Logical T1 Interfaces

If channelized mode is configured for the T3 controller, use the following procedure to configure the logical T1 interfaces:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# controller t3 <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the Channelized T3 SPA port. See the “Specifying the Interface Address on a SPA” section on page 16-7.

	Command	Purpose
Step 3	Router(config-controller)# t1 <i>t1-number</i> channel-group <i>channel-number</i> timeslots <i>range</i> [speed {56 64}]	Specifies the T1 channel and time slots to be mapped to each channel. <ul style="list-style-type: none"> • <i>t1-number</i>—T1 number from 1 to 28. • <i>channel-number</i>—Specifies a channel-group mapping (0 to 23) under the designated T1. • <i>range</i>—List of time slots under the channel group. Time slots assigned to this T1 can be 1–24 or a combination of subranges within 1–24. You can indicate a range using a hyphen, commas, or a combination of both. One time slot equals one DS0. • speed— (Optional) Specifies the speed of a time slot in kilobits per second. Valid values are 56 and 64. The default speed of 64 kbps is not mentioned in the configuration.
Step 4	Router(config-controller)# t1 <i>t1-number</i> framing { esf sf [hdlc-idle {0x7e 0xff}]} [mode {j1}]}	(Optional) Specifies the T1 framing type using the framing command. <ul style="list-style-type: none"> • sf—Specifies Super Frame as the T1 frame type. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <p>Note If you select sf framing, you should consider disabling yellow alarm detection because the yellow alarm can be incorrectly detected with sf framing.</p> </div> <ul style="list-style-type: none"> • esf—Specifies Extended Super Frame as the T1 frame type. This is the default. • hdlc-idle—Allows you to set the idle pattern for the T1 interface to either 0x7e (the default) or 0xff. • mode j1—(Optional) Specifies the JT-G704 Japanese frame type.

	Command	Purpose
Step 5	Router(config-controller)# t1 channel-number clock source {internal line}	(Optional) Specifies the T1 clock source. <ul style="list-style-type: none"> internal—Specifies that the internal clock source is used. This is the default. line—Specifies that the network clock source is used.
Step 6	Configure the serial interfaces.	
	Note After a T1 channel is configured, it appears to the Cisco IOS software as a serial interface; therefore, all the configuration commands for a serial interface are available. However, not all commands are applicable to the T1 interface. All the encapsulation formats, such as PPP, HDLC, and Frame Relay are applicable to the configured T1. Encapsulation can be set via the serial interface configuration commands.	

For detailed interface configuration information, see the *Cisco IOS Interface Configuration Guide* for your Cisco IOS software release.

Verifying T3 Controller Configuration

Use the **show controllers** command to verify the controller configuration:

```
Router# show controller t3 2/0/0
T3 2/0/0 is up.
  Hardware is SPA-2XCT3/DS0
  IO FPGA version: 2.7, HDLC Framers version: 0
  T3/T1 Framers(1) version: 2
  SUBRATE FPGA version: 1.4
  HDLC controller available FIFO buffers 4084
  Applique type is Channelized T3/T1
  No alarms detected.
  MDL transmission is disabled
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Cablelength is 224
Clock Source is Internal
Equipment customer loopback
Data in current interval (726 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 0 LOS Defect Secs
Data in Interval 1:
  2 Line Code Violations, 6 P-bit Coding Violation
  0 C-bit Coding Violation, 1 P-bit Err Secs
  1 P-bit Severely Err Secs, 1 Severely Err Framing Secs
  0 Unavailable Secs, 1 Line Errored Secs
  1 C-bit Errored Secs, 1 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  10 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 1 Far-end path failures
  0 Far-end code violations, 10 FERF Defect Secs
```

```

    0 AIS Defect Secs, 0 LOS Defect Secs
Total Data (last 1 15 minute intervals):
    2 Line Code Violations, 6 P-bit Coding Violation,
    0 C-bit Coding Violation, 1 P-bit Err Secs,
    1 P-bit Severely Err Secs, 1 Severely Err Framing Secs,
    0 Unavailable Secs, 1 Line Errored Secs,
    1 C-bit Errored Secs, 1 C-bit Severely Errored Secs
    0 Severely Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
    10 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 1 Far-end path failures
    0 Far-end code violations, 10 FERF Defect Secs
    0 AIS Defect Secs, 0 LOS Defect Secs
T1 1 is down
timeslots: 1-24
FDL per AT&T 54016 spec.
Transmitter is sending LOF Indication.
Receiver is getting AIS.
Framing is ESF, Clock Source is Internal
Data in current interval (734 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    733 Unavail Secs, 0 Stuffed Secs
    367 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
Data in Interval 1:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    706 Unavail Secs, 0 Stuffed Secs
    353 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
Total Data (last 1 15 minute intervals):
    0 Line Code Violations, 0 Path Code Violations,
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
    706 Unavail Secs, 0 Stuffed Secs
    353 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
T1 2
    Not configured.

```

Verifying Interface Configuration

Use the **show interface serial** command to verify the interface configuration. The following example shows the output for the serial interface for an unchannelized T3:

```

Router# show interface serial13/0/0
Serial13/0/0 is down, line protocol is down
  Hardware is SPA-4XCT3/DS0
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles

```



```

        0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions alarm present
DSU mode 0, bandwidth 44210 Kbit, scramble 0, VC 0

```

The following example shows the output for a serial interface for the first T1 on a channelized T3:

```

Router# show interface serial2/0/1/1:0
serial2/0/1/1:0 is administratively down, line protocol is down
  Hardware is SPA-4XCT3/DS0
  MTU 1500 bytes, BW 832 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions alarm present
  VC 1: timeslot(s): 2-14, Transmitter delay 0, non-inverted data

```

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 2:

```
Router(config)# interface serial 2/0/0
```

This command shows a serial SPA as a representative example, however the same *slot/subslot/port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

For the 4-Port Channelized T3 SPA, the interface address format is *slot/subslot/port/t1-number:channel-group*, where:

- **t1-number**—Specifies the logical T1 number in channelized mode.
- *channel-group*—Specifies the logical channel group assigned to the time slots within the T1 link.

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs”](#) section on page 4-1.

Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your serial SPA.

- [Configuring Data Service Unit Mode, page 16-8](#)
- [Configuring Maintenance Data Link, page 16-9](#)
- [Configuring Encapsulation, page 16-11](#)
- [Configuring T3 Framing, page 16-13](#)
- [Configuring FDL, page 16-13](#)
- [Configuring Scramble, page 16-15](#)

Configuring Data Service Unit Mode

Configure the SPA to connect with customer premises Data Service Units (DSUs) by setting the DSU mode. Subrating a T3 or E3 interface reduces the peak access rate by limiting the data transfer rate. To configure the DSU mode, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none">• <i>slot/subslot/port</i>—Specifies the location of the interface. See also the “Specifying the Interface Address on a SPA” section on page 16-7.

	Command	Purpose
Step 3	Router(config-if)# dsu mode {0 1 2 3 4}	<p>Specifies the interoperability mode used by the T3 controller.</p> <ul style="list-style-type: none"> 0—Connects a T3 controller to another T3 controller or to a Digital Link DSU. Bandwidth range is from 300 to 44210 kbps. This is the default. 1—Connects a T3 controller to a Kentrox DSU. Bandwidth range is from 1500 to 35000, or 44210 kbps. <p>Note If the bandwidth is set between 35000 and 44210 kbps, an error message is displayed.</p> <ul style="list-style-type: none"> 2—Connects a T3 controller to a Larscom DSU. Bandwidth range is from 3100 to 44210 kbps. 3—Connects a T3 controller to an Adtran T3SU 300. Bandwidth range is from 75 to 44210 kbps. 4—Connects a T3 controller to a Verilink HDM 2182. Bandwidth range is from 1500 to 44210 kbps.
Step 4	Router(config-if)# dsu bandwidth <i>kbps</i>	<p>Specifies the maximum allowable bandwidth.</p> <ul style="list-style-type: none"> <i>kbps</i>—Bandwidth range is from 1 to 44210 kbps.

Verifying DSU Mode

Use the **show controllers serial** command to display the DSU mode of the controller:

```
Router# show controllers serial
Serial2/1/0 -
  Framing is c-bit, Clock Source is Internal
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 0, since reset 0
  Data in current interval (0 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
    0 Severely Errorred Line Secs
    0 Far-End Errorred Secs, 0 Far-End Severely Errorred Secs
    0 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures
    0 Far-end code violations, 0 FERF Defect Secs
    0 AIS Defect Secs, 0 LOS Defect Secs
  Transmitter is sending AIS.
```

Configuring Maintenance Data Link

MDL messages are used to communicate identification information between local and remote ports. The type of information included in MDL messages includes the equipment identification code (EIC), location identification code (LIC), frame identification code (FIC), unit, Path Facility Identification (PFI), port number, and Generator Identification numbers.

To configure Maintenance Data Link (MDL), use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# controller t3 <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. See also the “Specifying the Interface Address on a SPA” section on page 16-7.
Router(config-controller)# mdl [string { eic fic generator lic pfi port unit } <i>string</i> }] [transmit { idle-signal path test-signal }]	Configures the MDL message. <ul style="list-style-type: none"> string eic—Specifies the Equipment Identification Code; can be up to 10 characters. string fic—Specifies the Frame Identification Code; can be up to 10 characters. string generator—Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters. string lic— Specifies the Location Identification Code; can be up to 11 characters. string pfi—Specifies the Path Facility Identification Code sent in the MDL Path message; can be up to 38 characters. string port—Specifies the port number string sent in the MDL Idle Signal message; can be up to 38 characters. string unit—Specifies the Unit Identification Code. <i>string</i>—Specifies the length of the Unit Identification Code, up to 6 characters. transmit idle-signal—Enables MDL Idle-Signal message transmission. transmit path—Enables MDL Path message transmission. transmit test-signal—Enables MDL Test-Signal message transmission.

Verifying MDL

Use the **show controllers t3** command to display the MDL settings:

```
Router# show controllers t3 3/0/0
T3 3/0/0 is down. Hardware is 2 ports CT3 SPA
ATLAS FPGA version: 0, FREEDM336 version: 0
TEMUX84(1) version: 0, TEMUX84(1) version: 0
```

```

SUBRATE FPGA version: 0
Applique type is Subrate T3
Receiver has loss of signal.
MDL transmission is enabled
    EIC: new, LIC: US, FIC: 23, UNIT: myunit
    Path FI: test pfi
    Idle Signal PORT_NO: New-port
    Test Signal GEN_NO: test-message
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line
Equipment customer loopback
Data in current interval (869 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation, 0 P-bit Err Secs
    0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
    869 Unavailable Secs, 0 Line Errored Secs
    0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
    0 Severely Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
    869 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures
    0 Far-end code violations, 0 FERF Defect Secs
    0 AIS Defect Secs, 870 LOS Defect Secs

```

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.

Command	Purpose
Channelized Router(config)# interface serial <i>slot/subslot/port/t1-number:channel-group</i> Unchannelized Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> Channelized: <i>slot/subslot/port/t1-number:channel-group</i>—Specifies the location of the interface. See also the “Specifying the Interface Address on a SPA” section on page 16-7. Unchannelized: <i>slot/subslot/port</i>—Specifies the location of the interface. See also the “Specifying the Interface Address on a SPA” section on page 16-7.
Router(config-if)# encapsulation <i>encapsulation-type {hdlc ppp frame-relay}</i>	Sets the encapsulation type on the interface: <ul style="list-style-type: none"> hdlc—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. ppp—Point-to-Point Protocol (PPP) (for serial interface). frame-relay—Frame Relay (for serial interface).

Verifying Encapsulation

Use the **show interfaces serial** command to display the encapsulation method:

```
Router# show interfaces serial2/0/0
Serial3/0/0 is down, line protocol is down
  Hardware is SPA-2XCT3/DS0
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions alarm present
  DSU mode 0, bandwidth 44210 Kbit, scramble 0, VC 0
```

Configuring T3 Framing

To set the T3 framing type, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See also the “Specifying the Interface Address on a SPA” section on page 16-7.
Router(config-if)# framing {c-bit m13}	Specifies the framing type in unchannelized mode. <ul style="list-style-type: none"> c-bit—Specifies C-bit parity framing. This is the default. m13—Specifies DS3 Framing M13 (same as M23).

Verifying Framing

Use the **show controller** command to display the framing type:

```
Router# show controller t3 3/0/0
T3 3/0/0 is down. Hardware is 2 ports CT3 SPA
ATLAS FPGA version: 0, FREEDM336 version: 0
TEMUX84(1) version: 0, TEMUX84(1) version: 0
SUBRATE FPGA version: 0
Applique type is Subrate T3
Receiver has loss of signal.
Framing is M13, Line Code is B3ZS, Clock Source is Line
Equipment customer loopback
Data in current interval (656 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  666 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 666 LOS Defect Secs
```

Configuring FDL

Facility Data Link (FDL) is a far-end performance reporting tool. In ANSI mode, you can enable one-second transmissions of performance reports on both ends of the T1 connection. To configure FDL, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# controller t3 slot/subslot/port	Selects the controller to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. See also the “Specifying the Interface Address on a SPA” section on page 16-7.
Router(config-controller)# t1 number fdl {ansi}	(Optional) Enables FDL. <ul style="list-style-type: none"> <i>number</i>—Specifies the T1 channel number. ansi—Specifies the FDL bit per the ANSI T1.403 specification.

Verifying FDL

Use the **show controller** command to display the FDL setting:

```
Router# show controller t3 3/0/1/1
T3 3/0/1 is down. Hardware is 2 ports CT3 SPA
  ATLAS FPGA version: 0, FREEDM336 version: 0
  TEMUX84(1) version: 0, TEMUX84(1) version: 0
  SUBRATE FPGA version: 0
  Applique type is Channelized T3
  Receiver has loss of signal.
  Framing is M23, Line Code is B3ZS, Clock Source is Internal
  Equipment customer loopback
  Data in current interval (456 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation, 0 P-bit Err Secs
    0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
    456 Unavailable Secs, 0 Line Errored Secs
    0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
    0 Severely Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
    0 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures
    0 Far-end code violations, 0 FERF Defect Secs
    0 AIS Defect Secs, 456 LOS Defect Secs
T1 1 is down
  timeslots: 2-14
FDL per ANSI T1.403 and AT&T 54016 spec.
  Configured for FDL remotely line looped (bell)
  Transmitter is sending LOF Indication.
  Receiver is getting AIS.
  Framing is ESF, Clock Source is Line
  BERT running on timeslots 2,3,4,5,6,7,8,9,10,11,12,13,14,
  BERT test result (running)
    Test Pattern : All 1's, Status : Not Sync, Sync Detected : 0
    Interval : 2 minute(s), Time Remain : 2 minute(s)
    Bit Errors (since BERT started): 0 bits,
    Bits Received (since BERT started): 0 Kbits
    Bit Errors (since last sync): 0 bits
    Bits Received (since last sync): 0 Kbits
  Data in current interval (703 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```



```

0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
713 Unavail Secs, 0 Stuffed Secs
357 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs

```

Configuring Scramble

T3 scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns—in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

To configure scrambling, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See also the “Specifying the Interface Address on a SPA” section on page 16-7.
Router(config-if)# scramble [0 1]	Enables scrambling. Scrambling is disabled by default. <ul style="list-style-type: none"> 1—Enabled. 0—Disabled.

Verifying Scramble Configuration

Use the **show interface serial** command to display the scramble setting:

```

Router# show interface serial3/0/0
Serial3/0/0 is down, line protocol is down
  Hardware is SPA-2XCT3/DS0
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 4 interface resets
    0 output buffer failures, 0 output buffers swapped out

```

```
1 carrier transitions alarm present
DSU mode 0, bandwidth 44210 Kbit, scramble 1, VC 0
```

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications that corresponds to your Cisco IOS software release.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Routers configuration settings, you can use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your 2-Port and 4-Port Channelized T3 SPA.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the 2-Port and 4-Port Channelized T3 SPA, use the **show interfaces serial** command.

The following example provides sample output for the serial interface on an unchannelized T3:

```
Router# show interfaces serial3/0/0
Serial3/0/0 is down, line protocol is down
  Hardware is SPA-2XCT3/DS0
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 4 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions alarm present
  DSU mode 0, bandwidth 44210 Kbit, scramble 1, VC 0
```

The following example provides sample output for the serial interface on a channelized T3:

```
Router# show interfaces serial12/0/1/1:0
serial12/0/1/1:0 is down, line protocol is down
  Hardware is SPA-2XCT3/DS0
  MTU 1500 bytes, BW 832 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions alarm present
  VC 1: timeslot(s): 2-14, Transmitter delay 0, non-inverted data
```

To find detailed status and statistical information on a per-port basis for the 2-Port and 4-Port Channelized T3 SPA, use the **show controllers serial** command:

```
Router# show controllers serial 0/2/0
Serial0/2/0 - (SPA-4XT3/E3) is up
  Current mode is T3
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10 feet
  rx FEBE since last clear counter 0, since reset 0
  Data in current interval (30 seconds elapsed):
    1 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 1 Unavailable Secs
    1 Line Error Secs, 0 C-bit Error Secs, 0 C-bit Sev Err Secs
    0 Severely Errored Line Secs
    0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
    10 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures
    0 Far-end code violations, 10 FERF Defect Secs
    0 AIS Defect Secs, 0 LOS Defect Secs

  No alarms detected.

  No FEAC code is being received
  MDL transmission is disabled
```

Configuration Examples

This section includes the following configuration examples:

- [DSU Configuration Example, page 16-18](#)
- [MDL Configuration Example, page 16-18](#)
- [Encapsulation Configuration Example, page 16-18](#)

- [Framing in Unchannelized Mode Configuration Example, page 16-19](#)
- [Facility Data Link Configuration Example, page 16-19](#)
- [Scrambling Configuration Example, page 16-19](#)
- [Creating a Multilink Bundle Configuration Example, page 16-19](#)
- [Assigning a T1 Interface to a Multilink Bundle Configuration Example, page 16-20](#)

DSU Configuration Example

The following example sets the DSU mode on interface port 0 on slot 4, subslot 1:

```
! Specify the interface and enter interface configuration mode.
!
Router(config-int)# interface t3 4/1/0
!
! Specifies the interoperability mode used by the T3 interface.
!
Router(config-int)# dsu mode 2
!
! Specifies the maximum allowable bandwidth.

Router(config-int)# dsu bandwidth 23000
```

MDL Configuration Example

The following example configures the MDL strings on controller port 0 on slot 4, subslot 1:

```
! Enter controller configuration mode.
!
Router(config)# controller t3 4/1/0
!
! Specify the mdl strings.
!
Router(config-controller)# mdl string eic beic
Router(config-controller)# mdl string lic beic
Router(config-controller)# mdl string fic bfix
Router(config-controller)# mdl string unit bunit
Router(config-controller)# mdl string pfi bpfi
Router(config-controller)# mdl string port bport
Router(config-controller)# mdl string generator bgen
Router(config-controller)# mdl transmit path
Router(config-controller)# mdl transmit idle-signal
Router(config-controller)# mdl transmit test-signal
```

Encapsulation Configuration Example

The following example configures encapsulation on a channelized T1 interface:

```
! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 4/1/1/1:0
!
! Specify the encapsulation method.
!
Router(config-if)# encapsulation ppp
```

The following example configures encapsulation and framing on a unchannelized T3 interface:

```
! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 4/1/1
!
! Specify the encapsulation method.
!
Router(config-if)# encapsulation ppp
```

Framing in Unchannelized Mode Configuration Example

The following example configures framing on an unchannelized T3 interface:

```
! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 4/1/1
!
! Specify the framing type.
!
Router(config-if)# framing m13
```

Facility Data Link Configuration Example

The following example configures FDL on a channelized T1 interface:

```
! Specify the controller to configure and enter controller configuration mode.
!
Router(config)# controller t3 3/1/0
!
! Specify the T1 controller and set the FDL bit.
!
Router(config-controller)# t1 1 fdl ansi
```

Scrambling Configuration Example

The following example configures scrambling on the T3 interface:

```
! Enter global configuration mode.
!
Router# configure terminal
!
! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 4/1/3
!
! Enable scrambling.
!
Router(config-if)# scramble
```

Creating a Multilink Bundle Configuration Example

The following example configures multilink bundle 1 on the T3 interface:

```
!! Enter global configuration mode.
!
Router# configure terminal
```

```

!
! Create a multilink interface and enter interface configuration mode.
!
Router(config)# interface multilink 1
!
! Specify the IP address for the interface.
!
Router(config-if)# ip address 123.1.1.1 255.255.255.0
!

```

Assigning a T1 Interface to a Multilink Bundle Configuration Example

The following example assigns a T1 interface to multilink group 1:

```

! ! Enter global configuration mode.
!
Router# configure terminal
!
! Specify the T1 interface and enter interface configuration mode.
!
Router(config)# interface serial 1/0/1/1:0
!
! Specify PPP encapsulation.
!
Router(config-if)# encapsulation ppp
!
! Specify the multilink bundle the T1 will belong to.
!
Router(config-if)# ppp multilink group 1
!

```



CHAPTER 17

Configuring the 2-Port and 4-Port Clear Channel T3/E3 SPAs

This chapter provides information about configuring the 2-Port and 4-Port Clear Channel T3/E3 SPAs on the Cisco ASR 1000 Series Routers. It includes the following sections:

- [Configuration Tasks, page 17-1](#)
- [Verifying the Interface Configuration, page 17-16](#)
- [Configuration Examples, page 17-18](#)

For information about managing your system image and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications for your Cisco IOS software release.

For more information, see the [“Related Documentation” section on page xxvi](#).

Configuration Tasks

This section describes how to configure the 2-Port and 4-Port Clear Channel T3/E3 SPA for the Cisco ASR 1000 Series Routers and includes information about verifying the configuration.

It includes the following topics:

- [Required Configuration Tasks, page 17-2](#)
- [Specifying the Interface Address on a SPA, page 17-5](#)
- [Optional Configurations, page 17-5](#)
- [Saving the Configuration, page 17-16](#)

Required Configuration Tasks

This section lists the required configuration steps to configure the 2-Port and 4-Port Clear Channel T3/E3 SPA. Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command.

- [Setting the Card Type, page 17-2](#)
- [Setting the IP Address, page 17-3](#)
- [Verifying Controller Configuration, page 17-3](#)
- [Verifying Interface Configuration, page 17-4](#)



Note

To better understand the address format used to specify the physical location of the SIP, SPA, and interfaces, see the [“Specifying the Interface Address on a SPA” section on page 17-5](#).

Setting the Card Type

The SPA is not functional until the card type is set. Information about the SPA is not indicated in the output of any **show** commands until the card type has been set. There is no default card type.



Note

Mixing of interface types is not supported. All ports on a SPA must be of the same type.

To set the card type for the 2-Port and 4-Port Clear Channel T3/E3 SPA, complete these steps:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# card type {t3 e3} slot subslot	Sets the serial mode for the SPA: <ul style="list-style-type: none"> • t3—Specifies T3 connectivity of 44210 kbps through the network, using B3ZS coding. • e3—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34010 kbps. • <i>slot subslot</i>—Specifies the location of the SPA. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Step 3	Router(config)# exit	Exits configuration mode and returns to the EXEC command interpreter prompt.

Setting the IP Address

To set the IP address for the 2-Port and 4-Port Clear Channel T3/E3 SPA, complete these steps:

	Command	Purpose
Step 1	Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Step 2	Router(config-if)# ip address <i>address mask</i>	Sets the IP address and subnet mask. <ul style="list-style-type: none"> <i>address</i>—IP address. <i>mask</i>—Subnet mask.
Step 3	Router(config-if)# clock source { internal line }	Sets the clock source. <ul style="list-style-type: none"> internal—Specifies that the internal clock source is used. line—Specifies that the network clock source is used. This is the default.
Step 4	Router(config-if)# no shut	Enables the interface.
Step 5	Router(config)# exit	Exits interface configuration mode and returns to the EXEC command interpreter prompt.

Verifying Controller Configuration

Use the **show controllers** command to verify the controller configuration:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Data in current interval (546 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 44:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    560 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Total Data (last 44 15 minute intervals):
    0 Line Code Violations, 0 P-bit Coding Violation,
    0 C-bit Coding Violation,
    0 P-bit Err Secs, 0 P-bit Sev Err Secs,
    0 Sev Err Framing Secs, 0 Unavailable Secs,
```

```

24750 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs

Transmitter is sending AIS.

Receiver has loss of signal.

40434 Sev Err Line Secs, 0 Far-End Err Secs, 0 Far-End Sev Err Secs
0 P-bit Unavailable Secs, 0 CP-bit Unavailable Secs
0 CP-bit Far-end Unavailable Secs
0 Near-end path failures, 0 Far-end path failures

No FEAC code is being received
MDL transmission is disabled

```

Use the **show controllers brief** command to view a subset of the **show controllers** output:

```

Router# show controllers serial 2/0/2 brief
Serial2/0/2 -
  Framing is c-bit, Clock Source is Internal
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 0, since reset 22

  No alarms detected.

  No FEAC code is being received
  MDL transmission is disabled

```

Verifying Interface Configuration

Use the **show interfaces** command to verify the interface configuration:

```

Router# show interfaces serial 2/0/0
Serial2/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 12/255, rxload 56/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent 13477, LMI stat recvd 13424, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 19, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/256, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 00:00:09, output 00:00:09, output hang never
  Last clearing of "show interface" counters 1d13h
  Input queue: 0/75/3/3891 (size/max/drops/flushes); Total output drops: 5140348
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 9716000 bits/sec, 28149 packets/sec
  5 minute output rate 2121000 bits/sec, 4466 packets/sec
    14675957334 packets input, 645694448563 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
      0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    14562482078 packets output, 640892196653 bytes, 0 underruns
    0 output errors, 0 applique, 4 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  rxLOS inactive, rxLOF inactive, rxAIS inactive
  txAIS inactive, rxRAI inactive, txRAI inactive
Serial2/0/0.16 is up, line protocol is up
  Hardware is SPA-4T3E3

```

```
Internet address is 110.1.1.2/24
MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 11/255, rxload 53/255
Encapsulation FRAME-RELAY
```

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 2:

```
Router(config)# interface serial 2/0/0
```

This command shows a serial SPA as a representative example, however the same *slot/subslot/port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs”](#) section on page 4-1.

Optional Configurations

There are several standard, but optional configurations, that might be necessary to complete the configuration of your serial SPA.

- [Configuring Data Service Unit Mode, page 17-5](#)
- [Configuring Maintenance Data Link, page 17-7](#)
- [Configuring Scramble, page 17-9](#)
- [Configuring Framing, page 17-11](#)
- [Configuring Encapsulation, page 17-12](#)
- [Configuring Cable Length, page 17-13](#)
- [Configuring Invert Data, page 17-14](#)
- [Configuring the Trace Trail Buffer, page 17-15](#)
- [Configuring QoS Features on Serial SPAs, page 17-16](#)

Configuring Data Service Unit Mode

Configure the SPA to connect with customer premises Data Service Units (DSUs) by setting the DSU mode. Subrating a T3 or E3 interface reduces the peak access rate by limiting the data transfer rate.

To configure the DSU mode and bandwidth, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial slot/subslot/port	<p>Selects the interface to configure and enters interface configuration mode.</p> <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
T3 Router(config-if)# dsu mode {0 1 2 3 4} E3 Router(config-if)# dsu mode {0 1}	<p>Specifies the interoperability mode used by a T3 controller.</p> <ul style="list-style-type: none"> 0—Connects a T3/E3 controller to another T3/E3 controller or to a Digital Link DSU (DL3100 in T3 mode and DL3100E in E3 mode). This is the default. 1—Connects a T3/E3 controller to a Kentrox DataSMART T3/E3 IDSU. 2—Connects a T3 controller to a Larscom Access-T45 DS3 DSU. 3—Connects a T3 controller to an Adtran T3SU 300. 4—Connects a T3 controller to a Verilink HDM 2182.
Router(config-if)# dsu bandwidth kbps	<p>Specifies the allowable bandwidth.</p> <ul style="list-style-type: none"> <i>kbps</i>—The bandwidth range and increment values are based on the specific DSU. Default for T3 mode is 44010 kbps and 34010 kbps for E3 mode. <ul style="list-style-type: none"> Digital Link DL3100 bandwidth range is 300 to 44210 kbps. Digital Link DL3100E bandwidth range is 358 to 34010 kbps. Kentrox DataSMART T3/E3 IDSU bandwidth range is 1000 to 34000 kbps for E3 mode and 1500 to 44210 kbps for T3 mode. Larscom Access-T45 DS3 bandwidth range is 3100 to 44210 kbps. Adtran T3SU 300 bandwidth range is 80 to 44210 kbps. Verilink HDM 2182 bandwidth range is 1600 to 31600 kbps.

Command	Purpose
Router(config-if)# remote {accept fullrate}	Specifies where the DSU bandwidth is set. <ul style="list-style-type: none"> • accept—Accepts incoming remote requests to reset the DSU bandwidth. • fullrate—Sets far end DSU to its fullrate bandwidth.

Verifying DSU Mode

Use the **show controllers serial** command to display the DSU mode of the controller:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Data in current interval (546 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
```

Configuring Maintenance Data Link

MDL messages are used to communicate identification information between local and remote ports. The type of information included in MDL messages includes the equipment identification code (EIC), location identification code (LIC), frame identification code (FIC), unit, Path Facility Identification (PFI), port number, and Generator Identification numbers.



Note

C-bit framing must be enabled in order to transport MDL messages between source and destination T3 ports.

To configure Maintenance Data Link (MDL), use the following commands.

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure. <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.

Command	Purpose
Router(config-if)# mdl [string { eic fic generator lic pfi port unit } <i>string</i> }] [transmit { idle-signal path test-signal }]	<p>Configures the Maintenance Data Link (MDL) message.</p> <ul style="list-style-type: none"> • eic <i>string</i>—Specifies the Equipment Identification Code (up to 10 characters), which is a value used to describe a specific piece of equipment according to ANSI T1.107-1995. • fic <i>string</i>—Specifies the Frame Identification Code (up to 10 characters), which is a value used to identify where the equipment is located within a building at a given location according to ANSI T1.107-1995. • generator <i>string</i>—Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters. • lic <i>string</i>—Specifies the Location Identification Code (up to 11 characters), which is a value used to describe a specific location according to ANSI T1.107-1995. • pfi <i>string</i>—Specifies the Path Facility Identification Code sent in the MDL Path message; can be up to 38 characters. • port <i>string</i>—Specifies the port number string sent in the MDL Idle Signal message; can be up to 38 characters. • unit <i>string</i>—Specifies the Unit Identification Code (up to 6 characters), which is a value that identifies the equipment location within a subslot according to ANSI T1.107-1995. • transmit idle-signal—Enables transmission of the MDL Idle-Signal message. An MDL Idle-Signal message, as defined by ANSI T1.107, is distinguished from path and test signal messages in that it contains a port number as its final data element. • transmit path—Enables transmission of the MDL Path message. An MDL Path message, as defined by ANSI T1.107, is distinguished from idle and test signal messages in that it contains a facility identification code as its final data element. • transmit test-signal—Enables transmission of the MDL Test-Signal message. An MDL Test-Signal message, as defined by ANSI T1.107, is distinguished from path and idle signal messages in that it contains a generator number as its final data element.

Verifying MDL

Use the **show controllers serial** command to display the MDL settings:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Data in current interval (546 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs

  Data in Interval 96:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
  Total Data (last 24 hours)
    0 Line Code Violations, 0 P-bit Coding Violation,
    0 C-bit Coding Violation,
    0 P-bit Err Secs, 0 P-bit Sev Err Secs,
    0 Sev Err Framing Secs, 0 Unavailable Secs,
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs

  No alarms detected.

    0 Sev Err Line Secs, 1 Far-End Err Secs, 0 Far-End Sev Err Secs
    0 P-bit Unavailable Secs, 0 CP-bit Unavailable Secs
    0 CP-bit Far-end Unavailable Secs
    0 Near-end path failures, 0 Far-end path failures

  No FEAC code is being received
  MDL transmission is enabled
    EIC: tst, LIC: 67,
    Test Signal GEN_NO: test
  Far-End MDL Information Received
    EIC: tst, LIC: 67,
    Test Signal GEN_NO: test
```

Configuring Scramble

T3/E3 scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns—in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

To configure scrambling, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Router(config-if)# [no] scramble	Enables scrambling. Scrambling is disabled by default. <ul style="list-style-type: none"> scramble—Enables scramble. no scramble—Disables scramble. <p>Note When using framing bypass, no scrambling must be configured.</p>

Verifying Scramble Configuration

Use the **show controllers serial** command to display the scrambling setting:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Scrambling is enabled
  Data in current interval (356 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
```


Configuring Framing

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. To configure framing, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the T3/E3 interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
T3 Router(config-if)# framing { bypass c-bit m13 }	Sets the framing on the interface. <ul style="list-style-type: none"> bypass—Configures framing bypass to use the full T3 or E3 bandwidth.
E3 Router(config-if)# framing { bypass g751 g832 }	<ul style="list-style-type: none"> c-bit—Specifies C-bit parity framing. This is the default for T3. m13—Specifies M13 framing. g751— Specifies g751 framing. This is the default for E3. g832—Specifies g832 framing.

Verifying Framing Configuration

Use the **show controllers serial** command to display the framing method:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Data in current interval (546 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
```

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Router(config-if)# encapsulation <i>encapsulation-type</i> { hdlc ppp frame-relay }	Sets the encapsulation type on the interface: <ul style="list-style-type: none"> hdlc—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. ppp—PPP (for serial interface). frame-relay—Frame Relay (for serial interface).

Verifying Encapsulation

Use the **show interfaces serial** command to verify encapsulation on the interface:

```
Router# show interfaces serial 2/0/1
Serial2/0/1 is up, line protocol is up
  Hardware is SPA-4T3E3
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 223/255, rxload 222/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent 13076, LMI stat recvd 13076, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/256, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 00:00:04, output 00:00:04, output hang never
  Last clearing of "show interface" counters 1d12h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 38579000 bits/sec, 109611 packets/sec
  5 minute output rate 38671000 bits/sec, 109852 packets/sec
    14374551065 packets input, 632486376132 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  14408526130 packets output, 633974757440 bytes, 0 underruns
  0 output errors, 0 applique, 0 interface resets
```

```

0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
rxLOS inactive, rxLOF inactive, rxAIS inactive
txAIS inactive, rxRAI inactive, txRAI inactive

```

Configuring Cable Length

The **cablelength** command compensates for the loss in decibels based on the distance from the device to the first repeater in the circuit. A longer distance from the device to the repeater requires that the signal strength on the circuit be boosted to compensate for loss over that distance. To configure cable length, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Router(config-if)# cablelength <i>length</i>	Sets the cable length. <ul style="list-style-type: none"> <i>length</i>—Range is 0 to 450 feet. The default is 10 feet.

Verifying Cable Length Setting

Use the **show interfaces serial** command to verify the cable length setting:

```

Router# show interfaces serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Internal
  Bandwidth limit is 44210, DSU mode 0, Cable length is 200
  rx FEBE since last clear counter 0, since reset 22
  Data in current interval (446 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs
  Data in Interval 2:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errorred Secs, 0 C-bit Errorred Secs, 0 C-bit Sev Err Secs

```

Configuring Invert Data

Delays between the terminal equipment (TE) clock and data transmission indicate that the transmit clock signal might not be appropriate for the interface rate and length of cable being used. Different ends of the wire may have variances that differ slightly. Invert the clock signal to compensate for these factors. To configure invert data, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Router(config-if)# invert data	Inverts the data stream.

Verifying Invert Data Setting

Use the **show running configuration** command to verify that invert data was set on the interface:

```
Router# show running configuration
interface Serial2/0/0
 ip address 51.1.1.1 255.255.255.0
 logging event link-status
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 clock source internal
 invert data
 mdl string eic tst
 mdl string lic 67
 mdl string generator test
 mdl transmit path
 mdl transmit test-signal
 no cdp enable
!
```

Configuring the Trace Trail Buffer

Configure Trace Trail Buffer (TTB) to send messages to the remote device. The TTB messages check for the continued presence of the transmitter. To configure TTB, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 17-5.
Router(config-if)# ttb { country rnode serial snode soperator x } <i>string</i>	Sends a Trace Trail Buffer message in E3 g.832 framing mode. <ul style="list-style-type: none"> country—Two character country code. rnode—Receive node code. serial—M.1400 serial. snode—Sending location/Node ID code. soperator—Sending operator code (must be numeric). x—X0. <i>string</i>—TTB message.

Verifying TTB Settings

Use the **show controllers serial** command to display the TTB settings for the interface:

```
Router# show controllers serial 2/0/0
Serial2/0/0 -
  Framing is c-bit, Clock Source is Line
  Bandwidth limit is 44210, DSU mode 0, Cable length is 10
  rx FEBE since last clear counter 2, since reset 0
  Data in current interval (546 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
  Data in Interval 1:
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation
    0 P-bit Err Secs, 0 P-bit Sev Err Secs
    0 Sev Err Framing Secs, 0 Unavailable Secs
    0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
No alarms detected.
TTB transmission is disabled
TTB Rx: country: us soperator: s snode: sn rnode: rn x: x serial: 1
```

Configuring QoS Features on Serial SPAs

The SIPs and SPAs support many QoS features using modular QoS CLI (MQC) configuration. Since there are no serial SPA-specific QoS features, refer to your network processor documentation for QoS configuration information.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For information about managing your system image and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications for your Cisco IOS software release.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Routers configuration settings, you can use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your 2-Port and 4-Port Clear Channel T3/E3 SPA.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the 2-Port and 4-Port Clear Channel T3/E3 SPA, use the **show interfaces serial** command.

The following example provides sample output for interface port 1 on the SPA located in the first subslot of the SIP installed in slot 2 of a Cisco ASR 1000 Series Routers:

```
Router# show interface serial 2/0/1
Serial2/0/1 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 120.1.1.1/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 234/255, rxload 234/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 40685000 bits/sec, 115627 packets/sec
  5 minute output rate 40685000 bits/sec, 115624 packets/sec
    4652915554 packets input, 204728203496 bytes, 0 no buffer
    Received 4044 broadcasts (0 IP multicast)
    130 runts, 0 giants, 0 throttles
```

```

0 parity
1595 input errors, 543 CRC, 0 frame, 0 overrun, 0 ignored, 922 abort
4653081242 packets output, 204735493748 bytes, 0 underruns
0 output errors, 0 applique, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions

```

Monitoring Per-Port Interface Statistics

To find detailed status and statistical information on a per-port basis for the 2-Port and 4-Port Clear Channel T3/E3 SPA, use the **show controllers serial** command.

The following example provides sample output for interface port 1 on the SPA located in the first subslot of the SIP that is installed in slot 2 of the Cisco ASR 1000 Series Router:

```

Router#show controllers serial 2/0/2
Serial2/0/2 -
Framing is c-bit, Clock Source is Line
Bandwidth limit is 44210, DSU mode 0, Cable length is 10
rx FEBE since last clear counter 0, since reset 0
Data in current interval (807 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Sev Err Secs
  0 Sev Err Framing Secs, 306 Unavailable Secs
  500 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
Data in Interval 1:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Sev Err Secs
  0 Sev Err Framing Secs, 0 Unavailable Secs
  564 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
Data in Interval 2:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Sev Err Secs
  0 Sev Err Framing Secs, 0 Unavailable Secs
  564 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
Data in Interval 3:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Sev Err Secs
  0 Sev Err Framing Secs, 0 Unavailable Secs
  562 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
Data in Interval 4:
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Sev Err Secs
  0 Sev Err Framing Secs, 0 Unavailable Secs
  560 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
Total Data (last 44 15 minute intervals):
  0 Line Code Violations, 0 P-bit Coding Violation,
  0 C-bit Coding Violation,
  0 P-bit Err Secs, 0 P-bit Sev Err Secs,
  0 Sev Err Framing Secs, 0 Unavailable Secs,
  24750 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs

Transmitter is sending AIS.

Receiver has loss of signal.

40434 Sev Err Line Secs, 0 Far-End Err Secs, 0 Far-End Sev Err Secs

```

```
0 P-bit Unavailable Secs, 0 CP-bit Unavailable Secs
0 CP-bit Far-end Unavailable Secs
0 Near-end path failures, 0 Far-end path failures

No FEAC code is being received
MDL transmission is disabled
```

Configuration Examples

This section includes the following configuration examples:

- [DSU Configuration Example, page 17-18](#)
- [MDL Configuration Example, page 17-18](#)
- [Scrambling Configuration Example, page 17-19](#)
- [Framing Configuration Example, page 17-19](#)
- [Encapsulation Configuration Example, page 17-19](#)
- [Cable Length Configuration Example, page 17-19](#)
- [Invert Data Configuration Example, page 17-20](#)
- [Trace Trail Buffer Configuration Example, page 17-20](#)

DSU Configuration Example

The following example configures DSU on interface port 0 on slot 2, subslot:

```
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/0
!
! Specify the DSU mode
!
Router(config-if)# dsu mode 0
!
! Specify the DSU bandwidth
!
Router(config-if)# dsu bandwidth 10000
!
! Set the DSU bandwidth to accept or reject the incoming remote requests
!
Router(config-if)# dsu remote accept
```

MDL Configuration Example

The following example configures the MDL strings on interface port 0 on slot 2, subslot 1:

```
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/0
!
! Specify the MDL strings
!
Router(config-if)# mdl string eic beic
Router(config-if)# mdl string lic beic
Router(config-if)# mdl string fic bfix
```



```
Router(config-if)# mdl string unit bunit
Router(config-if)# mdl string pfi bpfi
Router(config-if)# mdl string port bport
Router(config-if)# mdl string generator bgen
Router(config-if)# mdl transmit path
Router(config-if)# mdl transmit idle-signal
Router(config-if)# mdl transmit test-signal
```

Scrambling Configuration Example

The following example configures scrambling on the T3/E3 interface:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3
!
! Enable scrambling
!
Router(config-if)# scramble
```

Framing Configuration Example

The following example configures framing on interface port 1 on slot 2, subslot 1:

```
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/1
!
! Specify the framing method
!
Router(config-if)# framing m13
```

Encapsulation Configuration Example

The following example configures encapsulation on interface port 1 on slot 2, subslot 1:

```
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/1
!
! Specify the encapsulation method
!
Router(config-if)# encapsulation PPP
```

Cable Length Configuration Example

The following example sets the cable length to 200 feet:

```
! Enter global configuration mode
!
Router# configure terminal
!
```

```
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3
!
! Specify the cable length
!
Router(config-if)# cablelength 200
```

Invert Data Configuration Example

The following example enables invert data:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3
!
! Enable invert data
!
Router(config-if)# invert data
```

Trace Trail Buffer Configuration Example

The following example configures the TTB attributes:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3
!
! Specify the TTB attributes
!
Router(config-if)# ttb country ab
Router(config-if)# ttb soperator 56
Router(config-if)# ttb snode 34
Router(config-if)# ttb rnode cd
Router(config-if)# ttb x 7
Router(config-if)# ttb serial 12
```



CHAPTER 18

Configuring the 4-Port Serial Interface SPA

This chapter provides information about configuring the 4-Port Serial Interface SPA on Cisco ASR 1000 Series Routers. It includes the following sections:

- [Configuration Tasks, page 18-1](#)
- [Verifying the Interface Configuration, page 18-12](#)
- [Configuration Examples, page 18-13](#)

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications for your Cisco IOS software release.

For more information about the commands used in this chapter, refer to the *Cisco IOS Software Releases Command Reference* for your Cisco IOS software release. For more information, see the [“Related Documentation”](#) section on page xxvi.

Configuration Tasks

This section describes how to configure the 4-Port Serial Interface SPA for the Cisco ASR 1000 Series Routers and includes information about verifying the configuration.

It includes the following topics:

- [Configuring the 4-Port Serial Interface SPA, page 18-2](#)
- [Verifying the Configuration, page 18-2](#)
- [Verifying the Configuration, page 18-2](#)
- [Optional Configurations, page 18-7](#)
- [Saving the Configuration, page 18-12](#)

Configuring the 4-Port Serial Interface SPA

To configure the 4-Port Serial Interface SPA, complete these steps:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Verifying the Configuration” section on page 18-2 and the “Specifying the Interface Address on a SPA” section on page 18-7.
Step 3	Router(config-if)# ip address <i>address mask</i>	Sets the IP address and subnet mask. <ul style="list-style-type: none"> <i>address</i>—IP address. <i>mask</i>—Subnet mask.
Step 4	Router(config-if)# clock rate <i>bps</i>	Configures the clock rate for the hardware to an acceptable bit rate per second (bps).



Note

Each port should first be connected with the appropriate cable before attempting full configuration. Some commands are enabled only based upon the cable type connected to the port.



Note

The bandwidth of each interface is 2 MB by default; setting the clock rate does not change the interface bandwidth. We recommend that you configure the bandwidth value with the **clock rate** command at the DCE and DTE side.



Note

A clock rate of 2016000 does not appear in the configuration because it is the default value.

Verifying the Configuration

After configuring the new interface, use the **show** commands to display the status of the new interface or all interfaces, and use the **ping** and **loopback** commands to check connectivity. This section includes the following subsections:

- [Using show Commands, page 18-3](#)
- [Using the ping Command to Verify Network Connectivity, page 18-6](#)
- [Using loopback Commands, page 18-6](#)

Using show Commands

The table below shows the **show** commands you can use to verify the operation of the 4-Port Serial Interface SPA. Sample displays of the output of selected **show** commands appear in the section that follows. For complete command descriptions and examples, refer to the publications listed in the “[Related Documentation](#)” section on page xxvi.



Note

The outputs that appear in this document may not match the output you receive when running these commands. The outputs in this document are examples only.

Command	Purpose
Router# show version	Displays system hardware configuration, the number of each interface type installed, Cisco IOS software version, names and sources of configuration files, and boot images.
Router# show controllers	Displays all the current interface processors and their interfaces.
Router# show controllers serial	Displays serial line statistics.
Router# show interfaces type <i>port-adapter-slot-number/</i> <i>interface-port-number</i>	Displays status information about a specific type of interface (for example, serial).
Router# show platform	Displays types of hardware installed in your system and the firmware version.
Router# show running-config	Displays the running configuration file.
Router# show startup-config	Displays the configuration stored in NVRAM.

Verification Examples

The following is an example of the **show version** command with the 4-Port Serial Interface SPA:

```
Router# show version
Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVIPSERVICESK9-M), Version
12.2(33)XN1, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 14-Feb-08 08:59 by
```

```
ROM: IOS-XE ROMMON
```

```
mcp-2ru-2 uptime is 4 minutes
Uptime for this control processor is 6 minutes System returned to ROM by reload System
image file is
''tftp://tftpboot/mcp-2ru-1/asr1000rpl-advipservicesk9.02.00.01.122-33.XN1.bin''
Last reload reason: Reload command
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
cisco ASR1002 (RP1) processor with 1647841K/6147K bytes of memory.
4 Gigabit Ethernet interfaces
6 Serial interfaces
2 Channelized T3 ports
32768K bytes of non-volatile configuration memory.
3728208K bytes of physical memory.
7798783K bytes of eUSB flash at bootflash:.
```

Configuration register is 0x0

The following is an example of the **show controllers serial** command with the 4-Port Serial Interface SPA:

```
Router# show controllers serial 2/1/1

Serial2/1/1 - (SPA-4XT-SERIAL) is up
Encapsulation : Frame Relay
Cable type: RS-232 DTE
mtu 1500, max_buffer_size 1524, max_pak_size 1608 enc 84
loopback: Off, crc: 16, invert_data: Off
nrzi: Off, idle char: Flag
tx_invert_clk: Off, ignore_dcd: Off
rx_clockrate: 552216, rx_clock_threshold: 0
serial_restartdelay:60000, serial_restartdelay_def:60000

RTS up, CTS up, DTR up, DCD up, DSR up
```



Note

The acronyms are defined as follows: RTS (Request to Send); CTS (Clear To Send); DTR (Data Transmit Ready); DCD (Data Carrier Detect); DSR (Data Set Ready).

The following is an example of the **show interfaces serial** command with the 4-Port Serial Interface SPA:

```
Router# show interfaces serial2/0/0
Serial 2/0/0 is up, line protocol is up
Hardware is SPA-4XT-SERIAL
Internet address is 192.168.33.1/29
MTU 4470 bytes, BW 8000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive not set
Clock Source Internal.
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters 1h
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 applique, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```

The following is an example of the **show platform** command:

```
Router# show platform
Chassis type: ASR1002
```

Slot	Type	State	Insert time (ago)
0	ASR1002-SIP10	ok	5d04h
0/0	4XGE-BUILT-IN	ok	5d04h
0/1	SPA-4XT-SERIAL	ok	4d05h
0/2	SPA-4XT3/E3	ok	4d04h
0/3	SPA-8XCHT1/E1	ok	4d04h
R0	ASR1002-RP1	ok, active	5d04h
F0	ASR1000-ESP5	ok, active	5d04h
P0	ASR1002-PWR-AC	ok	5d04h
P1	ASR1002-PWR-AC	ok	5d04h
Slot	CPLD Version	Firmware Version	
0	07092701	12.2(33r)XN2	
R0	07100216	12.2(33r)XN2	
F0	07091401	12.2(33r)XN2	

The following is an example of the **show running-config** command with the 4-Port Serial Interface SPA:

```
Router# show running-config serial
Building configuration...

Current configuration : 54 bytes
!
interface Serial2/0/0
  no ip address
  shutdown
end
```

The following is an example of the **show running interface** command with the 4-Port Serial Interface SPA:

```
Router# show running interface ser2/0/1
Building configuration...

Current configuration : 54 bytes
!
interface Serial2/0/1
  no ip address
  shutdown
end
```

The following is an example of the **show startup-config** command with the 4-Port Serial Interface SPA:

```
Router# show startup-config | b Serial2/0/0
interface Serial2/0/0
  no ip address
  shutdown
!
interface Serial2/0/1
  no ip address
  shutdown
!
interface Serial2/0/2
  no ip address
  shutdown
!
interface Serial2/0/3
  no ip address
  shutdown
!
```

Using the ping Command to Verify Network Connectivity

Using the **ping** command, you can verify that an interface port is functioning properly. This section provides a brief description of this command. Refer to the publications listed in the [“Related Documentation”](#) section on page xxvi for detailed command descriptions and examples.

The **ping** command sends echo request packets out to a remote device at an IP address that you specify. After sending an echo request, the system waits a specified time for the remote device to reply. Each echo reply is displayed as an exclamation point (!) on the console terminal; each request that is not returned before the specified timeout is displayed as a period (.). A series of exclamation points (!!!!!) indicates a good connection; a series of periods (.....) or the messages [timed out] or [failed] indicate a bad connection.

Following is an example of a successful **ping** command to a remote server with the address 10.0.0.10:

```
Router# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.0.0.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/64 ms
Router#
```

If the connection fails, verify that you have the correct IP address for the destination and that the device is active (powered on), and repeat the **ping** command.

Proceed to the next section, [“Using loopback Commands,”](#) to finish checking network connectivity.

Using loopback Commands

With the loopback test, you can detect and isolate equipment malfunctions by testing the connection between the 4-Port Serial Interface SPA and a remote device such as a modem or a channel service unit (CSU) or a data service unit (DSU). The **loopback** command places an interface in loopback mode, which enables test packets that are generated from the **ping** command to loop through a remote device or compact serial cable. If the packets complete the loop, the connection is good. If not, you can isolate a fault to the remote device or compact serial cable in the path of the loopback test.

**Note**

You must configure a clock rate on the port *before* performing a loopback test. However, if no cable is attached to the port, the port is administratively up, and the port is in loopback mode; you do not have to configure a clock rate on the port *before* performing a loopback test.

Depending on the mode of the port, issuing the **loopback** command checks the following path:

- When no compact serial cable is attached to the 4-Port Serial Interface SPA port, or if a data communication equipment (DCE) cable is attached to a port that is configured as line protocol up, the **loopback** command tests the path between the network processing engine and the interface port only (without leaving the network processing engine and port adapter).
- When a data terminal equipment (DTE) cable is attached to the port, the **loopback** command tests the path between the network processing engine and the near (network processing engine) side of the DSU or modem to test the 4-Port Serial Interface SPA and compact serial cable. (The X.21 DTE interface cable does not support this loopback test.)

**Note**

The X.21 interface definition does not include a loopback definition. On the 4-Port Serial Interface SPA, the X.21 DTE interface does not support the loopback function. Because of the internal clock signal present on the 4-Port Serial Interface SPAs, loopback will function on an X.21 DCE interface.

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with “0” from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 2:

```
Router(config)# interface serial 2/0/0
```

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Optional Configurations

There are several, but optional, configurations that may be necessary to complete the configuration of your serial SPA.

- [Configuring Timing Signals, page 18-7](#)
- [Inverting the Clock Signal, page 18-9](#)
- [Configuring NRZI Format, page 18-9](#)
- [Configuring Cyclic Redundancy Checks, page 18-10](#)
- [Configuring Encapsulation, page 18-10](#)

Configuring Timing Signals

All interfaces support both DTE and DCE mode, depending on the mode of the compact serial cable attached to the port. To use a port as a DTE interface, you need only connect a DTE compact serial cable to the port. When the system detects the DTE mode cable, it automatically uses the external timing signal. To use a port in DCE mode, you must connect a DCE compact serial cable and set the clock speed with the clock rate configuration command. You must also set the clock rate to perform a loopback test. This section describes how to set the clock rate on a DCE port and, if necessary, how to invert the clock to correct a phase shift between the data and clock signals.

Use the following commands when configuring timing signals:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. For further information, see the “Specifying the Interface Address on a SPA” section on page 18-7.
Router(config-if)# invert txclock	Inverts the transmit clock signal. When the EIA/TIA-232 interface is a DTE, the invert txclock command inverts the TxC signal the DTE receives from the remote DCE. When the EIA/TIA-232 interface is a DCE, the invert txclock command inverts the clock signal to the remote DTE port. The no form of this command changes the clock signal back to its original phase.
Router(config-if)# clock rate <i>bps</i>	Set standard clock rate, in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000. Any nonstandard clock rates that are entered are rounded off to the nearest hardware-supported clock rate. The actual clock rate is then displayed on the console. The no form of this command removes a clock rate that has been set.
Router(config-if)# invert data	Inverts the data signal. The no form of this command disables the inversion of the data signal.

**Note**

Clock rates supported for EIA/TIA-232: 1.2K, 2.4K, 4.8K, 9.6K, 14.4K, 19.2K, 28.8K, 32K, 38.4K, 56K, 64K, 128K.

**Note**

Clock rates supported for EIA-530, EIA-530A, EIA-449, V.35(bps): 1.2K, 2.4K, 4.8K, 9.6K, 14.4K, 19.2K, 28.8K, 32K, 38.4K, 56K, 64K, 72K, 115.2K, 2.048M, 2.341M, 2.731M, 3.277M, 4.09M, 5.461M, 8.064K.

**Note**

Clock rates supported for X.21: 1.2K, 2.4K, 4.8K, 9.6K, 14.4K, 19.2K, 28.8K, 32K, 38.4K, 56K, 64K, 72K, 115.2K, 2.016M.

Inverting the Clock Signal

Systems that use long cables or cables that are not transmitting the TxC (clock) signal might experience high error rates when operating at higher transmission speeds. If a 4-Port Serial Interface SPA port is reporting a high number of error packets, a phase shift might be the problem; inverting the clock might correct this phase shift.

When the EIA/TIA-232 interface is a DTE, the **invert-txclock** command inverts the TxC signal the DTE receives from the remote DCE. When the EIA/TIA-232 interface is a DCE, the **invert-txclock** command inverts the clock signal to the remote DTE port. Use the **no invert-txclock** command to change the clock signal back to its original phase.

Use the following commands when inverting the clock signal:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. For further information, see the “Specifying the Interface Address on a SPA” section on page 18-7.
Router(config-if)# invert txclock	Inverts the transmit clock signal. When the EIA/TIA-232 interface is a DTE, the invert txclock command inverts the TxC signal the DTE receives from the remote DCE. When the EIA/TIA-232 interface is a DCE, the invert txclock command inverts the clock signal to the remote DTE port. The no form of this command changes the clock signal back to its original phase.
Router(config-if)# invert data	Invert the data signal. The no form of this command disables the inversion of the data stream.

Configuring NRZI Format

All EIA/TIA-232 interfaces on the 4-Port Serial Interface SPA support non-return-to-zero (NRZ) and non-return-to-zero inverted (NRZI) formats. Both formats use two different voltage levels for transmission. NRZ signals maintain constant voltage levels with no signal transitions—no return to a zero voltage level—during a bit interval and are decoded using absolute values: 0 and 1. NRZI uses the same constant signal levels but interprets the absence of data—a space—at the beginning of a bit interval as a signal transition and the presence of data—a mark—as no signal transition. NRZI uses relational encoding to interpret signals rather than determining absolute values.

Use the following commands when configuring NRZI format:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. For further information, see the “Specifying the Interface Address on a SPA” section on page 18-7.
Router(config-if)# nrzi-encoding	Enables NRZI encoding.
Router(config-if)# no nrzi-encoding	Disables NRZI encoding.

Configuring Cyclic Redundancy Checks

Cyclic redundancy checking (CRC) is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. All interfaces use a 16-bit CRC (CRC-CITT) by default but also support a 32-bit CRC. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). The sender of a data frame calculates the frame check sequence (FCS). Before it sends a frame, the sender appends the FCS value to the message. The receiver recalculates the FCS and compares its calculation to the FCS from the sender. If there is a difference between the two calculations, the receiver assumes that a transmission error occurred and sends a request to the sender to resend the frame.

To set the length of the cyclic redundancy checks (CRC), use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. For further information, see the “Specifying the Interface Address on a SPA” section on page 18-7.
Router(config-if)# crc {16 32}	Specifies the length of the CRC, where: <ul style="list-style-type: none"> 16—Specifies a 16-bit length CRC. This is the default. 32—Specifies a 32-bit length CRC. To set the CRC length to the default value, use the no form of this command.

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Verifying the Configuration” section on page 18-2.
Router(config-if)# encapsulation <i>encapsulation-type {hdlc ppp frame-relay}</i>	Sets the encapsulation type on the interface. <ul style="list-style-type: none"> hdlc—High-Level Data Link Control (HDLC) protocol for serial interface. This is the default. ppp—Point-to-Point Protocol (PPP) (for serial interface). frame-relay—Frame Relay (for serial interface).

Verifying Encapsulation

Use the **show interfaces serial** command to display the encapsulation method:

```
Router# show interfaces serial13/1/1
```

```
Serial13/1/1 is up, line protocol is down
  Hardware is SPA-4XT-SERIAL
  MTU 1500 bytes, BW 2016 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent 13698, LMI stat recvd 0, LMI upd recvd 0, DTE LMI down
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input never, output 00:00:05, output hang never
  Last clearing of "show interface" counters 1d14h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 3
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  19344 packets output, 254168 bytes, 0 underruns
    0 output errors, 0 collisions, 2283 interface resets
    0 output buffer failures, 0 output buffers swapped out
  4566 carrier transitions
  RTS up, CTS up, DTR up, DCD up, DSR up
```

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For more information about managing your system image and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* publications for your Cisco IOS software release.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Routers configuration settings, you can use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your 4-Port Serial Interface SPA.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the 4-Port Serial Interface SPA, use the **show interfaces serial** command.

The following example provides sample output for the serial interface:

```
Router# show interface serial14/0/0
Serial14/0/0 is down, line protocol is down
Hardware is SPA-4XT-SERIAL
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    Reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
      RTS down, CTS down, DTR down, DCD down, DSR down
```

To find detailed status and statistical information on a per-port basis for the 4-Port Serial Interface SPA, use the **show controllers serial** command:

```
Router# show controllers serial 2/0/0
```

```

Serial2/0/0 - (SPA-4XT-SERIAL) is down
  Encapsulation : HDLC
  Cable type: RS-232 DTE
  mtu 1500, max_buffer_size 1524, max_pak_size 1656 enc 132
  loopback: Off,  crc: 16, invert_data: Off
  nrzi: Off, idle char: Flag
  tx_invert_clk: Off, ignore_dcd: Off
  rx_clockrate: 0, rx_clock_threshold: 0
  serial_restartdelay:60000,  serial_restartdelay_def:60000

  RTS up, CTS down, DTR up, DCD down, DSR down

```

Configuration Examples

This section includes the following configuration examples:

- [Inverting the Clock Signal Configuration Example, page 18-13](#)
- [NRZI Format Configuration Example, page 18-13](#)
- [Cyclic Redundancy Checks Configuration Example, page 18-13](#)
- [Encapsulation Configuration Example, page 18-14](#)
- [Distributed Multilink PPP Configuration Example, page 18-14](#)

Inverting the Clock Signal Configuration Example

The following example configures the interface to invert the clock signal:

```

Router(config-if)# interface serial3/0/0
Router(config-if)# invert txclock ?
<cr>
Router(config-if)# invert txclock
Router(config-if)# invert ?
  data      Invert data stream
  txclock   Invert transmit clock

Router(config-if)# invert data

```

NRZI Format Configuration Example

The following example configures the interface for NRZI format:

```

Router(config-if)# nrzi-encoding ?
<cr>

```

Cyclic Redundancy Checks Configuration Example

The following example configures the interface for 32-bit CRC error-checking:

```

Router(config-if)# crc ?
  16  crc word-size
  32  crc word-size

Router(config-if)# crc 32

```

Encapsulation Configuration Example

The following example configures Point-to-Point Protocol encapsulation method on the Serial SPA:

```
Router(config-if)# encapsulation ppp
```

Distributed Multilink PPP Configuration Example

The following example configures multilink Point-to-Point Protocol encapsulation method for port 0 of the Serial SPA in subslot 2 of the SIP in slot 1 of the router and sets the IP address and subnet mask:

```
Router(config)# interface multilink1
Router(config-if)# ip addr 10.0.0.1 255.255.255.0
Router(config)# interface serial3/2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp chap hostname X1
Router(config-if)# ppp multilink gr 1
```




CHAPTER 19

Configuring the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA

This chapter provides information about configuring the 1-Port Channelized OC-3/STM-1 SPA and the 1-Port Channelized OC-12/STM-4 SPA on the Cisco ASR 1000 Series Aggregation Services Routers. It includes the following sections:

- [Restrictions for Configuring the 1-Port Channelized OC-12/STM-4 SPA, page 19-1](#)
- [Configuration Tasks, page 19-2](#)
- [Verifying the Interface Configuration, page 19-25](#)
- [Configuration Examples, page 19-27](#)

For information about managing your system images and configuration files, refer to the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide* and *Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2*.

For more information about the commands used in this chapter, refer to the *Cisco IOS XE Software Command References* site on Cisco.com. For more information, see the [“Related Documentation” section on page -xxvi](#).

Restrictions for Configuring the 1-Port Channelized OC-12/STM-4 SPA

This chapter contains information for configuring two models of the channelized SPAs on the Cisco ASR 1000 Series Routers, but some features are not yet supported on both models.

Consider the following restrictions when configuring the 1-Port Channelized OC-12/STM-4 SPA on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.6:

- E3 and E1 framing and related functionality is not supported.
- Synchronous digital hierarchy (SDH) framing is not supported.
- Multilink Frame Relay (MLFR) is not supported.
- A maximum of 2000 NxDS0 channels are supported.

**Note**

Before Cisco IOS XE Release 3.1S, APS (Automatic Protection Switching) was not supported for POS SPAs. The Cisco IOS XE Release 3.1S implements 1+1 bidirectional SR APS feature support for POS SPAs. Hence, 1+1 bidirectional SR APS feature will be supported in Cisco IOS XE Release 3.1S and later releases for POS SPAs.

Configuration Tasks

This section describes how to configure the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA on the Cisco ASR 1000 Series Router, including required and optional configurations. It includes information about configuring the SPAs in either synchronous optical network (SONET) or synchronous digital hierarchy (SDH) framing modes.

**Note**

In Cisco IOS XE Release 2.6, only SONET framing is supported on the 1-Port Channelized OC-12/STM-4 SPA.

**Note**

The SDH mode is supported on 1-Port Channelized OC-12/STM-4 SPA from Cisco IOS XE Release 3.1.2 onwards.

It includes the following topics:

- [Specifying the Physical Address for Controller and Interface Configuration, page 19-2](#)
- [Required Configuration Tasks, page 19-3](#)
- [Optional Configurations, page 19-15](#)
- [Saving the Configuration, page 19-25](#)

Specifying the Physical Address for Controller and Interface Configuration

This section describes how to specify the physical location of the SIP, SPAs, and interfaces on the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA.

To specify the physical address for controller or interface configuration, use the **interface** and **controller sonet** commands, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed.
- *subslot*—Specifies the slot of the SIP where the SPA is installed.
- *port*—Specifies the SONET port number. There is only one port on a 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA, therefore the port number is always 0.

For example, if the 1-Port Channelized OC-3/STM-1 SPA or 1-Port Channelized OC-12/STM-4 SPA is installed in subslot 0 of a Cisco ASR 1000 SIP in slot 3 of the chassis, the controller configuration address is specified as **controller sonet 3/0/0**.

For channelized SPA configuration, the interface address format is: *slot/subslot/port:channel-group*, where:

- *channel-group*—Specifies the logical channel group assigned to the time slots within the T1 link.
- For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Naming the Interface

Interface names are automatically generated, and the format will be dependent on the mode each particular linecard is operating on. The name formats of the serial interface created are listed below.

Channelized T3 mode

If framing is SONET or SDH with au-3:

```
interface serial [slot/subslot/port][ds3\ds1]:[channel-group]
```

SONET Mode

- If framing is SONET and mode is vt-15:

```
interface serial [slot/subslot/port].[sts1/vtght1]:[channel-group]
```

- If framing is SONET and mode is CT3

```
interface serial [slot/subslot/port].[ds3/t1]:[channel-group]
```

- If framing is SONET and mode is T3:

```
interface serial [slot/subslot/port].[ds3]
```

SDH Mode

If the aug mapping is au-4, the au-4 value is always 1; if the aug mapping is au-3, then the only supported mode is c-11 (carrying a T1).

- If SDH-AUG mapping is au-4 and if the tug-3 is mode t3/e3:

```
interface serial [slot/subslot/port].[au-4/tug-3/tug-2/e1]:[channel-group]
```

- If SDH-AUG mapping is au-3:

```
interface serial [slot/subslot/port/au-3/tug-2/t1]:[channel-group]
```

POS on the 1-Port Channelized OC-12/STM-4 SPA

If framing is SONET and *n* is from 1-12:

```
interface pos slot/subslot/port:nsts-1
```

Required Configuration Tasks

This section lists the required configuration steps to configure the 1-Port Channelized OC-3/STM-1 SPA. Some of the required configuration commands implement default values that might be appropriate for your network.

This section includes the following topics:

- [Configuring the Controller for SONET or SDH Mode, page 19-4](#)
- [Configuring SONET Mode, page 19-4](#)
- [Configuring SDH Mode, page 19-6](#)
- [Configuring Channelized DS3 Mode, page 19-8](#)

- [Configuring DS1 \(Channelized T3 mode\), page 19-9](#)
- [Configuring E1 \(Channelized T3/E3 mode\), page 19-12](#)
- [Configuring Unchannelized E3 Serial Interface, page 19-13](#)
- [Verifying the Interface Configuration, page 19-14](#)

Configuring the Controller for SONET or SDH Mode

Controller configuration is required for both SONET and SDH framing modes. To configure the controller on the 1-Port Channelized OC-3/STM-1 SPA or 1-Port Channelized OC-12/STM-4 SPA, complete the following step:

Command	Purpose
Router(config)# controller sonet <i>slot/subslot/port</i>	<p>Selects the controller to configure and enters controller configuration mode, where:</p> <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the interface. <p>Note The port number is always zero on the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA.</p>

Configuring SONET Mode

To configure SONET mode, complete the following steps:

	Command	Purpose
Step 1	Router(config-controller)# framing sonet	Specifies SONET as the frame type. This is the default.
Step 2	Router(config-controller)# clock source { internal line }	<p>Sets the clock source, where:</p> <ul style="list-style-type: none"> • internal—Specifies that the internal clock source is used. • line—Specifies that the network clock source is used. This is the default for T1 and E1.
Step 3	Router(config-controller)# loopback { local network }	<p>Enables or disables loopback mode on a SONET controller, where:</p> <ul style="list-style-type: none"> • local loopback—Loops data from the transmit path to the receive path. • network loopback—Loops data received on the external port to the transmit path and back out the external port. <p>The default is disabled loopback.</p>

	Command	Purpose
Step 4	Router(config-controller)# sts-1 <i>sts1</i> -#	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS1 configuration mode, where: <ul style="list-style-type: none"> <i>sts-1 #</i>—Number from 1 to 3 for the 1-Port Channelized OC-3/STM-1 SPA, and 1 to 12 for the 1-Port Channelized OC-12/STM-4 SPA.
Step 5	Router(config-ctrlr-sts1)# mode { ct3 ct3-e1 t3 vt-15 }	Specifies the mode of operation of an STS-1 path, where: <ul style="list-style-type: none"> ct3—A STS-1 carrying a DS3 signal is divided into 28 T1s (Plesiochronous Digital Hierarchy [PDH]). ct3-e1—The channelized T3 is carrying E1 circuits. t3—STS-1 carries an unchannelized (clear channel) T3. vt-15—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each VTG is then divided into four VT1.5's, each carrying a T1. <p>Note In Cisco IOS XE Release 2.6, ct3-e1 is not supported on the 1-Port Channelized OC-12/STM-4 SPA.</p>
Step 6	Router(config-ctrlr-sts1)# vtg <i>vtg#</i>	Configures the T1 on the VTG, where: <ul style="list-style-type: none"> <i>vtg#</i>—Specifies the VTG number. For SONET framing, values are 1 to 7.

Configuring SDH Mode


Note

In Cisco IOS XE Release 2.6, SDH mode is not supported on the 1-Port Channelized OC-12/STM-4 SPA.


Note

The SDH mode is supported on 1-Port Channelized OC-12/STM-4 SPA from Cisco IOS XE Release 3.1.2 onwards.

To configure SDH mode, complete the following steps:

	Command	Purpose
Step 1	Router(config-controller)# framing sdh	Specifies SDH as the frame type.
Step 2	Router(config-controller)# aug mapping {au-3 au-4}	<p>Configures AUG mapping for SDH framing.</p> <p>If the AUG mapping is configured to be AU-4, then the following muxing, alignment, and mapping will be used: TUG-3 <--> VC-4 <--> AU-4 <--> AUG</p> <p>If the mapping is configured to be AU-3, then the following muxing, alignment, and mapping will be used: VC-3 <--> AU-3 <--> AUG</p> <p>Default is au-4.</p>
Step 3	Router(config-controller)# clock source {internal line}	<p>Sets the clock source, where:</p> <ul style="list-style-type: none"> internal—Specifies that the internal clock source is used. line—Specifies that the network clock source is used. This is the default for T1 and E1.

	Command	Purpose
Step 4	<p>Router(config-controller)# au-4 <i>au-4</i># tug-3 <i>tug-3</i>#</p> <p>or</p> <p>Router(config-controller)# au-3 <i>au-3</i>#</p>	<p>Configures AU-3, AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode.</p> <p>Depending on the framing mode of SONET or SDH, each STS-1, AU-3, TUG-3, and AU-4 of a 1-Port Channelized OC-3/STM-1 SPA can be configured with one of these commands.</p> <p>Depending on currently configured AUG mapping setting, this command further specifies TUG-3, AU-3, AU-4 or STS-1 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode), config-ctrlr-au3 (SDH mode), or config-ctrlr-sts1 parser mode (SONET mode), which makes only relevant commands visible.</p> <ul style="list-style-type: none"> • <i>au-4</i>#—Range is from 1 to 4. • <i>tug-3</i>#—Range is from 1 to 3. • <i>au-3</i># —Range is from 1 to 12.
Step 5	<p>In SDH framing in AU-4 mode:</p> <p>Router(config-ctrlr-tug3)# mode {c-11 c-12 t3 e3}</p> <p>In SDH framing AU-3 mode:</p> <p>Router(config-ctrlr-au3)# mode {c-11 c-12 t3 e3 ct3 ct3-e1}</p>	<p>Configures mode of operation for AU-3 or AU-4 mode, where:</p> <p>C-11 and C-12 are container level-n (SDH) channelized T3s. They are types of T3 channels that are subdivided into 28 T1 channels.</p> <ul style="list-style-type: none"> • c-11—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2s. Each TUG-2 is then divided into four TU11s, each carrying a C-11 T1. • c-12—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2. Each TUG-2 is then divided into three TU12s, each carrying a C-12 E1. • t3—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) T3. • e3—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) E3. • ct3—Specifies an AU-3 carrying a DS3 signal divided into 28 T1s Plesiochronous Digital Hierarchy [PDH]). • ct3-e1—Specifies a channelized T3 carrying E1 circuits.

Configuring Channelized DS3 Mode

To configure channelized DS3 mode, complete the following steps:

	Command	Purpose
Step 1	Router(config)# controller sonet <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode, where: <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 2	Router(config-controller)# sts-1 <i>sts1-#</i>	Selects STS mode and enters sts1 configuration mode. <ul style="list-style-type: none"> <i>sts-1#</i>—A value from 1 to y, y being the SONET STS level.
Step 3	Router(config-ctrlr-sts1)# t3 framing { c-bit m23 auto-detect }	Specifies the framing mode, where: <ul style="list-style-type: none"> c-bit—Specifies C-bit parity framing. m23—Specifies M23 framing. auto-detect—Detects the framing type of the device at the end of the line and switches to that framing type. If both devices are set to auto-detect, c-bit framing is used. This is the default.
Step 4	Router(config-ctrlr-sts1)# t3 clock source { internal line }	Sets the clock source, where: <ul style="list-style-type: none"> internal—Specifies that the internal clock source is used. line—Specifies that the network clock source is used. This is the default. <p>Note The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal.</p>
Step 5	Router(config-ctrlr-sts1)# t3 loopback { local network [line payload] remote [line payload] }	Enables or disables loopback mode on a SONET controller, where: <ul style="list-style-type: none"> local loopback—Loops data from the transmit path to the receive path. network loopback—Loops data received on the external port to the transmit path and back out the external port. remote loopback—Applicable only to c-bit framing. <p>The default is no loopback.</p>

	Command	Purpose
Step 6	Router(config-ctrlr-sts1)# t3 mdl string { eic fic generator lic pfi port unit } <i>string</i>	<p>Configures maintenance data link (MDL) support parameters, where:</p> <ul style="list-style-type: none"> • eic—Specifies equipment ID code. • fic—Specifies frame ID code. • generator—Specifies the generator number in MDL test signal. • lic—Specifies location ID code. • pfi—Specifies the Path Facility Identification code in MDL the path message. • port— Specifies the port number in the MDL idle string message. • unit—Specifies unit identification code. • <i>string</i>—Specifies user identifier for the chosen support parameter. <p>The default is no mdl string.</p>
Step 7	Router(config-ctrlr-sts1)# t3 mdl transmit { path idle-signal test-signal }	<p>Configures MDL transmit parameters, where:</p> <ul style="list-style-type: none"> • path—Enables MDL path message transmission. • idle-signal—Enables MDL idle signal message transmission. • test-signal—Enables MDL test-signal message transmission. <p>The default is no mdl transmit.</p>
Step 8	Router(config-ctrlr-sts1)# t3 equipment { customer network } loopback	<p>Enables the port to honor remote loopback request. Equipment network loopback disables this functionality.</p> <p>Note Remote loopbacks are only available in c-bit framing mode.</p>
Step 9	Router(config-ctrlr-sts1)# t3 bert pattern <i>pattern</i> interval <i>1-14400</i>	<p>Enables Bit Error Rate Testing (BERT), where:</p> <ul style="list-style-type: none"> • <i>pattern</i>—Specifies the length of the repeating BERT test pattern. Allowed values are 0s, 1s, 2^15, 2^20, 2^23, and alt-0-1. • interval—Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.

Configuring DS1 (Channelized T3 mode)

To configure DS1, complete the following steps:

	Command	Purpose
Step 1	Router(config)# controller sonet slot/subslot/port	Selects the controller to configure and enters controller configuration mode, where: <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 2	Router(config-controller)# sts-1 sts-1#	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS configuration mode, where: <ul style="list-style-type: none"> <i>sts-1#</i>—STS values are 1 to 3.
Step 3	Router(config-ctrlr-sts1)# mode {ct3 vt-15}	Specifies the mode of operation of an STS-1 path, where: <ul style="list-style-type: none"> ct3—A STS-1 carrying a DS31 signal is divided into 28 T1s (Plesiochronous Digital Hierarchy [PDH]) vt-15—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each VTG is then divided into four VT1.5's, each carrying a T1.
Step 4	Router(config-ctrlr-sts1)# t1 t1# clock source {internal line}	Configures the clocking source, where: <ul style="list-style-type: none"> <i>t1#</i>—Number indicating the T1 channel. internal—Specifies that the internal clock source is used. line—Specifies that the network clock source is used. This is the default.
Step 5	Router(config-ctrlr-sts1)# t1 t1# fdl ansi	Enables the one-second transmission of the remote performance reports using Facility Data Link (FDL), where: <ul style="list-style-type: none"> <i>t1#</i>—Number indicating the T1 channel. fdl ansi—Specifies FDL and ANSI T1.403 standard. <p>Without this command, FDL runs in ATT, the default mode. ATT is the AT&T TR54016 standard.</p>
Step 6	Router(config-ctrlr-sts1)# t1 t1# framing {sf esf}	Specifies the type of framing, where: <ul style="list-style-type: none"> <i>t1#</i>—Number indicating the T1 channel. sf—Specifies that Super Frame (SF) is used as the T1 framing type. esf—Specifies that Extended Super Frame (ESF) is used as the T1 framing type.
Step 7	Router(config-ctrlr-sts1)# t1 t1# yellow {detection generation}	Enables detection and generation of DS1 yellow alarms, where: <ul style="list-style-type: none"> detection—Detects yellow alarms. generation—Generates yellow alarms.

	Command	Purpose
Step 8	Router(config-ctrlr-sts1)# t1 t1# channel-group channel-group# timeslots list-of-timeslots speed [56 64]	Configures a T1 or E1 interface, where: <ul style="list-style-type: none"> • <i>t1#</i>—Number indicating the T1 channel. • <i>channel-group#</i>—Specifies the channel-group number, from 0 to 23. • <i>list-of-timeslots</i>—Specifies one or more time slots. • speed [56 64]—(Optional) Specifies the line speed in kilobits per second. Valid values are 56 and 64.
Step 9	Router(config-ctrlr-sts1)# t1 t1# loopback [local network {line payload} remote {line {fdl {ansi bellcore} inband} payload [fdl] [ansi]}]	Enables specific t1 channels to loopback, where: <ul style="list-style-type: none"> • <i>t1#</i>—Number indicating the T1 channel. • local loopback—(Optional) Loops data from the transmit path to the receive path. • network loopback—(Optional) Loops data received on the external port to the transmit path and back out the external port. • remote line fdl {ansi bellcore}—(Optional) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word to the remote end requesting that it enter into a network line loopback. Specify the ansi keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel. Specify the bellcore keyword to enable the remote SmartJack loopback on the T1 channel. • remote line inband— (Optional) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback. • remote payload [fdl] [ansi]—(Optional) Sends a repeating, 16-bit ESF data link code word to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.
Step 10	Router(config-ctrlr-sts1)# t1 t1# shutdown	Shuts down the specified T1 channel, where: <ul style="list-style-type: none"> • <i>t1#</i>—Number indicating the T1 channel.

Configuring E1 (Channelized T3/E3 mode)


Note

In Cisco IOS XE Release 2.6, E1 is not supported on the 1-Port Channelized OC-12/STM-4 SPA.

E1 configuration must be done in channelized DS3 mode. To configure E1, complete the following steps:

	Command	Purpose
Step 1	Router(config-controller)# e1 <i>e1#</i> channel-group <i>channel-group#</i> timeslots <i>list-of-timeslots</i> speed [56 64]	Creates a logical channel group on an E1 line, where: <ul style="list-style-type: none"> • <i>e1#</i>—A number in the range of 1 to 3. • channel-group—Defines a logical channel group to be a channelized E1 line. • <i>channel-group#</i>—Specifies the channel group number. • <i>list-of-timeslots</i>—Specifies the number of timeslots that make up the E1 line. • speed [56 64]—Specifies the line speed in kilobits per second. Valid values are 56 and 64
Step 2	Router(config-controller)# e1 <i>e1#</i> unframed	Creates an E1 unframed (clear channel) logical channel group on an E1 line, where: <ul style="list-style-type: none"> • <i>e1#</i>—A number in the range of 1 to 3.
Step 3	Router(config-controller)# e1 <i>e1#</i> [unframed framing] {crc4 no-crc4}	Sets the type of framing (including unframed) used by an E1 line, where: <ul style="list-style-type: none"> • <i>e1#</i>—A number in the range of 1 to 3. • crc4—Specifies 4-bit cyclic redundancy check (CRC) framing. • no-crc4—Specifies basic framing.
Step 4	Router(config-controller)# e1 <i>e1#</i> clock source {internal line}	Sets the clock source on an E1 line, where: <ul style="list-style-type: none"> • internal—Specifies that the internal clock source is used. • line—Specifies the E1 line as the clock source.
Step 5	Router(config-controller)# e1 <i>e1#</i> national bits <i>pattern</i>	Sets the national reserved bits on an E1 line, where: <ul style="list-style-type: none"> • <i>e1#</i>—A number in the range of 1 to 3. • <i>pattern</i>—A hexadecimal value in the range 0x0 to 0x1F (hexadecimal) or 0 to 31 (decimal).

	Command	Purpose
Step 6	Router(config-controller)# e1 e1# loopback [local network]	Specifies a loopback on an E1 line, where: <ul style="list-style-type: none"> e1#—A number in the range of 1 to 3. local loopback—(Optional) Loops data from the transmit path to the receive path. network loopback—(Optional) Loops data received on the external port to the transmit path and back out the external port.
Step 7	Router(config-controller)# e1 e1# shutdown	Shuts down an individual E1 line, where: <ul style="list-style-type: none"> e1#—A number in the range of 1 to 3.

Configuring Unchannelized E3 Serial Interface



Note In Cisco IOS XE Release 2.6, E3 is not supported on the 1-Port Channelized OC-12/STM-4 SPA.



Note E3 channelization is not supported.

To configure an unchannelized E3 serial interface, complete the following:

	Command	Purpose
Step 1	Router(config-controller)# dsu mode {cisco digital-link kentrox}	Specifies the interoperability mode used by a T3 or E3 controller, where: <ul style="list-style-type: none"> cisco—Specifies cisco as the data service unit (DSU) mode. digital-link—Specifies Digital link as the DSU mode. Range is from 300-34010. kentrox—Specifies kentrox as the DSU mode. Range is 1000-24500, or 34010. The default is cisco .
Step 2	Router(config-controller)# dsu bandwidth number	Specifies the maximum allowed bandwidth in kbps, where: <ul style="list-style-type: none"> number—Allowed values are 0 to 34368. The default is 34368.
Step 3	Router(config-controller)# scramble	Enables scrambling for the E3 physical layer interface. The default is no scramble.
Step 4	Router(config-controller)# national bit {0 1}	Sets the national reserved bits on an E3 line. The default is 0.

	Command	Purpose
Step 5	Router(config-controller)# framing {bypass g751 g832}	Sets the framing on the interface, where: <ul style="list-style-type: none"> bypass—Configures framing bypass to use the full E3 bandwidth. g751— Specifies g751 framing. This is the default for E3. g832—Specifies g832 framing.
Step 6	Router(config-controller)# crc {16 32}	Selects the CRC size in bits, where: <ul style="list-style-type: none"> 16—16-bit CRC. This is the default 32—32-bit CRC.
Step 7	Router(config-controller)# loopback {network local remote}	Specifies loopback is enabled for the unchannelized E3 serial interface, where: <ul style="list-style-type: none"> local loopback—Loops data from the transmit path to the receive path. network loopback—Loops data received on the external port to the transmit path and back out the external port. remote loopback—Sends a far-end alarm control request to the remote end requesting that it enter into a network line loopback.
Step 8	Router(config-controller)# shutdown	Shuts down the E3 interface.
Step 9	Router(config-controller)# bert pattern pattern interval 1-14400	Sends a BERT pattern on an E3 line, where: <ul style="list-style-type: none"> pattern—Specifies the length of the repeating BERT test pattern. Allowed values are 2¹⁵, 2²⁰, 2²³, 0s, 1s, and alt-0-1. interval time—Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.

Verifying the Interface Configuration

Use the **show interface serial** command to verify the interface configuration:

```
Router# show interface serial 1/0/0.1/1:0
Serial1/0/0.1/1:0 is up, line protocol is up
  Hardware is SPA-1XCHSTM1/OC3
  Internet address is 10.1.1.1/16
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```

0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions no alarm present
VC 0: timeslot(s): 1, Transmitter delay 0, non-inverted data

```

Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your serial SPA.

- [Configuring Encapsulation, page 19-15](#)
- [Configuring the CRC Size for T1, page 19-16](#)
- [Configuring FDL, page 19-17](#)
- [Configuring FRF.12, page 19-18](#)
- [Configuring Multilink Point-to-Point Protocol \(Hardware-Based on the QFP\), page 19-18](#)
- [Configuring LFI, page 19-21](#)
- [Inverting Data on the T1/E1 Interface, page 19-21](#)
- [Inverting Data on the T1/E1 Interface, page 19-21](#)
- [Changing a Channel Group Configuration, page 19-22](#)
- [Configuring BERT, page 19-22](#)
- [Configuring QoS Features on Serial SPAs, page 19-24](#)

Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic. To set the encapsulation method, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port:channel-group</i>	<p>Selects the interface to configure and enters interface configuration mode.</p> <ul style="list-style-type: none"> • <i>slot/subslot/port:channel-group</i>—Specifies the location of the interface. <p>For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2. and “Naming the Interface” section on page 19-3.</p>

	Command	Purpose
Step 3	Router(config-if)# encapsulation <i>encapsulation-type {hdlc ppp frame-relay}</i>	Sets the encapsulation method on the interface, where: <ul style="list-style-type: none"> • hdlc—Sets the High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • ppp—Sets point-to-point protocol (PPP) for serial interface. • frame-relay—Sets Frame Relay (for serial interface).
Step 4	Router(config-if)# crc {16 32}	Selects the CRC size in bits, where: <ul style="list-style-type: none"> • 16—16-bit CRC. This is the default • 32—32-bit CRC.

Configuring the CRC Size for T1

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA uses a 16-bit cyclic redundancy check (CRC) by default, but also supports a 32-bit CRC. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

To set the length of the cyclic redundancy check (CRC) on a T1 interface, use these commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port:channel-group</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> • <i>slot/subslot/port:channel-group</i>—Specifies the location of the interface. For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2 and “Naming the Interface” section on page 19-3.
Step 3	Router(config-if)# crc {16 32}	Selects the CRC size in bits, where: <ul style="list-style-type: none"> • 16—16-bit CRC. This is the default. • 32—32-bit CRC.

Configuring FDL

Facility Data Link (FDL) is a 4-kbps channel provided by the Extended Super Frame (ESF) T1 framing format. The FDL performs outside the payload capacity and allows you to check error statistics on terminating equipment without intrusion. To configure FDL, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# controller sonet <i>slot/subslot/port</i>	Selects the controller to configure and enters controller configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 3	Router(config)# sts-1 sts-#	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS1 configuration mode, where: <i>sts-1#</i> —STS values are 1 to 3.
Step 4	Router(config-ctrlr-sts1)# mode { ct3 ct3-e1 t3 vt-15 }	Specifies the mode of operation of an STS-1 path, where: <ul style="list-style-type: none"> ct3—A STS-1 carrying a DS3 signal is divided into 28 T1s (Plesiochronous Digital Hierarchy [PDH]). ct3-e1—The channelized T3 is carrying E1 circuits. t3—STS-1 carries an unchannelized (clear channel) T3. vt-15—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each VTG is then divided into four VT1.5's, each carrying a T1.
Step 5	If vt-15 mode was selected: Router(config-ctrlr-sts1)# vtg <i>vtg#</i>	Configures the T1 on the VTG, where: <ul style="list-style-type: none"> <i>vtg#</i>—Specifies the VTG number. Values are 1 to 7.
Step 6	Router(config-ctrlr-sts1)# t1 t1# framing {sf esf}	Specifies the type of framing, where: <ul style="list-style-type: none"> <i>t1#</i>—Number indicating the T1 channel. sf—Specifies that Super Frame (SF) is used as the T1 framing type. esf—Specifies that Extended Super Frame (ESF) is used as the T1 framing type. Select esf to configure FDL.
Step 7	Router(config-ctrlr-sts1)# t1 t1# fdl ansi	Configures the format used for Facility Data Link (FDL) if the framing format was configured for esf , where: <ul style="list-style-type: none"> <i>t1#</i>—Number indicating the T1 channel. fdl ansi—Selects ANSI for FDL to use the ANSI T1.403 standard.

Verifying FDL

Use the **show controllers t1** command to verify the **fdl** setting:

```
Router# show controllers t1
```

```

T1 6/0/1 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Framing is ESF, FDL is ansi, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (742 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 73 15 minute intervals):
    1278491 Line Code Violations, 3 Path Code Violations,
    0 Slip Secs, 1 Fr Loss Secs, 177 Line Err Secs, 0 Degraded Mins,
    3 Errored Secs, 0 Bursty Err Secs, 1 Severely Err Secs, 227 Unavail Secs
.
.
.

```

Configuring FRF.12

The 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA support FRF.12 end-to-end fragmentation for Frame Relay. For information about how to configure Frame Relay fragmentation support, see the “Frame Relay Queueing and Fragmentation at the Interface” chapter of the *Cisco IOS XE Wide-Area Networking Configuration Guide*, Release 2 at:

http://www.cisco.com/en/US/docs/ios/ios_xe/wan/configuration/guide/wan_frque_frag_if_xe.html

Configuring Multilink Point-to-Point Protocol (Hardware-Based on the QFP)

Multilink Point-to-Point Protocol (MLPPP) allows you to combine interfaces which correspond to an entire T1 or E1 multilink bundle. You can choose the number of bundles and the number of T1 or E1 lines in each bundle in any any combination of E1, T1, and NxDS0 member links interfaces.

On the Cisco ASR 1000 Series Router, MLPPP functionality is implemented on the Quantum Flow Processor (QFP)—not the SPA. On other platforms that implement SPA-based MLPPP, the MLPPP member links must reside on the same SPA—this is not a restriction on the Cisco ASR 1000 Series Routers. QFP-based MLPPP supports member links in the MLPPP bundle across different SPAs and SIPs on the Cisco ASR 1000 Series Routers.

For more information about configuring MLPPP in Cisco IOS XE software, see the “[Configuring Media-Independent PPP and Multilink PPP](#)” chapter of the *Cisco IOS XE Wide-Area Networking Configuration Guide, Release 2*.

This section includes the following topics:

- [MLPPP Configuration Guidelines, page 19-18](#)
- [Creating a Multilink Bundle, page 19-19](#) (required)
- [Assigning an Interface to a Multilink Bundle, page 19-19](#) (required)
- [Configuring Fragmentation Size and Delay on an MLPPP Bundle, page 19-20](#) (optional)
- [Disabling Fragmentation on an MLPPP Bundle, page 19-20](#) (optional)

MLPPP Configuration Guidelines

When configuring MLPPP, consider the following guidelines:

- Only T1, E1, or NxDS0 links are supported in a bundle. The configuration will not prohibit higher bandwidth links from being added to the bundle, but they are not supported.

- Links of differing bandwidths are supported in the same bundle.
- PPP encapsulation must be enabled before configuring multilink-related commands.

Creating a Multilink Bundle

To create a multilink bundle, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface multilink <i>group-number</i>	Creates a multilink interface and enters multilink interface mode, where: <ul style="list-style-type: none"> • <i>group-number</i>—The group number for the multilink bundle.
Step 3	Router(config-if)# ip address <i>address mask</i>	Sets the IP address for the multilink group, where: <ul style="list-style-type: none"> • <i>address</i>—The IP address. • <i>mask</i>—The IP netmask.

Assigning an Interface to a Multilink Bundle

To assign an interface to a multilink bundle, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode, where: <ul style="list-style-type: none"> • <i>slot/subslot/port</i>—Specifies the location of the controller. For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 3	Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
Step 4	Router(config-if)# ppp multilink group <i>group-number</i>	Assigns the interface to a multilink bundle, where: <ul style="list-style-type: none"> • <i>group-number</i>—The multilink group number for the T1 or E1 bundle.
Step 5	Router(config-if)# ppp multilink	Enables multilink PPP on the interface.
Step 6	Note Repeat these commands for each interface you want to assign to the multilink bundle.	

Configuring Fragmentation Size and Delay on an MLPPP Bundle

To configure the fragmentation size on a multilink PPP bundle, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface multilink <i>group-number</i>	Creates a multilink interface and enters multilink interface mode, where: <ul style="list-style-type: none"> <i>group-number</i>—The group number for the multilink bundle. Range 1-2147483647
Step 3	Router(config-if)# multilink fragment size <i>fragment-size</i>	Sets the fragmentation size in bytes. Fragmentation is disabled by default.
Step 4	Router(config-if)# ppp multilink fragment-delay <i>delay</i>	Sets the configured delay on the multilink bundle that satisfies the fragmentation size, where: <ul style="list-style-type: none"> <i>delay</i>—Delay in milliseconds.

The following example of the **show ppp multilink** command shows the MLPPP type and the fragmentation size:

```
Router# show ppp multilink
Multilink1, bundle name is test2
Bundle up for 00:00:13
Bundle is Distributed
0 lost fragments, 0 reordered, 0 unassigned
0 discarded, 0 lost received, 206/255 load
0x0 received sequence, 0x0 sent sequence
Member links: 2 active, 0 inactive (max not set, min not set)
Se4/2/0/1:0, since 00:00:13, no frags rcvd
Se4/2/0/2:0, since 00:00:10, no frags rcvd
Distributed fragmentation on. Fragment size 512. Multilink in Hardware..
```

Disabling Fragmentation on an MLPPP Bundle

By default, PPP multilink fragmentation is enabled. To disable fragmentation on a multilink bundle, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface multilink <i>group-number</i>	Specifies the multilink interface and enters multilink interface mode, where: <ul style="list-style-type: none"> <i>group-number</i>—The group number for the multilink bundle. Range 1-2147483647
Step 3	Router(config-if)# ppp multilink fragment disable	Disables PPP multilink fragmentation.

Configuring LFI

Link Fragmentation and Interleaving (LFI) is implemented on the QFP on the Cisco ASR 1000 Series Routers. QFP-based LFI supports LFI on a bundle with any number of links—from one link, up to the maximum number supported by the router. When using LFI on MLPPP, the QFP load balances the priority packets across all links in the bundle to minimize the latency on the priority interleaved traffic.

LFI Configuration Guidelines

When you configure LFI, consider the following guidelines:

- Configure LFI using the **ppp multilink interleave** command. For MLPPP, this is on the multilink interface.
- Configure and apply an output QoS service-policy that classifies the priority and non-priority traffic. For MLPPP, you can apply the output policy on the multilink interface.

LFI Restrictions

When you configure LFI, note the following restrictions:

- Virtual-template interfaces are not supported.
- Packet ordering is not guaranteed for priority traffic sent interleaved on an MLPPP bundle with multiple links.
- IP header compression (such as, cRTP, cUDP, or cTCP) is not supported on packets classified by QoS as priority packets when using LFI on an MLPPP bundle with multiple links. IP header compression requires packet ordering. LFI sends all priority packets using PPP encapsulation, which does not preserve packet order when there are multiple links in the bundle. If you must support IP header compression, then you should not configure LFI or you should not make the LFI traffic priority. MLP encapsulation on non-priority QoS classes does preserve packet ordering.

To configure LFI on a multilink interface, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface multilink group-number	Creates or specifies a multilink interface and enters multilink interface mode, where: <ul style="list-style-type: none"> • <i>group-number</i>—The group number for the multilink bundle. Range 1-2147483647
Step 3	Router(config-if) ppp multilink	Enables Multilink PPP.
Step 4	Router(config-if)# ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.

Inverting Data on the T1/E1 Interface

If the interface on the channelized SPA is used to drive a dedicated T1 line that does not have B8ZS encoding, you must invert the data stream on the connecting CSU/DSU or on the interface. Be careful not to invert data on both the CSU/DSU and the interface, as two data inversions will cancel each other out. To invert data on a T1/E1 interface, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port</i>	Selects the serial interface and enters interface configuration mode, where: <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 3	Router(config-if)# invert data	Inverts the data stream.

Use the **show running configuration** command to verify that invert data has been set:

```
router# show running configuration
interface Serial6/0/0:0
  no ip address
  encapsulation ppp
  logging event link-status
  load-interval 30
  invert data
  no cdp enable
  ppp chap hostname group1
  ppp multilink
  ppp multilink group 1
```

Changing a Channel Group Configuration

To alter the configuration of an existing channel group, the channel group needs to be removed first using the **no** form of the **channel-group** command. To remove an existing channel group, use the following commands:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface serial <i>slot/subslot/port</i>	Select the controller to configure and enters controller configuration mode, where: <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the controller. For addressing information, refer to the “Specifying the Physical Address for Controller and Interface Configuration” section on page 19-2.
Step 3	Router(config-controller)# no channel-group t1 t1-number	Selects the channel group you want to remove, where: <ul style="list-style-type: none"> <i>t1-number</i>—Channel-group number.

Configuring BERT

BERT (Bit-Error Rate Testing) is used for analyzing quality and for problem resolution of digital transmission equipments. BERT tests the quality of an interface by directly comparing a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

The BERT operation is data-intensive. Regular data cannot flow on the path while the test is in progress. The path is reported to be in alarm state when BERT is in progress and restored to a normal state after BERT has been terminated.

BERT Test Configuration Guidelines

When configuring BERT on the 1-Port Channelized OC-3/STM-1 SPA or 1-Port Channelized OC-12/STM-4 SPA, consider the following guidelines:

- Only DS1/T1 and DS3/T3 paths are supported on the 1-Port Channelized OC-12/STM-4 SPA.
- A maximum of 27 concurrent tests across all paths on the SPA is supported.

BERT Pattern Descriptions

Table 19-1 and Table 19-2 describe the supported BERT patterns on the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA.

Table 19-1 DS1/T1/E1 BERT Patterns

Pattern	Description
0s	All 0's in the test pattern (...000...).
1-in-8	8-bit test pattern where 1 out of 8 bits is set to 1.
1s	All 1's in the test pattern (...111...).
2^11	Pseudorandom 1 test pattern that is 2,048 bits in length.
2^15	Pseudorandom 1 O.151 test pattern that is 32,768 bits in length.
2^15-inverted	Pseudorandom 1 inverted O.151 test pattern that is 32,768 bits in length.
2^20-O153	Pseudorandom 1 O.153 test pattern that is 1,048,575 bits in length.
2^20-QRSS	Pseudorandom 1 quasi-random signal sequence (QRSS) 0.153 test pattern that is 1,048,575 bits in length.
2^23	Pseudorandom 1 O.151 test pattern that is 8,388,607 bits in length.
2^23-inverted	Pseudorandom 1 inverted O.151 test pattern that is 8,388,607 bits in length.
2^9	Pseudorandom 1 O.150 test pattern that is 511 bits in length.
3-in-24	24-bit test pattern where 3 out of 24 bits is set to 1.
alt-0-1	Repeating test pattern of alternating 0's and 1's (...01010...).

Table 19-2 DS3/T3/E3 BERT Patterns

Pattern	Description
0s	All 0's in the test pattern (...000...).
1s	All 1's in the test pattern (...111...).
2^15	Pseudorandom 1 O.151 test pattern that is 32,768 bits in length.
2^20	Pseudorandom 1 O.153 test pattern that is 1,048,575 bits in length.
2^23	Pseudorandom 1 O.151 test pattern that is 8,388,607 bits in length.
alt-0-1	Repeating test pattern of alternating 0's and 1's (...01010...).

To configure a BERT pattern for DS1/T1/E1, use one of the following commands:

**Note**

In Cisco IOS XE Release 2.6, E1 is not supported on the 1-Port Channelized OC-12/STM-4 SPA.

Command	Purpose
Router(config-controller)# t1 <i>channel-number</i> bert pattern <i>pattern interval time</i> or Router(config-ctrlr-sts1)# e1 <i>e1-number</i> bert pattern <i>pattern interval time</i>	Sends a BERT pattern on a line, where: <ul style="list-style-type: none"> • <i>channel-number</i>—Number identifying the specific T1 channel where you want to run BERT. • <i>e1-number</i> —Number identifying the specific E1 channel where you want to run BERT. • <i>pattern</i>—Specifies the type of repeating BERT test pattern. Supported values are 0s, 1s, 1-in-8, 2^11, 2^15, 2^15-inverted, 2^20-O.153, 2^20-QRSS, 2^23, 2^23-inverted, 2^9, 3-in-24, and alt-0-1. • interval time—Specifies the duration of the BERT test, in minutes. The range is 1 to 14400.

To configure a BERT pattern for DS3/T3/E3, use the following command in controller configuration mode:

Command	Purpose
Router(config-controller)# bert pattern {0s 1s 2^15 2^20 2^23 alt-0-1} interval time or Router(config-ctrlr-sts1)# bert pattern {0s 1s 2^15 2^20 2^23 alt-0-1} interval time	Sends a BERT pattern on the DS3 channel, where: <ul style="list-style-type: none"> • interval time—Specifies the duration of the BERT test, in minutes. The range is 1 to 14400.
	Note See Table 19-2 for pattern descriptions.

Configuring QoS Features on Serial SPAs

The SIPs and SPAs support many QoS features using modular QoS CLI (MQC) configuration. Since there are no serial SPA-specific QoS features, refer to your network processor documentation for QoS configuration information.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For more information about managing configuration files, refer to the *Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2* and *Cisco IOS Configuration Fundamentals Command Reference* publications.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 1000 Series Router configuration settings, you can use the **show interface serial** and the **show controllers sonet** commands to get detailed information on a per-port basis for your channelized SPA.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the channelized SPAs, use the **show interface serial** and **show controllers sonet** commands.

See the [“Verifying the Interface Configuration” section on page 14](#) for an example of the **show interface serial** command.

The following example provides sample output for interface port 0 on the SPA located in subslot 0 of the Cisco ASR 1000 SIP installed in slot 1 of a Cisco ASR 1000 Series Router:

```
Router#show controllers sonet 1/0/0

SONET 1/0/0 is up.
  Hardware is SPA-1XCHSTM1/OC3
  IO FPGA version: 1.7, HDLC Framer version: 0
  T3/T1 Framer(1) version: 1
  Sonet/SDH Framer version: 0
  SUBRATE FPGA version: 1.4
  HDLC controller available FIFO buffers 3760
  Applique type is Channelized Sonet/SDH

Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
SECTION:
  LOS = 0           LOF = 0           BIP(B1) = 85

SONET/SDH Section Tables
  INTERVAL      CV      ES      SES      SEFS
  23:15-23:20    0       0       0       0
  23:00-23:15    0       0       0       0
  22:45-23:00    85      1       1       0
Total of Data in Current and Previous Intervals
  22:45-23:20    85      1       1       0
```

```

LINE:
  AIS = 0          RDI = 1          REI = 65          BIP(B2) = 207
Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6

```

SONET/SDH Line Tables

INTERVAL	CV	ES	SES	UAS
23:15-23:20	0	0	0	0
23:00-23:15	0	0	0	0
22:45-23:00	272	1	0	5

Total of Data in Current and Previous Intervals

22:45-23:20	272	1	0	5
-------------	-----	---	---	---

.
.
.

SONET/SDH Path Tables

INTERVAL	CV	ES	SES	UAS
23:15-23:20	0	0	0	0
23:00-23:15	0	0	0	0
22:45-23:00	187382	2	0	0

Total of Data in Current and Previous Intervals

22:45-23:20	187382	2	0	0
-------------	--------	---	---	---

.
.
.

T3 1/0/0 Path 1 is up.

```

Hardware is SPA-1XCHSTM1/OC3
IO FPGA version: 1.7, HDLC Framers version: 0
T3/T1 Framer(1) version: 1
Sonet/SDH Framer version: 0
SUBRATE FPGA version: 1.4
HDLC controller available FIFO buffers 3760
Applique type is T3
No alarms detected.
MDL transmission is enabled

```

```

FEAC code received: No code is being received
Framing is C-BIT Parity, Cablelength is 224
Clock Source is Line
Equipment customer loopback
Data in current interval (346 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 0 LOS Defect Secs

```

.
.
.

CT3 1/0/0.2 is up.

```

Hardware is SPA-1XCHSTM1/OC3
IO FPGA version: 1.7, HDLC Framers version: 0
T3/T1 Framer(1) version: 1
Sonet/SDH Framer version: 0
SUBRATE FPGA version: 1.4

```

```

HDLC controller available FIFO buffers 3760
Applique type is Channelized T3 to T1
No alarms detected.
Framing is M23, Cablelength is 224
Clock Source is Internal
Equipment customer loopback
Data in current interval (356 seconds elapsed):
  0 Line Code Violations, 0 P-bit Coding Violation
  0 C-bit Coding Violation, 0 P-bit Err Secs
  0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
  0 Unavailable Secs, 0 Line Errored Secs
  0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  0 Severely Errored Line Secs
  0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
  0 CP-bit Far-end Unavailable Secs
  0 Near-end path failures, 0 Far-end path failures
  0 Far-end code violations, 0 FERF Defect Secs
  0 AIS Defect Secs, 0 LOS Defect Secs

```

(Remaining output omitted)

Configuration Examples

This section includes the following configuration examples:

- [T3 Framing Configuration Example, page 19-27](#)
- [Cyclic Redundancy Check Configuration Example, page 19-27](#)
- [Facility Data Link Configuration Example, page 19-28](#)
- [Invert Data on T1/E1 Interface Example, page 19-28](#)

T3 Framing Configuration Example

The following example configures framing on a T3 interface:

```

! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# controller sonet 3/0/0
!
! Select the STS mode.
!
Router(config-controller)# sts-1 2
!
!Select the framing mode.
!
Router(config-controller)# t3 framing m23

```

Cyclic Redundancy Check Configuration Example

The following example configures CRC on a T1 interface:

```

! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 2/0/0.1
!
! Specify the CRC type.

```

```
!  
Router(config-if)# crc 32
```

Facility Data Link Configuration Example

The following example configures FDL on a T1 interface:

```
! Specify the interface to configure and enter interface configuration mode.  
!  
Router(config)# interface serial 1/0/0.2  
!  
! Specify the T1 number and select fdl.  
!  
Router(config-controller)#t1 2 fdl ansi
```

Invert Data on T1/E1 Interface Example

The following example inverts the data on the serial interface:

```
! Specify the interface to configure and enter interface configuration mode.  
!  
Router(config)# interface serial 3/0/0.1/2/1:0  
!  
! Configure invert data.  
!  
Router(config-if)# invert data
```



CHAPTER 20

Troubleshooting the Serial SPAs

This chapter describes techniques that you can use to troubleshoot the operation of your serial SPAs. It includes the following sections:

- [General Troubleshooting Information, page 20-1](#)
- [Performing Basic Interface Troubleshooting, page 20-2](#)
- [Using Bit Error Rate Tests, page 20-15](#)
- [Using loopback Commands, page 20-18](#)
- [Using the Cisco IOS Event Tracer to Troubleshoot Problems, page 20-19](#)
- [Preparing for Online Insertion and Removal of a SPA, page 20-19](#)

The first section provides information about basic interface troubleshooting. If you are having a problem with your SPA, use the steps in the “[General Troubleshooting Information](#)” section on [page 20-1](#) to begin your investigation of a possible interface configuration problem.

To perform more advanced troubleshooting, see the other sections in this chapter.

For more information about troubleshooting serial lines, see the *Internetwork Troubleshooting Handbook* at http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm.

General Troubleshooting Information

This section describes general information for troubleshooting SIPs and SPAs. It includes the following sections:

- [Interpreting Console Error Messages, page 20-1](#)
- [Using debug Commands, page 20-2](#)
- [Using show Commands, page 20-2](#)

Interpreting Console Error Messages

To view the explanations and recommended actions for Cisco 7600 series router error messages, including messages related to Cisco 7600 series router SIPs and SPAs, refer to the *System Error Messages for Cisco IOS Release* publication for your Cisco IOS software release.

System error messages are organized in the documentation according to the particular system facility that produces the messages. The SIP and SPA error messages for serial SPAs use the following facility names:

- Cisco ASR 1000 Series SIP—ASR1000_SIP
- 2-Port and 4-Port Channelized T3 SPA—SPA_CHOC_DSX
- 2-Port and 4-Port Clear Channel T3/E3 Serial SPA—SPA_T3E3

Using debug Commands



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Along with the other **debug** commands supported on the Cisco 7600 series router, you can obtain specific debug information for SPAs on the Cisco 7600 series router using the **debug hw-module subslot** privileged EXEC command.

The **debug hw-module subslot** command is intended for use by Cisco technical support personnel. For information about other **debug** commands supported on the Cisco 7600 series router, refer to the *Cisco IOS Debug Command Reference* and any related feature documents for your Cisco IOS software release.

Using show Commands

There are several **show** commands that you can use to monitor and troubleshoot the SIPs and SPAs on the Cisco 7600 series router. This chapter describes using the **show interfaces** and **show controllers** commands to perform troubleshooting of your SPA.

For more information about **show** commands to verify and monitor SIPs and SPAs, see the following chapters of this guide:

- [Chapter 15, “Configuring the 8-Port Channelized T1/E1 SPA”](#)
- [Chapter 16, “Configuring the 2-Port and 4-Port Channelized T3 SPAs”](#)
- [Chapter 17, “Configuring the 2-Port and 4-Port Clear Channel T3/E3 SPAs”](#)
- [Chapter 18, “Configuring the 4-Port Serial Interface SPA”](#)
- [Chapter 19, “Configuring the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA”](#)

Performing Basic Interface Troubleshooting

You can perform most of the basic interface troubleshooting using the **show interfaces serial** command and examining several areas of the output to determine how the interface is operating.

The output of the **show interfaces serial** EXEC command displays information specific to serial interfaces.



Note The output of the **show interfaces serial** command will vary depending on the type of serial SPA.

This section describes how to use the **show interfaces serial** command to diagnose serial line connectivity problems in a wide-area network (WAN) environment. The following sections describe some of the important fields of the command output:

- [Serial Lines: show interfaces serial Status Line Conditions, page 20-3](#)
- [Serial Lines: Increasing Output Drops on Serial Link, page 20-7](#)
- [Serial Lines: Increasing Input Drops on Serial Link, page 20-8](#)
- [Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic, page 20-9](#)
- [Serial Lines: Troubleshooting Serial Line Input Errors, page 20-10](#)
- [Serial Lines: Increasing Interface Resets on Serial Link, page 20-13](#)
- [Serial Lines: Increasing Carrier Transitions Count on Serial Link, page 20-14](#)

Serial Lines: show interfaces serial Status Line Conditions

You can identify five possible problem states in the interface status line of the **show interfaces serial** display:

- Serial *x* is down, line protocol is down
- Serial *x* is up, line protocol is down
- Serial *x* is up, line protocol is up (looped)
- Serial *x* is up, line protocol is down (disabled)
- Serial *x* is administratively down, line protocol is down

The following example shows the interface statistics on the first port of a 4-Port Clear Channel T3/E3 SPA installed in subslot 0 of the SIP located in chassis slot 5:

Router# **show interfaces serial**

```
Serial5/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 110.1.1.2/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 234/255, rxload 234/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 40685000 bits/sec, 115624 packets/sec
  5 minute output rate 40685000 bits/sec, 115627 packets/sec
    4653081241 packets input, 204735493724 bytes, 0 no buffer
    Received 4044 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    4652915555 packets output, 204728203520 bytes, 0 underruns
    0 output errors, 0 applique, 4 interface resets
```

```

0 output buffer failures, 0 output buffers swapped out
2 carrier transitions

```

Table 20-1 shows the interface status conditions, possible problems associated with the conditions, and solutions to those problems.

Table 20-1 *Serial Lines: show interfaces serial Status Line Conditions*

Status Line Condition	Possible Problem	Solution
Serial <i>x</i> is up, line protocol is up	—	This is the proper status line condition. No action is required.
Serial <i>x</i> is down, line protocol is down	<p>The router is not sensing a carrier detect (CD) signal (that is, the CD is not active).</p> <p>The line is down or is not connected on the far end.</p> <p>Cabling is faulty or incorrect.</p> <p>Hardware failure has occurred in the channel service unit/data service unit (CSU/DSU).</p>	<ol style="list-style-type: none"> 1. Check the CD LEDs to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that you are using the proper cable (see your hardware installation documentation). 3. Insert a breakout box and check all control leads. 4. Contact your leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If you suspect faulty router hardware, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.

Table 20-1 **Serial Lines: show interfaces serial Status Line Conditions (continued)**


Status Line Condition	Possible Problem	Solution
Serial x is up, line protocol is down	<p>A local or remote router is misconfigured.</p> <p>Keepalives are not being sent by the remote router.</p> <p>A leased-line or other carrier service problem has occurred (noisy line or misconfigured or failed switch).</p> <p>A timing problem has occurred on the cable.</p> <p>A local or remote CSU/DSU has failed.</p> <p>Router hardware (local or remote) has failed.</p>	<p>1. Put the line in local loopback mode and use the show interfaces serial command to determine whether the line protocol comes up.</p> <p>Note If the line protocol comes up, a failed remote device is the likely problem.</p> <p>This solution will only work with High-Level Data Link Control (HDLC) encapsulation. For Frame Relay (FR) and Point-to-Point Protocol (PPP) encapsulation, a looped interface will always have the line protocol down. In addition, you may need to change the encapsulation to HDLC to debug this issue.</p> <p>2. If the problem appears to be on the remote end, repeat Step 1 on the remote interface.</p> <p>3. Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct remote termination point.</p> <p>4. Enable the debug serial interface EXEC command.</p> <p>Note First enable per-interface debugging using the command debug interface serial x, and depending on the encapsulation, enable the corresponding debug:</p> <p>For HDLC: debug serial interface For PPP: debug ppp negotiation For FR: debug frame-relay lmi</p> <p> Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p>

Table 20-1 **Serial Lines: show interfaces serial Status Line Conditions (continued)**

Status Line Condition	Possible Problem	Solution
		<ol style="list-style-type: none"> 5. If the line protocol does not come up in local loopback mode, and if the output of the debug serial interface EXEC command shows that the keepalive counter is not incrementing, a router hardware problem is likely. Swap router interface hardware. 6. If the line protocol comes up and the keepalive counter increments, the problem is <i>not</i> in the local router. 7. If you suspect faulty router hardware, change the serial line to an unused port. If the connection comes up, the previously connected interface has a problem.
Serial <i>x</i> is up, line protocol is up (looped)	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	<ol style="list-style-type: none"> 1. Use the show running-config privileged EXEC command to look for any loopback interface configuration command entries. 2. If you find a loopback interface configuration command entry, use the no loopback interface configuration command to remove the loop. 3. If you do not find the loopback interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. Reset the CSU or DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 5. If the CSU or DSU is not configured in manual loopback mode, contact the leased-line or other carrier service for line troubleshooting assistance.

Table 20-1 *Serial Lines: show interfaces serial Status Line Conditions (continued)*

Status Line Condition	Possible Problem	Solution
Serial <i>x</i> is up, line protocol is down (disabled)	<p>A high error rate has occurred due to a remote device problem.</p> <p>A CSU or DSU hardware problem has occurred.</p> <p>Router hardware (interface) is bad.</p>	<ol style="list-style-type: none"> 1. Troubleshoot the line with a serial analyzer and breakout box. Examine the output of show controller T1 or show controller T3 or show controller serial <i>x</i> depending on whether the SPA is an 8-Port Channelized T1/E1 SPA, 4-Port Channelized T3 SPA, or 4-Port Clear Channel T3/E3 SPA. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a telephone company problem. 3. Swap out bad hardware, as required (CSU, DSU, switch, local or remote router).
Serial <i>x</i> is administratively down, line protocol is down	<p>The router configuration includes the shutdown interface configuration command.</p> <p>A duplicate IP address exists.</p>	<ol style="list-style-type: none"> 1. Check the router configuration for the shutdown command. 2. Use the no shutdown interface configuration command to remove the shutdown command. 3. Verify that there are no identical IP addresses using the show running-config privileged EXEC command or the show interfaces EXEC command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

Serial Lines: Increasing Output Drops on Serial Link

Output drops appear in the output of the **show interfaces serial** command when the system is attempting to hand off a packet to a transmit buffer but no buffers are available.

Symptom: Increasing output drops on serial link

Table 20-2 outlines the possible problem that might cause this symptom and describes solutions to that problem.

Table 20-2 Serial Lines: Increasing Output Drops on Serial Link

Possible Problem	Solution
Input rate to serial interface exceeds bandwidth available on serial link	<div><div>1. Minimize periodic broadcast traffic, such as routing and Service Advertising Protocol (SAP) updates, by using access lists or by other means. For example, to increase the delay between SAP updates, use the ipx sap-interval interface configuration command.</div><div>2. Increase the output hold queue size in small increments (for instance, 25 percent), using the hold-queue out interface configuration command.</div><div>3. Implement priority queuing on slower serial links by configuring priority lists. For information on configuring priority lists, see the Cisco IOS configuration guides and command references for your Cisco IOS software release.</div><div>Note Output drops are acceptable under certain conditions. For instance, if a link is known to be overused (with no way to remedy the situation), it is often considered more preferable to drop packets than to hold them. This is true for protocols that support flow control and can retransmit data (such as TCP/IP and Novell Internetwork Packet Exchange [IPX]). However, some protocols, such as DECnet and local-area transport, are sensitive to dropped packets and accommodate retransmission poorly, if at all.</div></div>

Serial Lines: Increasing Input Drops on Serial Link

Input drops appear in the output of the **show interfaces serial EXEC** command when too many packets from that interface are still being processed in the system.

Symptom: Increasing number of input drops on serial link

Table 20-3 outlines the possible problem that might cause this symptom and describes solutions to that problem.

Table 20-3 **Serial Lines: Increasing Input Drops on Serial Link**

Possible Problem	Solution
Input rate exceeds the capacity of the router, or input queues exceed the size of output queues	<p>Note Input drop problems are typically seen when traffic is being routed between faster interfaces (such as Ethernet, Token Ring, and Fiber Distributed Data Interface [FDDI]) and serial interfaces. When traffic is light, there is no problem. As traffic rates increase, backups start occurring. Routers drop packets during these congested periods.</p> <ol style="list-style-type: none"> 1. Increase the output queue size on common destination interfaces for the interface that is dropping packets. Use the hold-queue number out interface configuration command. Increase these queues by small increments (for instance, 25 percent) until you no longer see drops in the show interfaces command output. The default output hold queue limit is 40 packets. 2. Reduce the input queue size, using the hold-queue number in interface configuration command, to force input drops to become output drops. Output drops have less impact on the performance of the router than do input drops. The default input hold queue is 75 packets.

Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic

If input errors appear in the **show interfaces serial** command output, there are several possible sources of those errors. The most likely sources, along with possible solutions, are summarized in [Table 20-4](#).



Note

Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts above 1 percent of the total interface traffic suggests some kind of link problem that should be isolated and repaired.

Symptom: Increasing number of input errors in excess of 1 percent of total interface traffic

Table 20-4 *Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic*

Possible Problem	Solution
<p>The following problems can result in this symptom:</p> <ul style="list-style-type: none">Faulty telephone company equipmentNoisy serial lineIncorrect clocking configurationIncorrect cable or cable that is too longBad cable or connectionBad CSU or DSUBad router hardwareData converter or other device being used between router and DSU	<p>Note We strongly recommend against the use of data converters when you are connecting a router to a WAN or a serial network.</p> <ol style="list-style-type: none">1. Use a serial analyzer to isolate the source of the input errors. If you detect errors, there likely is a hardware problem or a clock mismatch in a device that is external to the router.2. Use the loopback and ping tests to isolate the specific problem source.3. Look for patterns. For example, if errors occur at a consistent interval, they could be related to a periodic function, such as the sending of routing updates.

Serial Lines: Troubleshooting Serial Line Input Errors

Table 20-5 describes the various types of input errors displayed by the **show interfaces serial** command, possible problems that might be causing the errors, and solutions to those problems.

Table 20-5 **Serial Lines: Troubleshooting Serial Line Input Errors**

Input Error Type (Field Name)	Possible Problem	Solution
CRC errors (CRC)	<p>CRC errors occur when the CRC calculation does not pass (indicating that data is corrupted) for one of the following reasons:</p> <ul style="list-style-type: none"> • The serial line is noisy. • The serial cable is too long, or the cable from the CSU/DSU to the router is not shielded. • Serial clock transmit external (SCTE) mode is not enabled on the DSU. • The CSU line clock is incorrectly configured. • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). 	<ol style="list-style-type: none"> 1. Ensure that the line is clean enough for transmission requirements. Shield the cable, if necessary. 2. Make sure that the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). 3. Ensure that all devices are properly configured for a common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the “Configuring Invert Data” section on page 17-14 to invert the transmit clock signal. 4. Make certain that the local and remote CSU/DSU are configured for the same framing and coding scheme as that used by the leased-line or other carrier service (for example, Extended Superframe Format/binary eight-zero substitution [ESF/B8ZS]). 5. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.

Table 20-5 **Serial Lines: Troubleshooting Serial Line Input Errors (continued)**

Input Error Type (Field Name)	Possible Problem	Solution
Framing errors (frame)	<p>A framing error occurs when a packet does not end on an 8-bit byte boundary for one of the following reasons:</p> <ul style="list-style-type: none"> • The serial line is noisy. • The cable is improperly designed, the serial cable is too long, or the cable from the CSU or DSU to the router is not shielded. • SCTE mode is not enabled on the DSU, the CSU line clock is incorrectly configured, or one of the clocks is configured for local clocking. • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). 	<ol style="list-style-type: none"> 1. Ensure that the line is clean enough for transmission requirements. Shield the cable, if necessary. Make certain that you are using the correct cable. 2. Make sure that the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). 3. Ensure that all devices are properly configured to use a common line clock. Set SCTE on the local and remote DSU. 4. Make certain that the local and remote CSU/DSU are configured for the same framing and coding scheme as that used by the leased-line or other carrier service (for example, ESF/B8ZS). 5. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.

Table 20-5 *Serial Lines: Troubleshooting Serial Line Input Errors (continued)*

Input Error Type (Field Name)	Possible Problem	Solution
Aborted transmission (abort)	<p>Aborts indicate an illegal sequence of 1 bit (more than seven in a row).</p> <p>The following are possible reasons for this to occur:</p> <ul style="list-style-type: none"> • SCTE mode is not enabled on the DSU. • The CSU line clock is incorrectly configured. • The serial cable is too long, or the cable from the CSU or DSU to the router is not shielded. • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). • A packet was terminated in the middle of transmission (typical cause is an interface reset or a framing error or a buffer overrun). • A hardware problem has occurred (bad circuit, bad CSU/DSU, or bad sending interface on remote router). 	<ol style="list-style-type: none"> 1. Ensure that all devices are properly configured to use a common line clock. Set SCTE on the local and remote DSU. 2. Shield the cable, if necessary. Make certain that the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). Ensure that all connections are good. 3. Check the hardware at both ends of the link. Swap faulty equipment, as necessary. 4. Lower data rates and determine whether aborts decrease. 5. Use local and remote loopback tests to determine where aborts are occurring. 6. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.

Serial Lines: Increasing Interface Resets on Serial Link

Interface resets that appear in the output of the **show interfaces serial EXEC** command are the result of missed keepalive packets.

Symptom: Increasing interface resets on serial link

[Table 20-6](#) outlines the possible problems that might cause this symptom and describes solutions to those problems.

Table 20-6 *Serial Lines: Increasing Interface Resets on Serial Link*

Possible Problem	Solution
<p>The following problems can result in this symptom:</p> <ul style="list-style-type: none"> • Congestion on link (typically associated with output drops) • Bad line causing CD transitions • Possible hardware problem at the CSU, DSU, or switch 	<p>When interface resets are occurring, examine other fields of the show interfaces serial command output to determine the source of the problem. Assuming that an increase in interface resets is being recorded, examine the following fields:</p> <ol style="list-style-type: none"> 1. Check the Carrier Transitions field in the show interfaces serial command display. If carrier transitions are high while interface resets are being registered, the problem is likely to be a bad link or a bad CSU or DSU. Contact your leased-line or carrier service, and swap faulty equipment, as necessary. 2. Examine the Input Errors field in the show interfaces serial command display. If input errors are high while interface resets are increasing, the problem is probably a bad link or a bad CSU/DSU. Contact your leased-line or other carrier service, and swap faulty equipment, as necessary. <p>If there is a high number of output drops in the show interfaces serial output, see the “Serial Lines: Increasing Output Drops on Serial Link” section on page 20-7.</p>

Serial Lines: Increasing Carrier Transitions Count on Serial Link

Carrier transitions appear in the output of the **show interfaces serial EXEC** command whenever there is an interruption in the carrier signal (such as an interface reset at the remote end of a link).

Symptom: Increasing carrier transitions count on serial link

[Table 20-7](#) outlines the possible problems that might cause this symptom and describes solutions to those problems.

Table 20-7 *Serial Lines: Increasing Carrier Transitions Count on Serial Link*

Possible Problem	Solution
<p>The following problems can result in this symptom:</p> <ul style="list-style-type: none"> • Line interruptions due to an external source (such as physical separation of cabling, red or yellow T1 alarms, or lightning striking somewhere along the network) • Faulty switch, DSU, or router hardware 	<ol style="list-style-type: none"> 1. Check hardware at both ends of the link (attach a breakout box or a serial analyzer, and test to determine the source of problems). 2. If an analyzer or breakout box is incapable of identifying any external problems, check the router hardware. 3. Swap faulty equipment, as necessary.

Using Bit Error Rate Tests

BERT (Bit-Error Rate Testing) is used for analyzing quality and for problem resolution of digital transmission equipments. BERT tests the quality of an interface by directly comparing a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

The BERT operation is data-intensive. Regular data cannot flow on the path while the test is in progress. The path is reported to be in alarm state when BERT is in progress and restored to a normal state after BERT has been terminated.

BERT is built into most of the serial SPAs. With BER tests, you can test cables and signal problems in the field.

- For the 2-Port and 4-Port Channelized T3 SPA, you can configure individual T1 lines to run BER tests, but only one BER test circuit exists for all 28 T1 lines. Hence, only one BER test can be run on a single T3 port at any given time.
- For the 8-port Channelized T1/E1 SPA, there are six framer-assisted BERT engines, and six BER tests may run concurrently.
- For the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA, you can run a maximum of 27 concurrent tests across all paths on the SPA.

**Note**

BERT operation is data-intensive. Regular data cannot flow on the path while the test is in progress. The path is reported to be in alarm state when BERT is in progress and restored to a normal state after BERT has been terminated.

There are two categories of test patterns that can be generated by the onboard BER test circuitry: pseudorandom and repetitive. Pseudorandom test patterns are exponential numbers and conform to the CCITT/ITU O.151 and O.153 specifications; repetitive test patterns are all zeros, all ones, or alternating zeros and ones.

A description of the test patterns follows:

- Pseudorandom test patterns:
 - 2^{15} (per CCITT/ITU O.151)
 - 2^{20} (per CCITT/ITU O.153)
 - 2^{23} (per CCITT/ITU O.151)
 - QRSS (quasi-random signal sequence) (per CCITT/ITU O.151)
- Repetitive test patterns:
 - All zeros (0s)
 - All ones (1s)
 - Alternating zeros (0s) and ones (1s)

Table 20-8 provides information about some additional BERT patterns supported by some of the channelized SPAs on the Cisco ASR 1000 Series Routers:

Table 20-8 Additional BERT Pattern Support on the Channelized SPAs

Pattern	1-Port Channelized OC-3/STM-1 SPA	1-Port Channelized OC-12/STM-4 SPA	2-Port and 4-Port Channelized T3 SPA
1-in-8	Yes	Yes	Yes
3-in-24	Yes	Yes	Yes
2^9	Yes	Yes	Yes
2^11	Yes	Yes	Yes
2^15-inverted	Yes	Yes	Yes
2^20-QRSS	Yes	Yes	Yes
2^23-inverted	Yes	Yes	Yes
55Octet	Yes	No	Yes
55Daly	Yes	No	Yes
DS0-1, DS0-2, DS0-3, and DS0-4	Yes	No	Yes
Single Bit Error Injection	No	Yes	No

Both the total number of error bits received and the total number of bits received are available for analysis. You can set the testing period from 1 minute to 14,400 minutes (240 hours), and you can also retrieve the error statistics anytime during the BER test.

When running a BER test, your system expects to receive the same pattern that it is transmitting. To help ensure this:

- Use a loopback at a location of your choice in the link or network. To see how to configure a loopback, go to the [“Using loopback Commands”](#) section on page 20-18.
- Configure remote testing equipment to transmit the same BER test pattern at the same time.

Configuring a BER Test

To send a BER test pattern on an interface, use the **bert pattern** command. For more information, see [Chapter 19, “Configuring the 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA.”](#)

Viewing a BER Test

You can view the results of a BER test with the **show controllers** command.

You can view the results of a BER test at the following times:

- After you terminate the test using the **no bert** command.
- After the test runs completely.
- Anytime during the test (in real time).

```

Router# show controllers serial T3 1/0/0
T3 1/0/0 is up.
C2T3 H/W Version : 3, C2T3 ROM Version : 0.79, C2T3 F/W Version : 0.29.0
T3 1/0/0 T1 1
No alarms detected.
Clock Source is internal.
BERT test result (running)
  Test Pattern : 2^15, Status : Sync, Sync Detected : 1
  Interval : 5 minute(s), Time Remain : 5 minute(s)
  Bit Errors(Since BERT Started): 6 bits,
  Bits Received(Since BERT start): 8113 Kbits
  Bit Errors(Since last sync): 6 bits
  Bits Received(Since last sync): 8113 Kbits

```

Interpreting BER Test Results

Table 20-9 explains the output of the **show controllers** command.

Table 20-9 Interpreting BER Test Results

Field	Description
BERT test result (running)	Indicates the current state of the test. In this case, “running” indicates that the BER test is still in progress. After a test is completed, “done” is displayed.
Test Pattern : 2^15, Status : Sync, Sync Detected : 1	Indicates the test pattern you selected for the test (2^15), the current synchronization state (Sync), and the number of times synchronization has been detected during this test (1).
Interval : 5 minute(s), Time Remain : 5 minute(s)	Indicates the time the test takes to run and the time remaining for the test to run. If you terminate a BER test, you receive a message similar to the following: Interval : 5 minute(s), Time Remain : 2 minute(s) (unable to complete) “Interval: 5 minutes” indicates the configured run time for the test. “Time Remain : 2 minutes” indicates the time remaining in the test prior to termination. “(unable to complete)” signifies that you interrupted the test.
Bit Errors(Since BERT Started): 6 bits Bits Received(Since BERT start): 8113 Kbits Bit Errors(Since last sync): 6 bits Bits Received(Since last sync): 8113 Kbits	These four lines show the bit errors that have been detected versus the total number of test bits that have been received since the test started and since the last synchronization was detected.

Using loopback Commands

Loopback support is useful for testing the interface without connectivity to the network, or for diagnosing equipment malfunctions between the interface and a device. The 2-Port and 4-Port Clear Channel T3/E3 SPA supports both an internal and an external loopback mode. The external loopback mode requires the use of a loopback cable and implements a loopback through the transceiver on the SPA.

You can also configure an internal loopback without the use of a loopback cable that implements a loopback at the PHY device internally. By default, loopback is disabled.

To configure loopback, use the following commands:

Command	Purpose
Router# configure terminal	Enters global configuration mode.
T3/E3 Router(config)# interface serial <i>slot/subslot/port</i> T1/E1 Router(config)# controller <i>slot/subslot/port</i>	Selects the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <i>slot/subslot/port</i>—Specifies the location of the T3/E3 interface. <i>slot/subslot/port</i>—Specifies the location of the T1/E1 controller.
T3/E3 Router(config-if)# loopback { local dte network } { line payload } remote } T1/E1 Router(config-controller)# loopback { local [line payload] diag }	Specifies the loopback mode. <ul style="list-style-type: none"> local—Loops back after going through the framer toward the terminal. dte—Loops back after the LIU towards the terminal. network—Loops back towards the network. remote—Sends FEAC to set remote in loopback. line—Loops back toward network before going through framer. payload—Loops back toward network after going through framer. diag—Loops back after going through the HDLC controller towards the terminal.

Verifying Loopback Mode

The following example shows that local loopback is set:

```
Router# show interfaces serial 2/0/0
Serial2/0/0 is up, line protocol is up (looped)
  Hardware is SPA-4T3E3
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 255/255, txload 225/255, rxload 221/255
  Encapsulation FRAME-RELAY, crc 16, loopback set (local)
  Keepalive set (10 sec)
  LMI enq sent 13281, LMI stat recvd 13280, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 1, LMI stat sent 0, LMI upd sent 0
```

```
LMI DLCI 1023 LMI type is CISCO frame relay DTE
FR SVC disabled, LAPF state down
Broadcast queue 0/256, broadcasts sent/dropped 0/0, interface broadcasts 0
Last input 00:00:07, output 00:00:00, output hang never
Last clearing of "show interface" counters 1d12h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 612756
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 38446000 bits/sec, 109217 packets/sec
5 minute output rate 39023000 bits/sec, 110854 packets/sec
 14601577951 packets input, 642478074437 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
      0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 14545044296 packets output, 639982568049 bytes, 0 underruns
    0 output errors, 0 applique, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
rxLOS inactive, rxLOF inactive, rxAIS inactive
txAIS inactive, rxRAI inactive, txRAI inactive
```

Using the Cisco IOS Event Tracer to Troubleshoot Problems

This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, Route Processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

For more information about using the Event Tracer feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/evnttrcr.html

Preparing for Online Insertion and Removal of a SPA

The Cisco ASR 1000 Series Aggregation Services Routers support online insertion and removal (OIR) of the SIP, in addition to each of the SPAs. Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This means that a SIP can remain installed in the router with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see Chapter 5, “Troubleshooting the SIP”.



PART 6

Services Shared Port Adapters



CHAPTER 21

Overview of the Cisco WebEx Node for ASR 1000 Series

This chapter provides an overview of the release history, features, and MIB support for the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to in this document as the Cisco WebEx Node services shared port adapter (SPA).

This chapter includes the following sections:

- [Release History, page 21-1](#)
- [Displaying the SPA Hardware Type, page 21-6](#)
- [Supported Features, page 21-4](#)
- [Restrictions, page 21-4](#)
- [Supported MIBs, page 21-5](#)
- [Displaying the SPA Hardware Type, page 21-6](#)

Release History

Release	Modification
Cisco IOS XE Release 2.4	Support for the Cisco WebEx Node for ASR 1000 Series was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Overview of the Cisco WebEx Node SPA Environment

The Cisco WebEx Node is a SPA for the Cisco ASR 1000 Series Routers that integrates transparently with the Cisco WebEx collaboration cloud. The shared port adapter runs WebEx software that enables the module to act like a private extension of the WebEx service.

The Cisco WebEx Node for the Cisco ASR 1000 Series provides enhanced performance and reduced bandwidth consumption for WebEx web, voice over IP (VoIP), and video sessions in a large enterprise. This is achieved by extending the hosted Cisco WebEx collaboration cloud into a large enterprise by deploying primary software components of the WebEx platform to an embedded processor within the onsite router.

The Cisco WebEx Node SPA is a full-height SPA designed to run an application that is part of the Cisco WebEx Data Center. The Cisco WebEx node SPA improves the functionality of WebEx meeting services by adding the meeting servers into the SPA itself. This technology provides the following advantages:

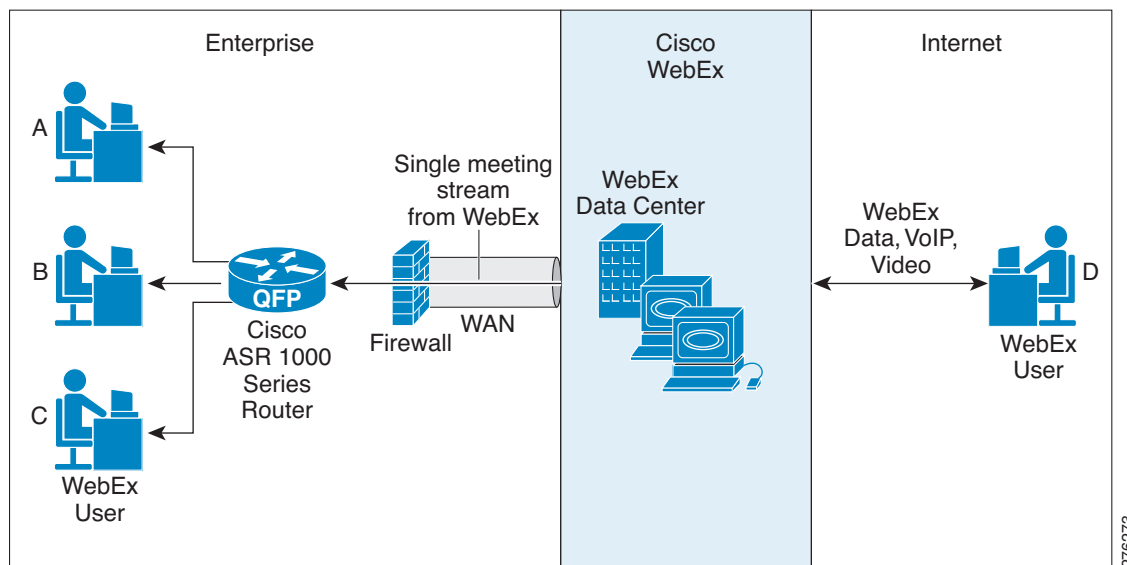
- Improves performance for users inside the company firewall.
- Reduces the bandwidth going out of the company firewall (to the WebEx Data Center).
- Provides better security by reducing traffic outside the company firewall.

Software that runs on the Cisco WebEx Node for the ASR 1000 Series includes Cisco WebEx collaboration cloud software components that are integral to meeting collaboration and voice and video conferencing. By moving these components and functions into the Cisco WebEx node SPA, the Cisco WebEx clients in the enterprise network need only connect to the Cisco WebEx node SPA. This reduces the traffic between the enterprise network and the Cisco WebEx Data Center, greatly reducing the customer's Internet bandwidth requirements.

By moving the switching components of the Cisco WebEx collaboration cloud into the Cisco WebEx Node for ASR 1000 Series, the Cisco WebEx clients in the enterprise network need only connect to the Cisco WebEx Node SPA. This reduces the traffic between the enterprise network and the Cisco WebEx Data Center, greatly reducing the customer's Internet bandwidth requirements, as shown in [Figure 21-1](#).

Instead of individual meeting streams from the Cisco WebEx Data Center to the enterprise, the use of the Cisco ASR 1000 Series router to implement some of the Cisco WebEx conferencing functions, allows for a single meeting stream from the Cisco WebEx Data Center to support enterprise conferencing traffic.

Figure 21-1 Cisco WebEx Network



Each Cisco WebEx node SPA can be configured to perform either web conferencing or voice/video conferencing, but not both features at the same time. Each Cisco WebEx node SPA uses the same software package that includes both features; the conferencing features that actually run on each SPA are determined by the Cisco WebEx Service Plan the customer has purchased. The WebEx Data Center retains the Cisco WebEx node SPA configuration files that the SPA retrieves each time the SPA boots. Multiple Cisco WebEx node SPAs can be installed on the same Cisco ASR 1000 Series Router to increase performance or to provide coverage for both media and video/VoIP sessions.

Cisco WebEx Node Management System

A web-based management tool located in the Cisco WebEx Data Center called the Cisco WebEx Node Management System (NMS) is available to access the following information through a web browser:

**Note**

For more information about getting started with the Cisco WebEx Node Management System, see [Chapter 22, “Configuring the Cisco WebEx Node for ASR 1000 Series.”](#)

For details about working with the Cisco WebEx Node Management System, refer to the *Cisco WebEx Node Management System Administrator's Guide*.

- Administration Account Management
 - Add or delete users and change passwords
 - Login history
- System Information
 - Memory usage and memory history (previous 24 hours)
 - CPU usage and CPU usage history (previous 24 hours)
 - Basic OS information
- Server Process Information
 - Check server version number on the SPA. Show the server version number in the Cisco WebEx Data Center.
 - Check server status
 - Number of server processes that are running and the up time
 - Memory and CPU usage of each server process
 - Server restart history for the last 30 days
- Cisco WebEx Meeting Information
 - Number of meetings on the SPA
 - Number of attendees on the SPA
 - Number of connections to the Cisco WebEx Data Center
 - Number of audio sessions on each multimedia platform.
 - Number of video sessions each multimedia platform.
 - Peak number of meetings and number of attendees in last 24 hours
- Server Management
 - Suspend, resume, or stop the server
 - Restart the server
- Troubleshooting and Support
 - Upload core and log files to Cisco WebEx Data Center
 - Turn on details traces
 - Performance information such as round trip time (RTT) to the top Cisco WebEx Data Center, RTT to client average, and so forth

- Test network connection to the Cisco WebEx Data Center.
- Configuration
 - Configure auto restart time

Supported Features

The Cisco WebEx Node for the ASR 1000 Series includes some of the following basic features:

- 4-GB RAM
- 250-GB hard disk drive, with self-monitoring, analysis, and reporting technology (SMART) support, for application data and system log storage
- Faceplate LEDs to indicate SPA status, hard disk drive activity, and system status
- A Shutdown button to stop hard drive access activity before removing the SPA to prevent data corruption
- Voltage and temperature monitoring
- Online insertion and removal (OIR)
- Downloadable configuration from the WebEx Data Center
- Support for web conferencing or voice and video conferencing, and up to 500 clients for media or 600 streams for mixed audio and multipoint video
- Secure Socket Layer (SSL) connection between the Cisco WebEx node SPA and the WebEx Data Center, and secure connection between the Cisco WebEx node SPA and Cisco WebEx clients
- Monitoring of the Cisco WebEx node SPA from the Cisco WebEx Data Center
- Automatic recovery for service failures on a Cisco WebEx Node SPA by another Cisco WebEx Node SPA, or by the Cisco WebEx collaboration cloud

For more detailed information about the hardware features and benefits of the Cisco WebEx Node for the Cisco ASR 1000 Series, refer to the product data sheet at:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10353/data_sheet_c78-530577.html

Restrictions

- Performance can be affected if there is a slow connection to the WebEx Data Center because communication between different Cisco WebEx node SPAs has to go through the WebEx Data Center.
- Before the Cisco WebEx node SPA is removed, the software and hard drive should be gracefully shut down, either using the Shutdown button or the **hw-module subslot stop** command.
- Either web conferencing or voice/video conferencing are supported, but not both on the same Cisco WebEx Node SPA.

Supported MIBs

The following MIBs are supported in Cisco IOS XE Release 2.4 for the Cisco WebEx node SPA on Cisco ASR 1000 Series Routers:

Common MIBs

- ENTITY-MIB
- IF-MIB
- MIB-II

Cisco-Specific Common MIBs

- CISCO-ENTITY-EXT-MIB
- OLD-CISCO-CHASSIS-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB

For more information about MIB support on a Cisco ASR 1000 Series Routers, refer to the *Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide*, at the following URL:

<http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1kmib.html>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Displaying the SPA Hardware Type

To verify the SPA hardware type that is installed in your Cisco ASR 1000 Series Routers, you can use the **show interfaces service-engine** or **show hw-module subslot service-engine status** command.

[Table 21-1](#) shows the hardware description that appears in the **show** command output for each Cisco WebEx node SPA that is supported on the Cisco ASR 1000 Series Routers.

Table 21-1 Cisco WebEx Node SPA Hardware Descriptions in show Commands

SPA	Description in show interfaces Command	Description in show hw-module subslot Command
Cisco WebEx Node for ASR 1000 SPA	“Hardware is SPA-WMA-K9”	“Service Engine is Cisco SPA-WMA-K9”

Example of the show interface service-engine Command

The following example shows output from the **show interfaces service-engine** command on a Cisco ASR 1000 Series Router with a Cisco WebEx Node SPA installed in subslot 0 of a SIP that is installed in slot 0:

```
Router# show interfaces Service-Engine 0/0/0
Service-Engine0/0/0 is up, line protocol is up
Hardware is SPA-WMA-K9
```

Example of the show hw-module subslot service-engine status Command

The following example shows output from the **show hw-module subslot service-engine status** command on a Cisco ASR 1000 Series Routers with a Cisco WebEx Node SPA installed in subslot 0 of a SIP that is installed in slot 0:

```
Router# show hw-module subslot 0/0 service-engine status
Service Engine is Cisco SPA-WMA-K9
```




CHAPTER 22

Configuring the Cisco WebEx Node for ASR 1000 Series

This chapter provides information about configuring the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to in this document as the Cisco WebEx Node SPA. This chapter includes the following sections:

- [Prerequisites, page 22-1](#)
- [Configuration Tasks, page 22-4](#)
- [Verifying the Service Engine Configuration, page 22-9](#)
- [Configuration Examples, page 22-10](#)

For information about managing your system images and configuration files, refer to the *Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2 and *Cisco IOS Configuration Fundamentals Command Reference* publications that correspond to your Cisco IOS XE software release.

Prerequisites

Complete the following prerequisites to successfully activate your Cisco WebEx Node for ASR 1000 Series:

- [Registering with the WebEx Data Center and the Cisco WebEx Node Management System, page 22-1](#)
- [Completing the Cisco WebEx Node SPA Configuration Prerequisites, page 22-4](#)

Registering with the WebEx Data Center and the Cisco WebEx Node Management System

To successfully activate a Cisco WebEx Node for ASR 1000 Series, certain registration and provisioning activities must be performed with the WebEx Data Center using the Cisco WebEx Node Management System. The Cisco WebEx Node Management System also provides monitoring and reporting for Cisco WebEx nodes.

Once the SPA is registered with the WebEx Data Center, certain node security information must be gathered and then configured on the Cisco WebEx Node for ASR 1000 Series.

**Note**

Registering your Cisco WebEx Node SPA and establishing an account in the Cisco WebEx Node Management System are two separate activities. If you are responsible for the management of Cisco WebEx Node SPAs for your enterprise, then it is likely that you will also acquire an account in the Cisco WebEx Node Management System application. Otherwise, you will work with your enterprise WebEx administrator to exchange the appropriate information to properly provision your Cisco WebEx Node SPA with the WebEx Data Center and configure it locally at the Cisco ASR 1000 Series Router.

**Note**

For details about working with the Cisco WebEx Node Management System, refer to the *Cisco WebEx Node Management System Administrator's Guide*.

Obtaining an Account in the Cisco WebEx Node Management System

If you will be monitoring and maintaining Cisco WebEx Node SPAs for your enterprise, then you will need to obtain an account in the Cisco WebEx Node Management System.

Consider the following important information about Cisco WebEx Node Management System accounts:

- You must change your password within 90 days. If you do not change your password, your account will move to “Inactive” status.
- If you do not successfully log in to the Cisco WebEx Node Management System after three attempts, the account moves to “Locked” status.

To acquire an account in the Cisco WebEx Node Management System, perform the following steps:

- Step 1** Contact your Cisco WebEx administrator with the following information to set up your initial account information:

**Note**

The first account associated with a Cisco WebEx Node SPA will already have the organization name automatically created by the WebEx provisioning team.

- User name—This name should be unique per organization.
- Password—Must contain at least 8 characters, a minimum of one mixed-case letters, and a minimum of one number. Your Cisco WebEx administrator will assign an initial password that you can change after logging into your account.
- Email address

- Step 2** Once your Cisco WebEx Node Management System account is created, you can log in to the application by going to the following URL:

<https://wma.webex.com>

- Step 3** On the login page for the Cisco WebEx Node Management System, enter your username and temporary password in the appropriate boxes.

**Note**

You can obtain login assistance by submitting your email address and your login information will be sent to you.

- Step 4** From the Account List page, go to the Edit Account page to change your password by checking the box next to your user account and click the pencil icon to access your account information page.

- Step 5** In the Password field, click the **Change Password** link to open the Change your password dialog box. Enter your old password, new password, and confirmation of your new password in the specified fields and click **OK**.
-

Registering a Cisco WebEx Node SPA in the Cisco WebEx Node Management System

This section describes the information required to perform initial activation of your Cisco WebEx Node SPA in the Cisco WebEx Node Management System.

**Note**

This task must be performed by a registered Cisco WebEx Node Management user. This could be someone in the role of a Cisco WebEx administrator for your enterprise, or multiple individuals responsible for Cisco WebEx Node management for your enterprise.

- Step 1** To register and provision your Cisco WebEx Node for ASR 1000 Series, contact your Cisco WebEx administrator with the following information to register your Cisco WebEx node SPA with the WebEx Data Center:
- Company name
 - Phone number (this number is used to uniquely identify a customer location, not as a number for actual contact)
 - Site name (for example, cisco.webex.com)
 - SPA serial number
 - Assigned hostname
 - Conferencing mode (either Web Conferencing or Voice and Video Conferencing)
- Step 2** Once the Cisco WebEx Node SPA has been registered in the Cisco WebEx Node Management System, you need to obtain the following information from the Node Information page for the SPA in the Cisco WebEx Node Management System:
- wma-passcode—Must match the value in the **service-engine wma-passcode** configuration command on the Cisco WebEx Node SPA.
 - wma-token—Must match the value in the **service-engine wma-token** configuration command on the Cisco WebEx Node SPA.
 - wma-url—The URL string from the Cisco WebEx Node Management System must be configured on the Cisco WebEx Node SPA using the **service-engine wma-url** command.

**Note**

This security information must be configured on the Cisco WebEx Node for ASR 1000 Series SPA using the CLI. For more information about configuring the CLI, see the [“Configuring the Virtual Service Engine Interface”](#) section on page 22-5.

Completing the Cisco WebEx Node SPA Configuration Prerequisites

Prior to configuring the Cisco WebEx Node SPA, you must ensure that the following tasks are completed:

- A Cisco IOS XE software image is loaded on your Cisco ASR 1000 Series Router that is compatible with the Cisco WebEx Node SPA. The Cisco WebEx Node SPA provides K9 encryption, and you must also download and install the optional “sipsawmak9” sub-package.

For more information about Cisco IOS XE package compatibility and installation instructions, see the [Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide](#).

- A DNS entry for the IP address is assigned to each Cisco WebEx Node SPA.
- An IP address is assigned for the Cisco IOS XE interface configuration on the Cisco ASR 1000 Series Router side.
- An IP address is also assigned for the internal interface configuration on the Cisco WebEx Node SPA side.
- A default gateway IP address is assigned for the SPA internal interface.
- The IP address that is assigned for the Cisco IOS XE interface configuration on the Cisco ASR 1000 Series Router side and the IP address that is assigned for the internal interface configuration on the Cisco WebEx Node SPA side must be on the same subnet.
- Verify that certain WebEx Data Center servers (such as the Cisco WebEx Data Center SSL gateway and the Cisco WebEx Node Management server) are reachable and not blocked from access by the Cisco ASR 1000 Series Router. If access to these servers is blocked, then the Cisco WebEx Node SPA might not activate properly.

Configuration Tasks

This section describes how to configure the Cisco WebEx Node for ASR 1000 Series and includes information about verifying the configuration.

It includes the following topics:

- [Specifying the Service Engine Interface Address on the Cisco WebEx Node SPA, page 22-4](#) (Required)
- [Configuring the Virtual Service Engine Interface, page 22-5](#) (Required)
- [Saving the Configuration, page 22-7](#) (Required)
- [Shutting Down and Removing the Cisco WebEx Node SPA, page 22-8](#) (Optional)

Specifying the Service Engine Interface Address on the Cisco WebEx Node SPA

To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot/subslot/port*, where:

- *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Routers where the SIP is installed.
- *subslot*—Specifies the subslot of the SIP where the SPA is installed.

- *port*—Specifies the number of the individual interface port, which is virtual and always 0 on the Cisco WebEx Node SPA.

The following example shows how to specify the service engine interface on a Cisco WebEx Node SPA installed in the first subslot of a SIP (0) installed in chassis slot 2:

```
Router(config)# interface service-engine 2/0/0
```

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for the SIP and SPAs” section on page 4-1](#).

Configuring the Virtual Service Engine Interface

Configuration of the Cisco WebEx Node SPA begins with the setup of a virtual service engine interface. This Cisco IOS XE virtual interface is created to allow services running on the Cisco WebEx Node SPA to communicate through the Cisco ASR 1000 Series Router with the Internet. The interface simulates a 2.5-GB Ethernet interface and facilitates the connection between the Cisco WebEx Data Center and Cisco WebEx clients.

A service-engine interface on the Cisco WebEx Node SPA has two IP addresses:

- Router-side IP address—Configured with the **ip address** command. The IP address on the router side acts like a gateway to the WebEx services running on the SPA side.
- Internal SPA interface IP address—Configured with the **service-engine ip address** command.

Virtual Service-Engine Interface Configuration Guidelines

To successfully configure the virtual service-engine interface, complete the following guidelines:

- The router-side IP address must be configured using the **ip address** command.
- The service-engine IP address must be on the same subnet as the router-side IP address for the service-engine interface (configured using the **ip address** command.)
- The **service-engine ip address** command must be configured before you configure the **service-engine default-gateway** command.
- The **service-engine default-gateway** IP address must match the router-side IP address.



Note

Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **no shutdown** command.

	Command	Purpose
Step 1	Router(config)# interface service-engine slot/subslot/0	Specifies the service engine interface to configure, where: <ul style="list-style-type: none"> • <i>slot/subslot/0</i>—Specifies the location of the interface. See the “Specifying the Service Engine Interface Address on the Cisco WebEx Node SPA” section on page 22-4. The port value is always 0.
Step 2	Router(config-if)# ip address router-side-ip-address	Specifies the IP address of the router-side interface.

	Command	Purpose
Step 3	Router(config-if)# service-engine ip address <i>module-side-ip-address</i> <i>subnet-mask</i>	Configures the Cisco WebEx Node SPA service engine IP address, where: <ul style="list-style-type: none"> <i>module-side-ip-address</i>—Specifies the IP address for the service engine interface. <i>subnet mask</i>—Specifies the mask for the associated IP subnet. Note The service-engine IP address must be on the same subnet as the router-side IP address for the service-engine interface.
Step 4	Router(config-if)# service-engine default-gateway <i>gateway-ip-address</i>	Specifies the IP address for the service engine default gateway. Note This IP address must match the IP address configured in the ip address command for the router-side IP address.
Step 5	Router(config-if)# service-engine nameserver <i>name-server1-ip-address</i> <i>name-server2-ip-address</i>	Specifies the primary and secondary domain name server that will be used by the WebEx Node SPA, where: <ul style="list-style-type: none"> <i>name-server1-ip-address</i>—Specifies the IP address of the primary domain name server. <i>name-server2-ip-address</i>—Specifies the IP address of the secondary domain nameserver.
Step 6	Router(config-if)# service-engine hostname <i>module-side-hostname</i> <i>module-side-domain-name</i>	Specifies the host name and domain name given to the Cisco WebEx Node SPA, where: <ul style="list-style-type: none"> <i>module-side-hostname</i>—Specifies the host name of the service engine interface. The default host name is “service-spa.” <i>module-side-domain-name</i>—Specifies the domain name of the service engine interface. Note The domain name must be assigned as a preliminary step. See the “Registering with the WebEx Data Center and the Cisco WebEx Node Management System” section on page 22-1.
Step 7	Router(config-if)# service-engine wma-url <i>url-string</i>	Specifies the URL provided by registration and provisioning of the SPA in the Cisco WebEx Node Management System. For more information, see the “Registering with the WebEx Data Center and the Cisco WebEx Node Management System” section on page 22-1.
Step 8	Router(config-if)# service-engine wma-token <i>token-string</i>	Specifies the encrypted token string provided by the Cisco WebEx Node Management System. Note The <i>token-string</i> must match the code provisioned in the Cisco WebEx Node Management System for the named SPA. For more information, see the “Registering with the WebEx Data Center and the Cisco WebEx Node Management System” section on page 22-1.

	Command	Purpose
Step 9	Router(config-if)# service-engine wma-passcode <i>name-string key-string</i>	Specifies the WebEx Node SPA name and key used for authentication, where: <ul style="list-style-type: none"> <i>name-string</i>—Specifies the SPA's assigned name. <i>key-string</i>—Specifies the password to use for encrypted authentication. <p>Note The <i>key-string</i> must match the passcode provisioned in the Cisco WebEx Node Management System for the named SPA. For more information, see the “Registering with the WebEx Data Center and the Cisco WebEx Node Management System” section on page 22-1.</p>
Step 10	Router(config-if)# no shutdown	Activates the interface.

The following is an example of the use of these configurations:

```
interface Service-Engine1/0/0
 ip address 10.200.72.17 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 service-engine ip address 10.200.72.18 255.255.255.252
 service-engine default-gateway 10.200.72.17
 service-engine nameserver 10.100.4.10 10.100.4.20
 service-engine hostname spawmal cisco.com
 service-engine wma-url https://wmabts.webex.com/wmams
 service-engine wma-token 45484b3e-8ea5-41e5-b050-49409006d14e
 service-engine wma-passcode SPAWMA1
0552055C271A4B5C4D5D424A5B5E007F73722B6B33264457125659500C0E555159
```



Note

Because the passcode is encrypted, the output will not reveal the configured token or passcode.

What To Do Next

Verify the configuration in the [“Verifying the Service Engine Configuration”](#) section on page 22-9.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

Command	Purpose
Router# copy running-config startup-config	Writes the new configuration to NVRAM.

For more information about managing your system images and configuration files, refer to the [Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2](#) and [Cisco IOS Configuration Fundamentals Command Reference](#) publications that correspond to your Cisco IOS XE software release.

Shutting Down and Removing the Cisco WebEx Node SPA

Because the Cisco WebEx Node SPA has a hard disk drive (HDD), it is necessary to shut down gracefully before physically removing the SPA from the Cisco ASR 1000 Series Router. This action allows the operating system to unmount the file system and put the HDD in standby mode to prevent data corruption or physical damage to the HDD.

The Cisco WebEx Node SPA can be shut down in one of two ways:

- You can use the **hw-module subslot stop** command to gracefully shut down the SPA before physically removing the hardware from the chassis. To shut down the Cisco WebEx Node SPA, use the following command in EXEC mode:

Command	Purpose
Router# hw-module subslot slot/subslot stop	Shuts down the Cisco WebEx Node SPA located in the slot and subslot locations indicated.

- You can use the Shutdown button located on the left side of the faceplate. Use the tip of a pen or other similar blunt object to press the button.

Once the shutdown operation is initiated by either method, the SYS LED starts to blink (green) to indicate the shutdown operation is in progress. Once the shutdown operation is completed, the SYS LED turns off to show that the SPA can now be removed.



Make sure to wait until the SYS LED turns off before removing the SPA.

The following example shows the use of the **hw-module subslot stop** command:

```
Router# hw-module subslot 0/0 stop
ASR1004#
*Feb 18 12:37:32.260: %SPA_OIR-6-OFFLINECARD: SPA (SPA-WMA-K9) offline in subslot 0/0
*Feb 18 12:37:32.260: %ASR1000_OIR-6-SOFT_STOPSPA: SPA(SPA-WMA-K9) stopped in subslot 0/0,
interfaces disabled

ASR1004# show platform
Chassis type: ASR1004
```

Slot	Type	State	Insert time (ago)
0	ASR1000-SIP10	ok	16:20:50
0/0	SPA-WMA-K9	stopped	00:00:13
0/1	SPA-WMA-K9	ok	16:18:32
R0	ASR1000-RP1	ok, active	16:20:50
F0	ASR1000-ESP10	ok, active	16:20:50
P0	ASR1004-PWR-AC	ok	16:19:23
P1	ASR1004-PWR-AC	ok	16:19:23

Slot	CPLD Version	Firmware Version
0	07091401	12.2(33r)XN2
R0	07062111	12.2(33r)XN2
F0	07051680	12.2(33r)XN2

Verifying the Service Engine Configuration

There are several commands that provide current information and status of the Cisco WebEx Node SPA, service engine, and other components.

Showing Cisco WebEx Node SPA Settings and Activity

You can use the **show interfaces service-engine** command to display Cisco WebEx Node SPA configuration settings and current activity. After configuration, be sure that the service-engine interface is “up” and the line protocol is “up” as shown in the following example:

```
Router# show interfaces service-engine 1/0/0
Service-Engine0/1/0 is up, line protocol is up
  Hardware is SPA-WMA-K9, address is 001f.6c25.bd10 (bia 001f.6c25.bd10)
  Internet address is 10.200.72.18/30
  MTU 1500 bytes, BW 2500000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:43:59, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    19 packets input, 1302 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    1091 packets output, 371289 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Showing Service Engine Status

To show service engine status including a listing of the applications that are active, use the **show hw-module subslot service-engine status** command as shown in the following example:

```
Router# show hw-module subslot 1/0 service-engine status
Service Engine is Cisco SPA-WMA-K9
Service Engine state: Steady (0x300)
Service Engine OS Version: 1.0.0, Application Version: 1.0.0

Application: WebEx Node (Web Conferencing)
Application Status: Online
Configuration:
  Int ip address: 10.200.72.18 , mask: 255.255.255.252
  GW ip address: 10.200.72.17
  Nameserver 1: 10.100.4.10 , Nameserver 2: 10.100.4.20
  Hostname: spawma1, Domain name: cisco.com
  WMA URL - https://wmabts.webex.com/wmams
  WMA Token - 45484b3e-8ea5-41e5-b050-49409006d14e
  WMA Passcode Name - cisco_test, key:0552055C271A4B5C4D5D424A5B5E007F
```

**Note**

Since the passcode and token are encrypted, the actual content is not displayed.

Verify that the service engine is reported in “Steady” state, and the Application Status is “Online.” If the Application Status is “Online,” then verify that the indicated operation mode (“Web Conferencing” or “Voice and Video Conferencing”) is correct. If not, contact Cisco WebEx Technical Support to correct the problem.

If the Application Status field is “Offline” then the operation mode (indicated in parenthesis in “Application” field) will show that it is not configured, as shown in the following sample output:

```
Router# show hw-module subslot 1/0 service-engine status
Service Engine is Cisco SPA-WMA-K9
Service Engine state: Steady (0x300)
Service Engine OS Version: 1.0.0, Application Version: 1.0.0

Application: WebEx Node (operation mode not configured)
Application Status: Offline
```

This occurs when the connection to the Cisco WebEx Data Center fails, and therefore provisioning information about the operation mode can not be retrieved. For more information about provisioning, see the [“Registering with the WebEx Data Center and the Cisco WebEx Node Management System” section on page 22-1](#). For additional troubleshooting information, refer to [Chapter 23, “Troubleshooting the Cisco WebEx Node for the ASR 1000 Series.”](#)

Configuration Examples

This section includes an example for configuring a Cisco WebEx Node SPA installed in a Cisco ASR 1000 Series Router:

```
Router# config t
Router(config)# interface service-engine 1/0/0
Router(config-if)# ip address 10.200.72.17 255.255.255.252
Router(config-if)# service-engine ip address 10.200.72.18 255.255.255.252
Router(config-if)# service-engine default-gateway 10.200.72.17
Router(config-if)# service-engine nameserver 10.100.4.10 10.100.4.20
Router(config-if)# service-engine hostname spawma1 cisco.com
Router(config-if)# service-engine wma-url https://wmabts.webex.com/wmams
Router(config-if)# service-engine wma-passcode spawma1 2b51221d2c08f405913bbec1eb9f6ec6
Router(config-if)# service-engine wma-token 45484b3e-8ea5-41e5-b050-49409006d14e
Router(config-if)# no shutdown
```



CHAPTER 23

Troubleshooting the Cisco WebEx Node for the ASR 1000 Series

This chapter describes techniques that you can use to troubleshoot the operation of the Cisco WebEx Node for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to in this document as the Cisco WebEx Node SPA.

- [General Troubleshooting Information, page 23-1](#)
- [Performing Basic Troubleshooting, page 23-8](#)
- [Using the Cisco IOS Event Tracer to Troubleshoot Problems, page 23-15](#)
- [Preparing for Online Insertion and Removal of a SPA, page 23-15](#)

For more information about troubleshooting your hardware installation, see also the *Cisco ASR 1000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide*.

General Troubleshooting Information

This section provides the following general information for troubleshooting the Cisco WebEx Node SPA:

- [Interpreting Console Error and System Messages, page 23-1](#)
- [Using show Commands, page 23-2](#)
- [Accessing the SIP and SPA Consoles for Troubleshooting, page 23-3](#)
- [Handling TraceBack and Core Dump Files on the Cisco WebEx Node SPA, page 23-5](#)

Interpreting Console Error and System Messages

To view the explanations and recommended actions for Cisco ASR 1000 Series Routers error messages, including messages related to Cisco ASR1000-SIP10 and SPAs, refer to the *System Messages for Cisco IOS XE*.

System error messages are organized in the documentation according to the particular system facility that produces the messages. The SIP and SPA error messages use the following facility names:

- Cisco ASR 1000 Series SIP:
 - ASR1000_SIP
 - ASR1000_SIP_SPA

- Cisco WebEx Node SPA:
 - SPA_SE1
 - SPA_WMA
- Cisco WebEx Node SPA Service Engine:
 - SPA_SRVCS_ENGINE
 - SPA_SRVCS_IF
- SPA Online Insertion and Removal—SPA_OIR

Using show Commands

There are several **show** commands, used in privileged EXEC mode, that you can use to monitor and troubleshoot the Cisco WebEx Node SPA on Cisco ASR 1000 Series Routers. For more information on these commands, refer to the Cisco IOS command references and see also the [“Performing Basic Troubleshooting”](#) section on page 23-8, and the “Verifying the Service Engine Configuration” section of the [“Configuring the Cisco WebEx Node for ASR 1000 Series”](#) chapter in this guide.

show Commands to Display Cisco WebEx Node SPA Status

- **show platform**—Displays the status of all modules installed in the Cisco ASR 1000 Series Router chassis. This command is not useful for out-of-service issues.
- **show hw-module subslot all oir**—Displays the OIR status of each Cisco WebEx Node SPA in the chassis. This command is useful for displaying out-of-service issues.
- **show hw-module subslot oir**—Displays the OIR status for a specified Cisco WebEx Node SPA.
- **show hw-module subslot service-engine status**—Displays the application and operational status and configuration of a specified Cisco WebEx Node SPA.

show Commands to Display Cisco WebEx Node SPA IDPROM

- **show diag subslot eeprom**—Displays main fields of the Cisco WebEx Node SPA IDPROM.
- **show diag subslot detail**—Display all the fields of the Cisco WebEx Node SPA IDPROM.
- **show diag subslot dump**—Dumps the content of the Cisco WebEx Node SPA IDPROM in hexadecimal format.

show Command to Display Cisco WebEx Node SPA Service Engine Status

The **show hw-module subslot service-engine status** command displays the operational status and configuration of the Cisco WebEx Node SPA. For successful configuration of the service-engine interface, the application status should be “Online.” You can also confirm the provisioned operation mode for the CiscoWex Node, which is “Web Conferencing” in the following example:

```
Router# show hw-module subslot 0/0 service-engine status
Service Engine is Cisco SPA-WMA-K9
Service Engine state: Steady (0x300)
Service Engine OS Version: 1.0.0, Application Version: 1.0.0

Application: WebEx Node (Web Conferencing)
Application Status: Online
```

Configuration:

```

Int ip address: 10.200.72.18 , mask: 255.255.255.252
GW ip address: 10.200.72.17
Nameserver 1: 10.100.4.10 , Nameserver 2: 10.100.4.20
Hostname: spawnma1, Domain name: cisco.com
WMA URL - https://wmabts.webex.com/wmams
WMA Token - 45484b3e-8ea5-41e5-b050-49409006d14e
WMA Passcode Name - cisco_test, key:0552055C271A4B5C4D5D424A5B5E007F

```

show Command to Display Cisco WebEx Node SPA FPD version

The **show hw-module all fpd** command displays the FPD version of each Cisco WebEx Node SPA in the Cisco ASR 1000 Series Router. The following example shows some sample output:

```
Router# show hw-module all fpd
```

```

=====
Slot Card Type                H/W   Field Programmable   Current   Min. Required
Ver.   Device: "ID-Name"   Version   Version
=====
0/0 SPA-WMA-K9                0.169 4-ADM1066            0.5       0.5
                    5-CPLD            1.2       1.2
                    1-Appl I/O FPGA   1.2       1.2
                    2-ROMMON          1.1       1.1
-----
0/1 SPA-5X1GE-V2              1.2   1-GE I/O FPGA        1.10      1.10
-----
0/3 SPA-2X1GE-V2              0.22  1-2xGE V2 I/O FPGA   1.1       1.1
-----
1/0 SPA-WMA-K9                0.133 4-ADM1066            0.5       0.5
                    5-CPLD            1.2       1.2
                    1-Appl I/O FPGA   1.2       1.2
                    2-ROMMON          1.1       1.1
-----
1/1 SPA-WMA-K9                0.165 4-ADM1066            0.5       0.5
                    5-CPLD            1.2       1.2
                    1-Appl I/O FPGA   1.2       1.2
                    2-ROMMON          1.1       1.1

```

show Command to Display Cisco WebEx Node SPA Error Messages on the RP Console

The **show logging** command displays the logged messages that have appeared on the RP console. The following is an example of a software error message that might appear when you run the **show logging** command:

```

Router# show logging
*May 22 17:11:58.712: %SPA_SRVCS_ENGINE-3-APP_MSG_ERR: SIP0/0: SPA-WMA-K9[0/0]: Connect
CWNMS server failed, check network availability to CWNMS server.

```

Accessing the SIP and SPA Consoles for Troubleshooting

Some troubleshooting for the Cisco WebEx Node SPA requires that you access the SIP or SPA consoles and run some commands to gather debug information or take other action. Under normal operation there is no need to access these consoles. However, sometimes it can be necessary to troubleshoot more complex problems and gather certain debug information.

Accessing the SIP Console

Use the **request platform software console attach** command to access the SIP console through the Cisco ASR 1000 Series Router RP console. The SIP console is used to collect debug information about the Cisco IOS code that is running on the SIP.

The following example shows how to access the SIP console and enter enable mode:

```
Router# request platform software console attach 0/0
#
# Connecting to the SPA console on 0/0.
# Enter Control-C to exit the console connection.
#
Router>enable
Router#
```

To exit the SIP console, enter **Control-C**.

Accessing the Cisco WebEx Node SPA Console

Use the **hw-module subslot service-engine session** command to access the Cisco WebEx Node SPA console through the Cisco ASR 1000 Series Router RP console. You will see a VEGAS Shell prompt and have access to the console commands.

Prerequisites

Before you can open a console session on a Cisco WebEx Node SPA, the SPA must first be configured with a minimum of the following commands and be in the “up” state:

- **ip address**
- **service-engine ip address**
- **service-engine default-gateway**

The **service-engine ip address** command must be configured before the **service-engine default-gateway** command.

Opening the Cisco WebEx Node SPA Console

The following example shows how to open the SPA console:



Note

The SPA console default prompt is “service-spa.” This prompt can be changed by configuring the **service-engine hostname** command.

```
Router# hw-module subslot 0/0 service-engine session

MontaVista(R) Linux(R) Carrier Grade Edition 5.0 (custom)
Linux/mips64 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be
Vegas Shell -- CGE 5.0 Version
      Copyright (c) 1985-2008 by Cisco Systems, Inc.
      All rights reserved.
service-spa#
```

Listing the Available Cisco WebEx SPA Console Commands

The Cisco WebEx SPA console supports a similar help function as the RP console. You can enter ? at the console to obtain a list of the available commands as shown in the following example:

```

service-spa# ?
Exec commands:
  clean      Clean commands
  copy       Copy files from src to destination
  delete     Remove files
  dir        Directory listing for files
  exit       Exit from the EXEC
  format     Format a device with ext3/fat16/dummy file system
  fsck       Perform file system check operation
  less       Shows content of file
  load       Load plug-in image
  mkdir      Create new directory
  move       Move files
  ping       Send echo messages
  rmdir      Remove existing directory
  show       Show system information
  terminal   Set terminal line parameters
  traceroute Trace route to destination
  webex      Webex Application Commands

```

Some of the most useful commands include:

- **show eventlog**—Dumps the content of the */var/log/messages* file.
- **show disk partitions**—Displays the partitions available on the hard disk drive (HDD).
- **show disk smart**—Displays S.M.A.R.T. output of the HDD.
- **show tech-support**—Gathers information for troubleshooting.
- **ping**—Sends echo messages.
- **copy tftp: disk0:**—Copies files from a TFTP server to the HDD first partition.
- **load**—Loads a plug-in image.
- **exit**—Exits from the Cisco WebEx Node SPA console.

Exiting the Cisco WebEx Node SPA Console

To exit the SPA console, use the **exit** command as shown in the following example:

```

service-spa# exit
Router#

```

Handling TraceBack and Core Dump Files on the Cisco WebEx Node SPA

This section describes how to gather traceback and core dump file information for troubleshooting by Cisco technical support.

Collecting Core Dump Files for the Cisco WebEx Node SPA

Linux utilities on the Cisco WebEx Node SPA and the WebEx application software can create core dump files when errors occur. When this happens an error message is logged on the RP console as shown in the following example:

```

*May 22 17:12:02.210: %SPA_SRVCS_ENGINE-2-APP_MSG_CRIT: SIP1/0: SPA-WMA-K9[1/0]: Core dump
generated for 'smartd' (corefile:smartd-626-11-1242970631.core.gz). If the problem
persists, contact your technical support representative for assistance.

```

The core file is saved on the hard disk on the Cisco WebEx Node SPA. Using commands from the Cisco WebEx Node SPA console, you can copy the file from the SPA to an external TFTP server. This file should be given to Cisco technical support as necessary for analysis of the problem.

To access the core dump file and copy it to a TFTP server, complete the following steps:

- Step 1** From the RP console, access the Cisco WebEx Node SPA console as shown in the following example:

```
Router# hw-module subslot 0/0 service-engine session
```

```
MontaVista(R) Linux(R) Carrier Grade Edition 5.0 (custom)
Linux/mips64 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be
```

```
Vegas Shell -- CGE 5.0 Version
Copyright (c) 1985-2008 by Cisco Systems, Inc.
All rights reserved.
```

```
service-spa#
```

- Step 2** From the Cisco WebEx Node SPA console, run the **dir core:** command to display the smartd file as shown in the following example:



Note The core dump file is compressed in gzip format before it is saved to the SPA hard disk.

```
service-spa# dir core:
```

```
1489726 May 22 05:37:27 2009 smartd-626-11-1242970631.core.gz
```

```
Usage for core: filesystem
221794304 bytes total used
1925689343 bytes free
2147483647 bytes total
```

- Step 3** Copy the core dump file from the SPA to a TFTP server as shown in the following example:



Note Copying the core file to a storage device on the RP is not supported.

```
service-spa# copy core:smartd-626-11-1242970631.core.gz tftp://dirt/tftpboot/username/
Trying to connect to tftp server.....
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
(some output has been removed to make this more readable)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
TFTP put operation was successful
```

```
1489726 bytes copied
service-spa# exit
```

```
Router#
```


Collecting Traceback Information for the Cisco WebEx Node SPA

Traceback information is generated during booting of the Cisco WebEx Node SPA and can be used to troubleshoot problems. You can access the traceback information from the SIP console.

No error messages are logged on the RP to indicate that a traceback event has occurred. These events are usually associated with other failures whose errors are reported on the RP console such as SYSINIT_FAILURE messages, as shown in the following example:

```
*May 1 07:46:32.650: %SPA_SE1-3-SYSINIT_FAILURE: SIP0/0: SPA-WMA-K9[0/0]: System init
failure was detected during bootup - application installation error. SPA will be disabled
because of this failure.
```

To collect traceback information for the Cisco WebEx Node SPA, complete the following steps:

- Step 1** From the RP console, access the SIP console and enter enable mode as shown in the following example:

```
Router# request platform software console attach 0/0
#
# Connecting to the SPA console on 0/0.
# Enter Control-C to exit the console connection.
#
Router> enable
Router#
```

- Step 2** From the SIP console, enter the **show hw-module subslot bay bootlog cpu-prev** or **show hw-module subslot bay bootlog cpu-last** commands to access the traceback from either the previous SPA boot (**cpu-prev** option) or last SPA boot (**cpu-last** option), as shown in the following examples:

```
Router# show hw-module subslot 0 bootlog cpu-last
% CPU boog log not available from last SPA-WMA-K9[0/0] bootup.
```

The following excerpt of a traceback shows a problem with the kernel that eventually causes the Cisco WebEx Node SPA to timeout. After 5 attempts to reload the Cisco WebEx Node SPA, the SPA enters an out-of-service state:



Note Some output has been removed to make the example more readable.

```
Router# show hw-module subslot 0 bootlog cpu-prev
----- CPU boot log from previous SPA-WMA-K9[0/0] bootup -----
Checking for the multiply/shift bug... no.
Checking for the daddi bug... no.
Checking for the daddiu bug... no.
CPU 0 Unable to handle kernel paging request at virtual address 0000000000000008,
epc == ffffffff8c029fb4, ra == ffffffff8c02a0bc
Oops[#1]:
Cpu 0
$ 0 : 0000000000000000 ffffffff8c4a3400 ffffffff8c4a5c00 ffffffff8c4a3400
$ 4 : 0000000000000028 0000000000000000 0000000000000000 0000000000000001
$ 8 : a800000414487e60 ffffffff8c00000000 0000000000000000 0000000000000000
$12 : 0000000000000000 0000000000000000 0000000000000000 0000000000000000
$16 : 0000000000000028 0000000000000000 0000000000000010 ffffffff8c4a5c70
$20 : 0000000000000001 0000000000000000 0000000000000000 0000000000000000
$24 : 0000000000000000 0000000000000000
$28 : a800000414484000 a800000414487e60 0000000000000000 ffffffff8c02a0bc
Hi : 0000000000000000
Lo : 0000000000000000
epc : ffffffff8c029fb4 octeon_unmask_ciu_irq+0x24/0x30 Not tainted
ra : ffffffff8c02a0bc octeon_irq_ciu_unmask+0x84/0xc8
Status: 10008ce2 KX SX UX KERNEL EXL
```

```

Cause : 00000008
BadVA : 0000000000000008
PrId : 000d030b
Modules linked in:
Process swapper (pid: 1, threadinfo=a800000414484000, task=a800000414481440)
Stack : 0000000000000001 0000000000000000 0000000000000028 a800000414469b80
        ffffffff8c4a5c00 ffffffff8c02a164 0000000000000001 ffffffff8c046a20
        ffffffff8c095c7c ffffffff8c095afc 0000000000000028 0000000000000080
        ffffffff8c0068d8 ffffffff8c0068d8 ffffffff8c40fa18 a800000414469b80
        ffffffff8c095dec ffffffff8c095dc0 0000000000000000 0000000000000000
        0000000000000000 0000000000000000 0000000000000000 0000000000000000
        ffffffff8c006be8 0000000000000000 ffffffff8c4c68b0 0000000000000000
        ffffffff8c4b1b24 0000000000000000 0000000000000000 0000000000000000
        a800000414484000 a800000414487fe0 0000000000000000 0000000000000000
        0000000000000000 0000000000000000 0000000000000000 0000000000000000

Call Trace:
[<fffffff8c029fb4>] octeon_unmask_ciu_irq+0x24/0x30
[<fffffff8c02a0bc>] octeon_irq_ciu_unmask+0x84/0xc8
[<fffffff8c02a164>] octeon_irq_ciu_startup+0x64/0x78
[<fffffff8c095c7c>] setup_irq+0x234/0x2b0
[<fffffff8c095dec>] request_irq+0xf4/0x118
[<fffffff8c006be8>] plat_prepare_cpus+0x98/0xe0
[<fffffff8c4c68b0>] smp_prepare_cpus+0xf8/0x140
[<fffffff8c4b1b24>] init+0x94/0x748
[<fffffff8c022808>] kernel_thread_helper+0x10/0x18
Code: 0061182d 0043102d dc460020 <dc90008> 03200008 00000000 7082fa32 3c030000
3c018c4a
Kernel panic - not syncing: Attempted to kill init!
Call Trace:
[<fffffff8c026570>] dump_stack+0x8/0x48
[<fffffff8c052220>] panic+0xb0/0x350
[<fffffff8c058a94>] do_exit+0xc7c/0xc80
[<fffffff8c02647c>] die+0x1ac/0x1b0
[<fffffff8c038034>] do_page_fault+0x1d4/0x480
[<fffffff8c01ff84>] ret_from_exception+0x0/0x10
[<fffffff8c029fb4>] octeon_unmask_ciu_irq+0x24/0x30
[<fffffff8c02a0bc>] octeon_irq_ciu_unmask+0x84/0xc8
[<fffffff8c02a164>] octeon_irq_ciu_startup+0x64/0x78
[<fffffff8c095c7c>] setup_irq+0x234/0x2b0
[<fffffff8c095dec>] request_irq+0xf4/0x118
[<fffffff8c006be8>] plat_prepare_cpus+0x98/0xe0
[<fffffff8c4c68b0>] smp_prepare_cpus+0xf8/0x140
[<fffffff8c4b1b24>] init+0x94/0x748
[<fffffff8c022808>] kernel_thread_helper+0x10/0x18
----- End of CPU previous boot log -----

```

Performing Basic Troubleshooting

This section includes the following topics:

- [Troubleshooting Booting Failures, page 23-9](#)
- [Troubleshooting Hardware Failures, page 23-12](#)
- [Troubleshooting Service Engine Application Status Errors, page 23-13](#)
- [Using the ping Command from the Cisco ASR1000 Series Router to Verify Network Connectivity, page 23-14](#)

Troubleshooting Booting Failures

You can perform most of the troubleshooting for booting failures using the **show platform** and **show hw-module subslot all oir** commands and examining the output to determine the source of an operational problem. Check the output of the **show platform** command to verify that the SIP and SPA are operational.

The following sections provide information about troubleshooting booting failures on the Cisco WebEx Node SPA:

- [Troubleshooting Longer Booting Times in the Cisco WebEx Node SPA, page 23-9](#)
- [Troubleshooting the Cisco WebEx Node SPA in an Out-of-Service State, page 23-10](#)

Troubleshooting Longer Booting Times in the Cisco WebEx Node SPA

Sometimes the Cisco WebEx Node SPA can remain in a booting state for longer-than-usual periods of time. There can be normal reasons for this, or it can be an indication of a problem.

Use the **show hw-module subslot all oir** command to display the operational status of the Cisco WebEx Node SPA. The following example shows sample output from the **show hw-module subslot all oir** command that shows the Cisco WebEx Node SPA in subslot 1/1 in the booting state:

```
Router#sh hw-module subslot all oir
Module      Model      Operational Status
-----
subslot 0/0  SPA-2X1GE-V2  ok
subslot 0/1  SPA-WMA-K9    ok
subslot 1/1  SPA-WMA-K9    booting
```

To troubleshoot a Cisco WebEx Node SPA that is remaining in the boot state, complete the following steps:

-
- Step 1** Review some of the possible causes for longer booting times for the Cisco WebEx Node SPA that are described in [Table 23-1](#).
- If none of the reasons described in [Table 23-1](#) are found, and the SPA remains in a booting state for more than 2 minutes, then the SPA will eventually timeout in 6 minutes. The OIR process will automatically try to recover from the problem. The OIR process will make 5 attempts to bring up the Cisco WebEx Node SPA before powering off the SPA.
- Step 2** Use the **show logging** command to look for the SPA_OIR-3-SPA_POWERED_OFF message as shown in the following example:
- ```
*Mar 3 23:27:39.884: %SPA_OIR-3-SPA_POWERED_OFF: subslot 1/0: SPA WMA SERVICES SPA
powered off after 5 failures within 1200 seconds
```
- Step 3** Reload the SIP as shown in the following example to try to correct the problem:
- ```
Router# hw-module subslot slot 1 reload
```
-

Table 23-1 describes the possible reasons why the Cisco WebEx Node SPA might remain in a booting state for a longer length of time than usual.

Table 23-1 Possible Reasons for Longer Booting Times in the Cisco WebEx Node SPA

Possible Problem	Observations and Comments	Solutions
An FPD upgrade is in progress.	When the system detects an incompatible FPD version on the Cisco WebEx Node SPA, it will attempt to perform an automatic FPD upgrade. This operation can take up to 4 minutes to complete.	From EXEC mode, enter the show upgrade fpd progress command to check if a field-programmable devices (FPD) upgrade is in progress. Tip You can also check if the STATUS LED is blinking in amber color.
Automatic file system checking and recovery of the hard disk drive is being performed.	This process can take around 7 minutes to complete.	Confirm that the following message appears on the RP console: *Mar 3 23:29:29.763: %SPA_SE1-3-CHECKING_DISK: SIP1/0: SPA-WMA-K9[1/0]: Disk is being checked because of previous unclean shutdown of the SPA. Boot time might take longer because of this operation.

Troubleshooting the Cisco WebEx Node SPA in an Out-of-Service State

Both hardware and software problems can cause “out of service” states on the Cisco WebEx Node SPA.

To verify the out-of-service reason for the Cisco WebEx Node SPA, use the **show hw-module subslot all oir** command as shown in the following example:

```
Router# show hw-module subslot all oir
Module           Model              Operational Status
-----
subslot 0/0      SPA-2X1GE-V2       ok
subslot 0/1      SPA-WMA-K9         ok
subslot 1/1      SPA-WMA-K9         out of service (Incompatible FPD)
```

Table 23-2 describes the possible problems and solutions for software-based out-of-service states. For more information about other hardware-based out-of-service states, refer to the troubleshooting chapter for the Cisco WebEx Node SPA in the *Cisco ASR 1000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide*.

Table 23-2 Possible Problems for Software-Based Out-of-Service States on the Cisco WebEx Node SPA

Possible Problem	Observations and Comments	Solutions
<p>The FPD image was corrupted for some of the following possible reasons:</p> <ul style="list-style-type: none"> • SPA was removed during an FPD upgrade • A reload of the router occurred during an FPD upgrade. • A power failure occurred on the router during an FPD upgrade. 	<p>The show hw-module subslot all oir command displays a “failed too many time” reason code for the out of service operational status and the show logging command displays a HW-INIT-TIMEOUT failure.</p> <p>The following is an example of a HW-INIT-TIMEOUT message:</p> <pre>*Mar 3 23:27:05.903: %SPA_OIR-6-ONLINECARD: SPA (SPA-WMA-K9) online in subslot 1/1 *Mar 3 23:27:16.488: %SPA_OIR-3-HW_INIT_TIMEOUT: subslot 1/0 *Mar 3 23:27:21.488: %SPA_OIR-3-RECOVERY_RELOAD: subslot 1/0: Attempting recovery by reloading SPA *Mar 3 23:27:21.489: %SPA_OIR-6-OFFLINECARD: SPA (SPA-WMA-K9) offline in subslot 1/0</pre>	<ol style="list-style-type: none"> 1. Enter the upgrade hw-module subslot fpd bundled command to start recovery of the FPD upgrade. If the problem was due to an FPD image corruption problem, then the SPA should boot normally after the upgrade is complete. 2. If the FPD upgrade completes successfully but you still have an error, then the SPA probably has a hardware problem. 3. Refer to the troubleshooting steps in the <i>Cisco ASR 1000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide</i>.

Table 23-2 Possible Problems for Software-Based Out-of-Service States on the Cisco WebEx Node SPA (continued)

Possible Problem	Observations and Comments	Solutions
The FPD upgrade was unable to be performed.	The show hw-module subslot all oir command displays an “Incompatible FPD” reason code for the out of service operational status.	<ol style="list-style-type: none"> 1. Enter the show hw-module all fpd command to verify the FPD versions. 2. Refer to the “Upgrading Field-Programmable Devices” chapter of this guide to get information about upgrading your FPD image.
The Cisco WebEx Node SPA software sub-package is not installed.	<p>The show hw-module subslot all oir command displays a “not allowed online” reason code for the out of service operational status, and the show logging command displays the ASR1000_RP_SPA-3-MISSING_SPA_PKG_ERR as shown in the following example:</p> <pre>*Mar 24 22:39:49.832: %ASR1000_RP_SPA-3-MISSING_SPA_PKG_ERR: sipspawma package is not installed for slot = 0 and subslot = 0, SPA bootup failed.</pre>	<p>The Cisco WebEx Node SPA requires you to install an independent software sub-package called “sipspawmak9.” To successfully install this sub-package you must complete the following steps:</p> <ol style="list-style-type: none"> 1. Extract the individual system sub-packages from the consolidated package for the router into a directory with the provisioning file (.conf file). <p>Note You cannot boot the router from a consolidated package when you are installing a Cisco WebEx Node SPA.</p> <ol style="list-style-type: none"> 2. Download the optional sipspawmak9 sub-package to the same location as the individual sub-packages and the provisioning file. 3. Configure the router to boot from a provisioning file. 4. Reload the router. <p>For more detailed information about installing the software for the Cisco WebEx Node SPA, refer to the <i>Cisco ASR 1000 Series Aggregation Services Router Software Configuration Guide</i>.</p>

Troubleshooting Hardware Failures

Depending on the severity of the error, the SPA may initiate a reload to recover from the failure. Any error message that is of SPA_CPU_ERR error type is an indication of a hardware problem on the SPA.

For more information about hardware-related failures, refer to the troubleshooting chapter of the *Cisco ASR 1000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide*.

Troubleshooting Service Engine Application Status Errors

After you configure the virtual service-engine interface, you should verify the configuration using the **show hw-module subslot service-engine status** command, and look for the Application Status field to be “Online” as shown in the following example:

```
Router# show hw-module subslot 1/0 service-engine status
Service Engine is Cisco SPA-WMA-K9
Service Engine state: Steady (0x300)
Service Engine OS Version: 1.0.0, Application Version: 1.0.0

Application: WebEx Node (Web Conferencing)
Application Status: Online
Configuration:
```

If the Application Status is “Offline,” refer to [Table 23-3](#), which describes the possible reasons and solutions for this state.

Table 23-3 Possible Reasons for Application Status Problems for the Cisco WebEx Node SPA

Possible Problem	Observations and Comments	Solutions
Provisioning error at the Cisco WebEx Data Center	<p>The output from the show hw-module subslot service-engine status command shows “Online” in the Application Status field, and “Web Conferencing” as the mistaken operation mode, when the desired mode is “Voice and Video Conferencing” as shown in the following example:</p> <pre>Router# show hw-module subslot 1/0 service-engine status Service Engine is Cisco SPA-WMA-K9 Service Engine state: Steady (0x300) Service Engine OS Version: 1.0.0, Application Version: 1.0.0 Application: WebEx Node (Web Conferencing) Application Status: Online</pre>	<p>Contact Cisco WebEx Data Center support to verify that the Cisco WebEx Node for ASR 1000 Series has been provisioned for the expected “Web Conferencing” or “Voice and Video Conferencing” mode.</p> <p>For more information, see the “Registering with the WebEx Data Center and the Cisco WebEx Node Management System” topic in Chapter 22, “Configuring the Cisco WebEx Node for ASR 1000 Series.”</p>
Provisioning error at the Cisco WebEx Data Center	<ul style="list-style-type: none"> The output from the show hw-module subslot service-engine status command shows “Offline” in the Application Status field. Confirm that a message similar to the following example appears on the RP console: <pre>Nov 3 20:42:29.791: %SPA_SRVCS_ENGINE-3-APP_MSG_ERR: SIP0/1: SPA-WMA-K9[0/1]: Authentication failed with Cisco WebEx Data Center SSL server. Please contact with WebEx support for assistance</pre>	<p>Contact Cisco WebEx support as directed by the system error message.</p>

Table 23-3 Possible Reasons for Application Status Problems for the Cisco WebEx Node SPA (continued)

Possible Problem	Observations and Comments	Solutions
Network connectivity problem, such as the subnet assigned to the service-engine interface is not routable.	<ul style="list-style-type: none"> The output from the show hw-module subslot service-engine status command shows “Offline” in the Application Status field. Confirm that a message similar to the following example appears on the RP console: <pre>Nov 3 13:45:51.943: %SPA_SRVCS_ENGINE-3-APP_MSG_ERR: SIP0/0: SPA-WMA-K9[0/1]: Connect CWNMS server failed, check network availability to CWNMS server.</pre> 	<ol style="list-style-type: none"> Check network connectivity to the Cisco WebEx Data Center, using the traceroute command from the Cisco WebEx SPA console as shown in the following example: <pre>service-spa# traceroute wma.webex.com traceroute to globalwatch.webex.com (10.114.169.228), 30 hops max, 38 byte packets 1 10.1.1.1 (12.1.1.1) 0.277 ms 0.254 ms 0.246 ms 2 10.1.99.65 (10.1.99.65) 0.577 ms 0.394 ms 0.387 ms</pre> Check network connectivity from the clients that will be joining the meeting being hosted on the Cisco WebEx Node SPA. Use the ping command from the Cisco WebEx SPA console as shown in the following example, where 172.16.144.153 is address of the client: <pre>service-spa# ping 172.16.144.153 PING 172.16.144.153 (172.16.144.153) 100(128) bytes of data. 108 bytes from 172.16.144.153: icmp_seq=1 ttl=41 time=69.1 ms 108 bytes from 172.16.144.153: icmp_seq=2 ttl=41 time=68.9 ms 108 bytes from 172.16.144.153: icmp_seq=3 ttl=41 time=68.8 ms 108 bytes from 172.16.144.153: icmp_seq=4 ttl=41 time=68.9 ms 108 bytes from 172.16.144.153: icmp_seq=5 ttl=41 time=68.9 ms --- 172.16.144.153 ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4000ms rtt min/avg/max/mdev = 68.882/68.976/69.133/0.299 ms</pre> <p>For more information about accessing the Cisco WebEx SPA console, see the “Accessing the Cisco WebEx Node SPA Console” section on page 23-4.</p>

Using the ping Command from the Cisco ASR1000 Series Router to Verify Network Connectivity



Note

The Cisco WebEx Node SPA might not activate properly if network access between the Cisco ASR Series 1000 Aggregation Services Router and certain Cisco WebEx servers is blocked, such as the Cisco WebEx Data Center SSL Gateway or Cisco WebEx Node Management server. Be sure to verify connectivity to these servers from the Cisco ASR 1000 Series Router.

The **ping** command is a convenient way to test the ability of an interface to send and receive packets over the network. The **ping** command sends ICMP echo request packets to a specified destination address, which should send an equal number of ICMP echo reply packets in reply. By measuring the numbering of packets that are successfully returned, as well as how long each packet takes to be returned, you can quickly obtain a rough idea of the Layer 3 to Layer 3 connectivity between two interfaces.

The IP **ping** command has the following syntax:

ping

or

ping *ip-address* [**repeat** *count*] [**data** *hex*] [**size** *datagram-size*]

If you enter just **ping**, the command interactively prompts you for all other parameters. Otherwise, you must specify at least a specific IP address as the destination for the ping. You can also optionally specify the following parameters:

- **repeat** *count*—Number of ICMP echo request packets to send. The default is five packets.
- **data** *hex*—The data pattern, in hexadecimal, to be sent in the ICMP echo request packets.
- **size** *datagram-size*—Specifies the size, in bytes, of the ICMP echo request packets to be sent. The range is 40 to 18024 bytes, with a default of 100 bytes.

Using the Cisco IOS Event Tracer to Troubleshoot Problems



Note

This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

Preparing for Online Insertion and Removal of a SPA

The Cisco ASR 1000 Series Aggregation Services Routers support online insertion and removal (OIR) of the SIP, in addition to each of the SPAs. Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This means that a SIP can remain installed in the router with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see [Chapter 5, “Troubleshooting the SIP.”](#)



CHAPTER 24

Overview of the Cisco DSP SPA for ASR 1000 Series

This chapter provides an overview of the release history, features, and MIB support for the Cisco Voice SPA for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to in this document as the SPA-DSP.

This chapter includes the following sections:

- [Release History, page 24-1](#)
- [Pre-requisites, page 24-2](#)
- [Overview of the Cisco DSP SPA, page 24-2](#)
- [Supported Features, page 24-4](#)
- [Restrictions, page 24-5](#)
- [Supported MIBs, page 24-5](#)

Release History

Release	Modification
Cisco IOS XE Release 3.2	Introduced a new DSP SPA, for the ASR 1000 Series to enable transcoding and transrating services for voice.

Pre-requisites

Table 24-1 provides the software and hardware compatibility requirement matrix for installing a SPA-DSP:

Table 24-1 SPA-DSP Hardware and Software Compatibility Requirements

Type of DSP SPA (Product ID)	ASR1000 Router Chassis supported	Route Processor supported	SIPs supported	ESPs supported	Minimum Cisco IOS XE Software Release supported
SPA-DSP	ASR 1002, ASR 1004, and ASR 1006 Chassis	RP1 and RP2	SIP10 and SIP40	ESP10 and ESP40	Cisco IOS XE Release 3.2s

Overview of the Cisco DSP SPA

The Cisco DSP SPA has been introduced on Cisco ASR 1000 Series Routers to provide voice transcoding and transrating functionalities. The DSP SPA is a half-height SPA. The Product ID of DSP SPA is SPA-DSP. The SPA-DSP is a service SPA and does not have external physical interfaces on the front panel. The SPA-DSP has 21 Digital Signal Processors (DSPs) which perform the encoding and decoding of voice streams. The SPA-DSP works in conjunction with the SBC application to provide the voice transcoding and transrating functionalities. The CUBE (ENT) can also use the SPA-DSP for transcoding and transrating.

The SPA-DSP in the transcoder case, provides functionality to translate one type of media stream using a specific codec type to another type of media stream that uses a different type of codec technologies. This not only includes translation between differing codecs, but also functionality such as the translation between different packetization settings (transrating), and the ability to perform DTMF interworking.

The SBC on the Cisco ASR1000 Series Router, externally known as Cisco Unified Border Element, Service Provider - CUBE (SP) can be configured as a Unified SBC or as a Distributed SBC. When configured as a distributed SBC, the SPA-DSP can be used externally as a centralized resource for other SBCs.

High-Level System Details

Based on the type of operational management, the SPA-DSP functions can be divided into two modules: Data Plane and Control Plane.

The data plane module is responsible for processing and sending the data. The SPA-DSP does not have any interfaces towards the network. The DSPs on the SPA process the voice packets that they receive from the QFP side and send the transcoded voice packets back to the QFP.

After initial set up a boot image is uploaded to the SPA-DSP. The full SPA-DSP image is then uploaded and the SPA-DSP is controlled through the DSP control packets.



Note

The SPA-DSP does not have a CPU or a hard disk.

Understanding Codecs and Maximum Channels Supported

Each SPA-DSP comprises of seven SP2603 DSP chips having a total of 21 DSP cores (3 DSP cores per SP2603). Based on the complexity of codec (low, medium, high), the density or maximum number of channels supported per DSP core and maximum channels supported per SPA-DSP are defined.

Following table provides a matrix for maximum channels supported on DSP core and SPA-DSP and the complexity type:

Table 24-2 **Codec -Complexity-and-Density-Supported Matrix**

Codec Complexity or Service	Maximum supported Density per DSP Core	Maximum supported Density per SPA-DSP
LC (Low complexity) Voice/xcode	43	903
MC (Medium complexity) Voice/xcode	28	588
HC (High Complexity) Voice/xcode	17	357
ISAC Voice/xcode	8	168

Table 24-3 **SPA-DSP-Supported Transcoding Codec List**

Codec Name	Codec Description
g711alaw	G.711 A Law 64000 bps
g711ulaw	G.711 u Law 64000 bps
g722-64	G722r64
g723r53	G.723.1 5300 bps
g723r63	G.723.1 6300 bps
g726r16	G.726 16000 bps
g726r24	G.726 24000 bps
g726r32	G.726 32000 bps
g726r40	G.726 40000 bps
g728	G.728 codec
g729abr8	G.729ab 8000 bps
g729ar8	G.729a 8000 bps
g729br8	G.729b 8000 bps
g729r8	G.729 8000 bps
gsmamr-nb	GSMAMR codec
ilbc	ILBC codec
isac	ISAC codec

Supported Features

The Cisco SPA-DSP for the ASR 1000 Series includes some of the following basic features:

- Enhances ASR 1000 Series Router capabilities by providing DSP based voice transcoding and transrating solutions.
- Translates one type of media stream (voice) to another type of media stream that uses different media encoding and decoding technologies.
- Enables translation between different packetization settings (transrating), and provides DTMF interworking.
- Provision to configure S/BC as a Unified SBC or Distributed SBC with on-board DSPs or as a centralized DSP providing transcoding for number of external SBCs.
- Faceplates LEDs to indicate SPA status.
- Voltage and temperature monitoring.
- Supports online insertion and removal (OIR).
- Provides a jitter buffer to be able to do packet loss concealment.
- Enables transcoding of voice packets for IPv4 (VoIPv4) as well as IPv6 (VoIPv6).

Inband DTMF Interworking

The Dual-Tone Multifrequency (DTMF) dialing consists of simultaneous voice-band tones generated when a button is pressed on a telephone. The use of DTMF signaling for this feature enables support for advanced telephony services. Currently there are a number of application servers and service creation platforms that do not support media connections. To provide value-added services to the network, these servers and platforms need to be aware of signaling events from a specific participant in the call. Once the server or platform is aware of the DTMF events that are being signaled, it can use third-party call control, or other signaling mechanisms, to provide enhanced services. Examples of the types of services and platforms that are supported by this feature are various voice web browser services, Centrex switches or business service platforms, calling card services, and unified message servers. All of these applications require a method for the user to communicate with the application outside of the media connection. The DTMF Events Through SIP Signaling feature provides this signaling capability.

This feature is related to the SIP INFO Method for DTMF Tone Generation feature, which adds support for out-of-band DTMF tone generation using the SIP INFO method. Together the two features provide a mechanism to both send and receive DTMF digits along the signaling path. The SPA-DSP supports the detection and reporting of inband DTMF tones and their conversion to RFC2833 based DTMF tones or out-of-band signalling (and vice versa).

**Note**

The SPA-DSP supports the conversion from RFC2833 DTMF tones to inband tones.

Managing Jitters for Voice Packets

This section explains how jitter in voice packets are managed by SPA-DSP to provide smooth flow of voice streams. Jitter is defined as the variation in the delay of received packets. In a packet-voice environment, the sender is expected to reliably transmit voice packets at a regular interval (for example, send one frame every 20 ms). These voice packets can be delayed throughout the packet network and not

arrive at that same regular interval at the receiving station (for example, they might not be received every 20 ms). The difference between when the packet is expected and when it is actually received is defined as a jitter.

To handle the jitters, the SPA-DSP maintains a jitter buffer to store a certain amount of voice frames in the buffer and wait for late arriving voice frames. The jitter buffer size is determined by counting the number of packets that arrive late and create a ratio of late arriving packets to the number of packets that are successfully processed. This ratio can be used to determine the jitter buffer size to determine a predetermined allowable later-packet ratio. After the jitter buffer is full with the specific voice packets, it plays all the RTP audio stream for VoIP in a steady stream to the SPA-DSP to be able to convert them into a steady audio stream.

Comfort Noise and VAD

This section discusses about how to deal with voice packets and silence period during a voice call. It also talks about how these voice quality issues can be rectified by using the voice activity detection (VAD) feature. The IP-based telephony systems need a voice activity detector to detect silence periods in the voice signal and temporarily discontinue transmission of the signal during the silence period. This saves bandwidth and allows the far-end to adjust its jitter-buffer. The downside is that during silence periods, the far-end phone has to generate its own signal to play to the listener. Usually, comfort noise is played out to the listener to mask the absence of an audio signal from the far-end. Comfort noise is usually modeled on the far-end noise so that there is not a stark contrast when you switch from the actual background noise to the comfort noise.

There are two possibilities to which comfort noise is injected in a voice call. The foremost is the use of VAD. Whenever VAD kicks-in, comfort noise packets are introduced in the audio stream. The second possibility (not a major contributor) is the kicking-in of echo-cancellation. Whenever echo-cancellation becomes active, comfort noise packets are introduced in the audio stream. The characteristics of these comfort packets is determined through an algorithm which includes monitoring on-going speech and receiving a signature of the background noise.

The SPA-DSP provides voice-activity detection and comfort noise functionalities by default. You can enable the local VAD settings by using the **vad on override** command from config-dspfarm-profile mode. Using the vad on override command will override the external vad settings. To disable the local vad settings use the **vad off override** command from config-dspfarm-profile mode.

Restrictions

- To enable voice transcoding and transrating functionality, first you need to enable the DSP SPA, create a dspfarm profile, and attach it to an SBC application. See the [Chapter 25, “Configuring the Cisco DSP SPA for the ASR 1000 Series.”](#) for these details.

Supported MIBs

The following MIBs are supported in Cisco IOS XE Release 3.2 for the DSP SPA on Cisco ASR 1000 Series Routers:

Common MIBs

- ENTITY-MIB

- ENTITY-SENSOR-MIB

Cisco-Specific Common MIBs

- CISCO-DSP-MGMT-MIB
- OLD-CISCO-CHASSIS-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB

For more information about MIB support on a Cisco ASR 1000 Series Routers, refer to the *Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide*, at the following URL:

<http://www.cisco.com/en/US/docs/routers/asr1000/mib/guide/asr1kmib.html>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<https://tools.cisco.com/RPF/register/register.do>



CHAPTER 25

Configuring the Cisco DSP SPA for the ASR 1000 Series

This chapter provides information about configuring the DSP SPA for ASR 1000 Series on the Cisco ASR 1000 Series Aggregation Services Routers, also referred to in this document as the SPA-DSP. This chapter includes the following sections:

- [Voice Transcoding Overview, page 25-1](#)
- [DSP Farm Profiles, page 25-1](#)
- [Configuration Tasks, page 25-2](#)

For information about SPA-DSP hardware details, refer the *Cisco ASR 1000 SIP and SPA Hardware Installation Guide*, managing your system images and configuration files, refer to the *Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2 and *Cisco IOS Configuration Fundamentals Command Reference* publications that correspond to your Cisco IOS XE software release.

Voice Transcoding Overview

This section provides a high-level overview of how the voice transcoding functionality is configured. After you insert the SPA-DSP in the SIP, the SPA-DSP is activated, and you can identify the status of the SPA-DSP, by executing the **show platform** command. If the SPA-DSP is operational and working fine, the **show platform** command output will display OK in the Status for SPA-DSP. Before you configure the voice transcoding functionality, you must enable the SPA-DSP. After you enable the voice card and set the SPA-DSP in DSP farm mode using the **dsp services dspfarm** command, you can create the DSP-farm service profiles.

DSP Farm Profiles

DSP-farm profiles are created to allocate DSP-farm resources. DSP-farm profiles can only be created after you set the DSP SPA in DSP farm mode. Under the profile, you select the service type (transcode), associate an application (SBC), and specify service-specific parameters such as codecs and maximum number of sessions. A DSP-farm profile allows you to group DSP resources based on the service type. Applications associated with the profile, such as SBC, can use the resources allocated under the profile. You can configure multiple profiles for the same service. The profile ID and service type uniquely identify a profile, allowing the profile to uniquely map to a SBC application. After creating the profile, you need to attach the profile to an application and enable the DSP farm profile.

The SPA-DSP and SBC application work in conjunction to provide voice transcoding and transrating functionalities. After the DSP-farm profiles are created, each profile is uniquely attached to a unique SBC identifier. The SBC configuration of Call-admission-control (CAC) and DTMF internetworking has been explained in the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*.

Configuration Tasks

Perform this procedure to enable a SPA-DSP and define a DSP farm profile. Additionally, you can enable or disable local voice activity detection (vad) irrespective of external configuration.

Prerequisites

Complete the following prerequisites to successfully enable the SPA-DSP and to set DSP SPA in DSP Farm mode on Cisco ASR 1000 Series Router:

- Requires Cisco IOS XE Software Release 3.2 or a later release installed on Cisco ASR 1000 Series Router
- DSP SPA installed and in operational state.

Configuring a DSP Farm Profile

Execute the following steps to enable the SPA-DSP and set DSP SPA in DSP farm mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot/sub-slot*
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm profile** *profile-identifier* {**transcoder** [**universal**]}
7. **description** *text*
8. **codec** *codec-type*
9. **maximum sessions** *number*
10. **associate application sbc**
11. **no shutdown**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-card slot/subslot Example: Router(config)# voice-card 1/1	Enters voice card configuration mode for the SPA-DSP on which you want to enable DSP-farm services.
Step 4	dsp services dspfarm Example: Router(config-voicecard)# dsp services dspfarm	Enables DSP-farm services for the SPA-DSP voice card.
Step 5	exit Example: Router(config-voicecard)# exit	Exits voice card configuration mode.
Step 6	dspfarm profile profile-identifier {transcode [universal]} Example: Router(config)# dspfarm profile 1 transcode universal	Enters DSP farm profile configuration mode to define a profile for DSP farm services. Note The <i>profile-identifier</i> and service type uniquely identify a profile. If the service type and <i>profile-identifier</i> pair are not unique, you are prompted to choose a different <i>profile-identifier</i> .
Step 7	description text Example: Router(config-dspfarm-profile)# description low2mediumcomp	(Optional) Includes a specific description about the Cisco DSP farm profile.
Step 8	codec codec-type Example: Router(config-dspfarm-profile)# codec g723r63 Router(config-dspfarm-profile)# codec g723r53	Specifies the codecs supported by a DSP farm profile. Note By default, the codecs g711ulaw, g711alaw, g729ar8, and g729abr8 are created for each DSP farm profile.

	Command or Action	Purpose
Step 9	maximum sessions <i>number</i> Example: Router(config-dspfarm-profile)# maximum sessions 4	Specifies the maximum number of sessions that are supported by the profile. <ul style="list-style-type: none"> <i>number</i>—Range is determined by the available registered DSP resources. Default is 0. Note By default, the maximum sessions are counted from the subslot where the SPA-DSP is available. If there are more than one SPA-DSPs and the maximum sessions exceed the session limit per SPA-DSP, the remaining sessions are managed by the second SPA-DSP.
Step 10	associate application sbc Example: Router(config-dspfarm-profile)# associate application sbc	Associates the SBC application to the DSP farm profile.
Step 11	no shutdown Example: Router(config-dspfarm-profile)# no shutdown	Enables the profile, allocates DSP farm resources, and associates the application.
Step 12	exit Example: Router(config-dspfarm-profile)# exit	Exits DSP farm profile configuration mode.

What to Do Next

For more information related to associating an SBC to a DSP farm profile, see the 'Cisco Unified Border Element (SP Edition) - SPA DSP Services' chapter in the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* at the following link:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_spadsp.html

Also, see the the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* for SBC configuration information (Call-admission-control (CAC) and DTMF interworking).

Enabling or Disabling Voice Activity Detection (VAD)

Execute the following steps to enable or disable local VAD settings irrespective of external VAD settings.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dspfarm profile** *profile-identifier*
4. **vad on override**

5. do show running-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dspfarm profile profile-identifier Example: Router(config)# dspfarm profile 1	Enters DSP farm profile configuration mode to enable or disable voice activity detection settings (VAD).
Step 4	vad on override Example: Router(config-dspfarm-profile)# vad on override	Enables the voice activity detection (VAD) feature locally and overrides the external VAD settings.
Step 5	do show running-config Example: Router(config-dspfarm-profile)# do show running-config !!! dspfarm profile 1 transcode codec g711ulaw codec g711alaw codec g729ar8 codec g729abr8 maximum sessions 588 associate application SBC vad on override !	Displays the local VAD settings which will override the external VAD settings for the current DSP farm profile.

Configuration Examples for Universal Voice Transcoding

This section includes an example for configuring a Cisco SPA-DSP installed in a Cisco ASR 1000 Series Router:

```
Router# config t
Router(config)# voice-card 1/1
Router(config-voice-card)# dsp services dspfarm
Router(config-voice-card)# exit
Router(config)# dspfarm profile 2 transcode universal
Router(config-dspfarm-profile)# description low2mediumcomp
```

```
Router(config-dspfarm-profile)# codec g723r63
Router(config-dspfarm-profile)# codec g723r53
Router(config-dspfarm-profile)# maximum sessions 10
Router(config-dspfarm-profile)# associate application sbc
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
Router(config)# exit
Router#show running-config
voice-card 1/1
  dsp services dspfarm
!
!
.....
dspfarm profile 2 transcode universal
  description low2mediumcomp
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g723r63
  codec g723r53
  maximum sessions 10
  associate application SBC
!
```

Additional References

The following sections provide references related to the SPA-DSP and Voice Transcoding Support.

Related Documents

Related Topic	Document Title
SBC configuration	<i>Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model</i>
SPA-DSP Hardware information	<i>Cisco ASR 1000 SIP and SPA Hardware Installation Guide</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
Common MIBs <ul style="list-style-type: none"> ENTITY-MIB ENTITY-SENSOR-MIB 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs
Cisco-Specific Common MIBs <ul style="list-style-type: none"> CISCO-DSP-MGMT-MIB OLD-CISCO-CHASSIS-MIB CISCO-ENTITY-FRU-CONTROL-MIB CISCO-ENTITY-SENSOR-MIB CISCO-ENTITY-ALARM-MIB CISCO-ENTITY-VENDORTYPE-OID-MIB 	

RFCs

RFC	Title
None	—

Technical Assistance

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



PART 7

Field-Programmable Devices



CHAPTER 26

Upgrading Field-Programmable Devices

In general terms, field-programmable devices (FPDs) are hardware devices implemented on router cards that support separate upgrades. The term “FPD” has been introduced to collectively and generically describe any type of programmable hardware device on SPAs. FPDs were introduced on the Cisco ASR 1000 Series Aggregation Services Routers to support the SPAs.

This chapter describes the information that you need to know to verify image versions and to perform SPA FPD upgrades.

This chapter includes the following sections:

- [Release History, page 26-1](#)
- [FPD Upgrade, page 26-1](#)
- [Optional FPD Procedures, page 26-4](#)
- [FPD Image Upgrade Examples, page 26-7](#)
- [Troubleshooting Problems with FPD Image Upgrades, page 26-9](#)

Release History

[Table 26-1](#) provides the release history for all FPD-related features on the Cisco ASR 1000 Series Routers.

Table 26-1 FPD Release History

Release	Modification
Cisco IOS XE Release 2.1	SIPs and SPAs were released on the Cisco ASR 1000 Series Routers for the first time. FPD images were introduced to support these SPAs.

FPD Upgrade

This section provides information if you want to upgrade FPDs for SPAs. These instructions are not always feasible for operating network environments. If these methods of upgrade are not suitable for your situation, see other sections of this document for other methods of upgrading FPDs.

This section contains the following topics:

- [Overview of FPD Images and Packages, page 26-2](#)
- [Upgrading Your Cisco IOS Release and FPD Image, page 26-2](#)

- [Upgrading Only Your Cisco IOS Release and Retaining Your Current FPD Image, page 26-2](#)
- [Upgrading FPD Images in a Production System, page 26-2](#)

Overview of FPD Images and Packages

With the Cisco ASR 1000 Series Routers, the Cisco IOS image comes bundled with the FPD image. An FPD incompatibility on a SPA disables all interfaces on that SPA until the incompatibility is addressed.

Upgrading Your Cisco IOS Release and FPD Image

To upgrade your Cisco IOS release and your FPD image, do the following steps:

-
- | | |
|---------------|---|
| Step 1 | Download the SPA package for the Cisco IOS release that you are upgrading to. The package contains both the Cisco IOS image and the FPD image. |
| Step 2 | Boot the new version of Cisco IOS. When the new version of Cisco IOS boots, search for the bundled FPD image. The FPD images will be updated automatically as part of the Cisco IOS boot process. |
| Step 3 | When the router has booted, verify the upgrade was successful by entering the show hw-module all fpd command. |
-

Upgrading Only Your Cisco IOS Release and Retaining Your Current FPD Image

You may choose to upgrade your Cisco IOS release with or without retaining your current FPD image. You may choose to upgrade your Cisco IOS image and retain your current FPD image, although this is not recommended.

-
- | | |
|---------------|--|
| Step 1 | Use the no upgrade fpd auto command to disable the bundled FPD image. |
|---------------|--|
-



Note The automatic upgrade feature is disabled once you enter the **no upgrade fpd auto** command.

- | | |
|---------------|--|
| Step 2 | Save the configuration before loading the new image. |
| Step 3 | Load the new image. |



Note If your current FPD image is not compatible with the new image, the SPAs do not come online.

Upgrading FPD Images in a Production System

Adding a SPA to a production system presents the possibility that the SPA may contain versions of FPD images that are incompatible with the Cisco IOS release currently running the router. In addition, the FPD upgrade operation can be a very CPU-intensive operation and therefore the upgrade operation may

take more time when it is performed on a production system. The performance impact will vary depending on various factors, including network traffic load, the type of processing engine used, type of SPA, and the type of service configured.

For these reasons, we recommend that one of the following alternatives be used to perform the FPD upgrade on a production system if possible:

- [Using a Non-Production System to Upgrade the Cisco ASR Series Router SPA FPD Image, page 26-3](#)
- [Verifying System Compatibility First, page 26-3](#)

Using a Non-Production System to Upgrade the Cisco ASR Series Router SPA FPD Image

Before beginning the upgrade, ensure:

- The spare system is running the same version of the Cisco IOS software release that the target production system is running.
- The automatic upgrade feature is enabled on the spare system. (The automatic upgrade feature is enabled by default. It can also be enabled using the **upgrade fpd auto** command).

Use the following procedure to perform an upgrade on a spare system:

-
- | | |
|---------------|---|
| Step 1 | Insert the SPA into the spare system.

If an upgrade is required, the system will perform the necessary FPD image updates so that when this SPA is inserted to the target production system it will not trigger an FPD upgrade operation there. |
| Step 2 | Verify the upgrade was successful by entering the show hw-module all fpd command. |
| Step 3 | Remove the SPA from the spare system after the upgrade. |
| Step 4 | Insert the SPA into the target production system. |
-

Verifying System Compatibility First

If a spare system is not available to perform an upgrade, you can check for system compatibility by disabling the automatic upgrade feature before inserting the SPA. (The automatic upgrade feature is enabled by default. It can be disabled using the **no upgrade fpd auto** command.)

- If the FPD images on the SPA are compatible with the system, you will only need to re-enable the automatic upgrade feature (the automatic upgrade feature can be re-enabled using the **upgrade fpd auto** command).
- If the FPD images on the SPA are not compatible with the system, the SPA is disabled but will not impact system performance by attempting to perform an automatic upgrade.

Use the following procedure to check the FPD images on the SPA for system compatibility:

-
- | | |
|---------------|--|
| Step 1 | Disable the automatic upgrade feature using the no upgrade fpd auto global configuration command. |
| Step 2 | Insert the SPA into the system. |

If the FPD images are compatible, the SPA will operate successfully after bootup.

If the FPD images are not compatible, the SPA is disabled. At this point we recommend that you wait for a scheduled maintenance when the system is offline to manually perform the FPD upgrade as described in the [“Manually Upgrading SPA FPD Images” section on page 26-4](#).

- Step 3** Re-enable the automatic upgrade feature using the **upgrade fpd auto** global configuration command.
-

Optional FPD Procedures

This section provides information for optional FPD-related functions. None of the topics discussed in this section are necessary for completing FPD upgrades, but may be useful in some FPD-related scenarios. It covers the following topics:

- [Manually Upgrading SPA FPD Images, page 26-4](#)
- [Upgrading Multiple FPD Images, page 26-4](#)
- [Displaying Current and Minimum Required FPD Image Versions, page 26-5](#)
- [Displaying Information About the Default FPD Image Package, page 26-6](#)
- [Verifying the FPD Image Upgrade Progress, page 26-7](#)

Manually Upgrading SPA FPD Images

To manually upgrade the current FPD version on a SPA, use the following command:

```
Router# upgrade hw-module subslot [slot-number/subslot-number] fpd bundle [reload]
```

In this example, *slot-number* is the slot where the SIP is installed, *subslot-number* is the subslot number where the SPA is located, **fpd** indicates the type of upgrade required, **bundle** selects the bundled FPD package, and **reload** specifies that the SPA is automatically reloaded after the upgrade. Note that **subslot slot-number/subslot-number** is used to specify a SPA FPD upgrade. The SPA will automatically be reloaded to complete the FPD upgrade.



Caution

An image upgrade can require a long period of time to complete depending on the SPA.

Upgrading Multiple FPD Images

A single piece of hardware can contain multiple FPD images. The Cisco ASR 1000 Series Routers can upgrade up to three FPD images simultaneously. However, only one FPD upgrade per router slot can occur at a time, so all FPD images on all SPAs in a single slot will have to wait for another FPD upgrade to finish.

Users should note that some FPD images require the SPA to reload to complete. The FPD upgrade process will perform this step automatically, so users do not have to intervene. However, the other FPDs in the hardware of the specified slot will have to wait for this reload to complete before their upgrade process begins.



Note

With a manual upgrade, you must include the **reload** option to cause the SPA to reload automatically. See the [“Manually Upgrading SPA FPD Images” section on page 26-4](#).

During an automatic upgrade, the Cisco ASR 1000 Series Routers will upgrade as many FPDs as possible at a time. No user intervention is possible or necessary. The upgrade process will not stop until all FPD images have been updated.

During manual upgrades, it is important to note that users can only specify upgrades for a single piece of hardware each time the **upgrade hw-module subslot** [*slot-number/subslot-number*] command is entered. The maximum of three simultaneous upgrades applies to manual upgrades as well. If you individually specify multiple manual FPD upgrades, only three FPDs can be upgraded simultaneously and that can only occur when the hardware is in different router slots. The FPD upgrade process will stop when all FPDs for the specified hardware have been upgraded.

Displaying Current and Minimum Required FPD Image Versions

To display the current version of FPD images on the SPAs installed on your router, use the **show hw-module** [*slot-number/subslot-number* | **all**] **fpd** command, where *slot-number* is the slot number where the SIP is installed, and *subslot-number* is the number of the SIP subslot where a target SPA is located. Entering the **all** keyword shows information for hardware in all router slots.

The following examples show the output when using this **show** command.

The output display in this example shows that FPD versions on the SPAs in the system meet the minimum requirements:

```
Router# show hw-module all fpd
```

Slot	Card Type	H/W Ver.	Field Programmable Device: "ID-Name"	Current Version	Min. Required Version
0/0	SPA-5X1GE-V2	1.1	1-GE I/O FPGA	1.10	1.10
0/1	SPA-8X1FE-TX-V2	1.1	1-FE I/O FPGA	1.1	1.1
0/2	SPA-2XCT3/DS0	1.1	1-ROMMON	2.12	2.12
			2-I/O FPGA	2.7	2.7
			3-T3 SUBRATE FPGA	1.4	1.4
1/0	SPA-2XOC3-POS	1.0	1-I/O FPGA	3.4	3.4
1/1	SPA-8XCHT1/E1	1.1	1-ROMMON	2.12	2.12
			2-I/O FPGA	2.7	2.7
1/2	SPA-2XT3/E3	1.0	1-ROMMON	2.12	2.12
			2-I/O FPGA	1.0	1.0
			3-E3 FPGA	1.4	1.4
			4-T3 FPGA	1.4	1.4

This example shows the output when using the *slot-number/subslot-number* argument to identify a particular SPA:

```
Router# show hw-module subslot 1/0 fpd
```

Slot	Card Type	H/W Ver.	Field Programmable Device: "ID-Name"	Current Version	Min. Required Version
1/0	SPA-2XOC3-POS	1.0	1-I/O FPGA	3.4	3.4

The output display in this example shows that the SPA in subslot 0/1 is disabled because one of the programmable devices does not meet the minimum version requirements.

Router# **show hw-module all fpd**

```

=====
Slot Card Type                H/W  Field Programmable  Current  Min. Required
=====
0/0 SPA-4XOC3-POS             1.0  1-I/O FPGA         3.4      3.4
-----
0/1 SPA-2XT3/E3 <DISABLED>    1.0  1-ROMMON           2.12     2.12
      2-I/O FPGA             0.6      1.0      *
      3-E3 FPGA              1.0      1.4      *
      4-T3 FPGA              1.0      1.4      *
-----
0/2 SPA-1X10GE-L-V2          1.0  1-10GE I/O FPGA    1.9      1.9
-----
0/3 SPA-1X10GE-L-V2          1.0  1-10GE I/O FPGA    1.9      1.9
=====
NOTES:
  - FPD images that are required to be upgraded are indicated with a '*'
    character in the "Minimal Required Version" field.
  - The following FPD image package file is required for the upgrade:
    asr1000-fpd-bundle.pkg
=====

```

Displaying Information About the Default FPD Image Package

You can use the **show upgrade fpd package default** command to find out which SPAs are supported with your current Cisco IOS release and which FPD image package you need for an upgrade.

Router# **show upgrade fpd package default**

```

*****
This Cisco IOS software image requires the following default FPD Image
Package for the automatic upgrade of FPD images (the package is available
from Cisco.com and is accessible from the Cisco Software Center page where
this IOS software image can be downloaded):
*****

```

Version: 12.2(XN)

Package Filename: asr1000-fpd-bundle.pkg

List of card type supported in this package:

No.	Card Type	Minimal HW Ver.
1)	4xT SERIAL SPA	0.0
2)	1xCHSTM1 SPA	0.0
3)	2xCT3 SPA	0.100
4)	2xCT3 SPA	0.200
5)	4xCT3 SPA	0.100

<additional output removed for readability>

Verifying the FPD Image Upgrade Progress

You can use the **show upgrade fpd progress** command to view a “snapshot” of the upgrade progress while an FPD image upgrade is taking place. The following example shows the type of information this command displays:

```
Router# show upgrade fpd progress
```

```
FPD Image Upgrade Progress Table:
```

Slot	Card Type	Field Programmable Device : "ID-Name"	Approx. Time Needed	Elapsed Time	State
0/1	SPA-8XCHT1/E1	2-I/O FPGA	00:01:00	00:00:23	Updating...
0/2	SPA-2XT3/E3	4-T3 FPGA	--:--:--	--:--:--	Waiting...

FPD Image Upgrade Examples

This section provides examples of automatic and manual FPD image upgrades. It includes the following examples:

- [Automatic FPD Image Upgrade Example, page 26-7](#)
- [Manual FPD Image Upgrade Example, page 26-8](#)

operation.

Automatic FPD Image Upgrade Example

The following example shows the output displayed when a SPA in slot 0 subslot 1 requires an FPD image upgrade and the **upgrade fpd auto** command is *enabled*. The required FPD image is automatically upgraded.

```
*Nov 28 13:14:22.782: %FPD_MGMT-3-INCOMP_IMG_VER: Incompatible I/O FPGA (FPD ID=2) image
version detected for SPA-2XT3/E3 card in subslot 0/1. Detected version = 0.6, minimum
required version = 1.0. Current HW version = 1.0.
*Nov 28 13:14:22.783: %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the
FPD image(s) for SPA-2XT3/E3 card in subslot 0/1. Use 'show upgrade fpd progress' command
to view the upgrade progress ...
*Nov 28 13:14:22.841: %FPD_MGMT-6-BUNDLE_DOWNLOAD: Downloading FPD image bundle for
SPA-2XT3/E3 card in subslot 0/1 ...
*Nov 28 13:14:22.981: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
SPA-2XT3/E3 card in subslot 0/1 = 00:01:00.
*Nov 28 13:14:22.983: %FPD_MGMT-6-UPGRADE_START: I/O FPGA (FPD ID=2) image upgrade in
progress for SPA-2XT3/E3 card in subslot 0/1. Updating to version 1.1. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
*Nov 28 13:14:43.267: %FPD_MGMT-6-UPGRADE_PASSED: I/O FPGA (FPD ID=2) image in the
SPA-2XT3/E3 card in subslot 0/1 has been successfully updated from version 0.6 to version
1.0. Upgrading time = 00:00:20.285
*Nov 28 13:14:43.267: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for SPA-2XT3/E3 card in subslot 0/1. Number of
successful/failure upgrade(s): 1/0.
```

```
*Nov 28 13:14:43.268: %FPD_MGMT-5-CARD_POWER_CYCLE: SPA-2XT3/E3 card in subslot 0/1 is
being power cycled for the FPD image upgrade to take effect.
```

Manual FPD Image Upgrade Example

In the following example, FPD for the 2-port T3/E3 SPA in subslot 0/3 is upgraded manually from the bundled FPD image package file. The command excludes the **reload** option so the SPA does not automatically reload.

```
Router#upgrade hw-module subslot 0/3 fpd bundled
```

```
% The following FPD will be upgraded for SPA-2XT3/E3 (H/W ver = 1.1) in subslot 0/3:
```

```
=====
Field Programmable   Current      Upgrade      Estimated
Device: "ID-Name"    Version      Version      Upgrade Time
=====
2-I/O FPGA           1.0          1.1          00:01:00
=====
```

```
% NOTES:
```

- Use 'show upgrade fpd progress' command to view the progress of the FPD upgrade.
- You must reload the card after the upgrade. The FPD upgrade is not finalized until the card is reloaded.
- The output of 'show hw-module <target> fpd' will not reflect the upgraded FPD version until the card is reloaded to finalize the upgrade.

```
% Are you sure that you want to perform this operation? [no]: yes
```

```
% Initiating the upgrade operation on the target card ...
```

```
(Use "show upgrade fpd progress" command to see upgrade progress)
```

```
Router#
```

```
*Mar 4 16:13:17.230: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
SPA-2XT3/E3 card in subslot 0/3 = 00:01:00.
```

```
*Mar 4 16:13:17.232: %FPD_MGMT-6-UPGRADE_START: I/O FPGA (FPD ID=2) image upgrade in
progress for SPA-2XT3/E3 card in subslot 0/3. Updating to version 1.1. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
```

```
*Mar 4 16:13:42.909: %FPD_MGMT-6-UPGRADE_PASSED: I/O FPGA (FPD ID=2) image in the
SPA-2XT3/E3 card in subslot 0/3 has been successfully updated from version 1.0 to version
1.1. Upgrading time = 00:00:25.676
```

```
*Mar 4 16:13:42.909: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for SPA-2XT3/E3 card in subslot 0/3. Number of
successful/failure upgrade(s): 1/0.
```

In the following example, FPD for the 2-port T3/E3 SPA in subslot 0/3 is upgraded manually from the bundled FPD image package file. The command includes the **reload** option so the SPA automatically reloads so the new FPD image takes effect immediately.

```
Router#upgrade hw-module subslot 0/3 fpd bundled reload
```

```
% The following FPD will be upgraded for SPA-2XT3/E3 (H/W ver = 1.1) in subslot 0/3:
```

```
=====
Field Programmable   Current      Upgrade      Estimated
Device: "ID-Name"    Version      Version      Upgrade Time
=====
2-I/O FPGA           1.0          1.1          00:01:00
=====
```

```
% NOTES:
- Use 'show upgrade fpd progress' command to view the progress of the FPD
  upgrade.
- The target card will be automatically reloaded after the upgrade
  operation. This reload will interrupt normal operation of the card. If
  necessary, ensure that appropriate actions have been taken to redirect
  card traffic before starting the FPD upgrade.

% Are you sure that you want to perform this operation? [no]: yes
% Initiating the upgrade operation on the target card ...
  (Use "show upgrade fpd progress" command to see upgrade progress)

Router#
*Mar  4 16:15:22.862: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
SPA-2XT3/E3 card in subslot 0/3 = 00:01:00.
*Mar  4 16:15:22.864: %FPD_MGMT-6-UPGRADE_START: I/O FPGA (FPD ID=2) image upgrade in
progress for SPA-2XT3/E3 card in subslot 0/3. Updating to version 1.1. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
*Mar  4 16:15:47.795: %FPD_MGMT-6-UPGRADE_PASSED: I/O FPGA (FPD ID=2) image in the
SPA-2XT3/E3 card in subslot 0/3 has been successfully updated from version 1.0 to version
1.1. Upgrading time = 00:00:24.931
*Mar  4 16:15:47.795: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for SPA-2XT3/E3 card in subslot 0/3. Number of
successful/failure upgrade(s): 1/0.
*Mar  4 16:15:47.796: %FPD_MGMT-5-CARD_POWER_CYCLE: SPA-2XT3/E3 card in subslot 0/3 is
being power cycled for the FPD image upgrade to take effect.
```

Troubleshooting Problems with FPD Image Upgrades

This section contains information to help troubleshoot problems that can occur during the upgrade process.

It contains the following topics:

- [Power Failure or Removal of a SPA During an FPD Image Upgrade, page 26-9](#)
- [Performing an FPD Recovery Upgrade, page 26-10](#)
- [Verifying a Successful Upgrade, page 26-12](#)

Power Failure or Removal of a SPA During an FPD Image Upgrade

These instructions should only be used if a previous upgrade attempt has failed due to an external factor such as a power failure or a SPA removal.

If the FPD upgrade operation is interrupted by a power failure or the removal of the SPA, it could corrupt the FPD image. This corruption of the FPD image file makes the SPA unusable by the router and the system will display the following messages when it tries to power up the SPA:



Note

To find more information about FPD-related messages, check the system error messages guide for your Cisco IOS XE software release.

```
Nov.28 11:30:36:%SPA_OIR-3-RECOVERY_RELOAD:subslot 0/1:Attempting
recovery by reloading SPA
Nov.28 11:30:51:%SPA_OIR-3-HW_INIT_TIMEOUT:subslot 0/1
Nov.28 11:30:56:%SPA_OIR-3-RECOVERY_RELOAD:subslot 0/1:Attempting
recovery by reloading SPA
```

```
Nov.28 11:31:11:%SPA_OIR-3-HW_INIT_TIMEOUT:subslot 0/1
Nov.28 11:31:16:%SPA_OIR-3-RECOVERY_RELOAD:subslot 0/1:Attempting
recovery by reloading SPA
Nov.28 11:31:31:%SPA_OIR-3-HW_INIT_TIMEOUT:subslot 0/1
Nov.28 11:31:31:%SPA_OIR-3-SPA_POWERED_OFF:subslot 0/1:SPA 4xOC3 POS
SPA powered off after 5 failures within 600 seconds
```

The **show hw-module all fpd** command can be used to verify that the SPA is using a corrupted FPD image. In this example, the SPA in slot 0/1 is corrupted.

```
Router# show hw-module all fpd
```

```
==== =====
Slot Card Type          H/W   Field Programmable   Current   Min. Required
Ver.   Device: "ID-Name"   Version   Version
==== =====
0/0 SPA-4XOC3-POS        1.0    1-I/O FPGA           3.4       3.4
-----
0/1 SPA-4XOC3-PO<DISABLED> 1.0    ??????????????      ??        ??
-----
0/2 SPA-1X10GE-L-V2      1.0    1-10GE I/O FPGA      1.9       1.9
-----
0/3 SPA-1X10GE-L-V2      1.0    1-10GE I/O FPGA      1.9       1.9
=====
```

Performing an FPD Recovery Upgrade

The recovery upgrade procedure can only be performed on a SPA that has been powered off by the system after it has failed all of the retries attempted to initialize the SPA.

The following example displays the output of an attempt to perform a recovery upgrade before all the initialization retries have been attempted for the SPA in subslot 0/1.



Note

Because a recovery upgrade is done at a more conservative speed, it may take more than the estimated upgrade time.



Note

Other factors can cause the system to ask “Do you want to perform the recovery upgrade operation?” Only answer **y** to this question if you have attempted an FPD upgrade that has failed due to a power failure or a SPA removal.

If you are prompted for this question without having previously had a failed upgrade attempt for one of the aforementioned reasons, contact Cisco Technical Support.

```
Nov.28 11:29:55:%SPA_OIR-3-RECOVERY_RELOAD:subslot 0/1:Attempting
recovery by reloading SPA
Nov.28 11:30:10:%SPA_OIR-3-HW_INIT_TIMEOUT:subslot 0/1
Nov.28 11:30:15:%SPA_OIR-3-RECOVERY_RELOAD:subslot 0/1:Attempting
recovery by reloading SPA
Nov.28 11:30:31:%SPA_OIR-3-HW_INIT_TIMEOUT:subslot 0/1
Router# upgrade hw-module subslot 0/1 fpg bundled
```

```
% Cannot get FPD version information for version checking. If a previous
upgrade attempt has failed for the target card, then a recovery upgrade
would be required to fix the failure.
```

```
% The following FPD(s) will be upgraded for SPA-4XOC3-POS (H/W ver =
1.0) in subslot 0/1:
```

```

=====
Field Programmable   Current      Upgrade      Estimated
Device:"ID-Name"     Version      Version      Upgrade Time
=====
1-I/O FPGA           ??          3.4          00:00:50
=====

```

```

% Do you want to perform the recovery upgrade operation? [no]:y
% Cannot perform recovery upgrade operation because the target card is
not in a failed state. Please try again later.

```

Once the following error message is displayed, you can perform the recovery upgrade:

```

Nov.28 11:31:31:%SPA_OIR-3-SPA_POWERED_OFF:subslot 0/1:SPA 4xOC3 POS SPA powered off after
5 failures within 600 seconds

```



Note

You must wait to see this error message before you attempt the upgrade.

Perform the manual FPD image upgrade method using the **upgrade hw-module subslot** command to recover from a corrupted image after the SPA has been powered off by the system. In this command, *slot-number* is the slot where the SIP is installed, *subslot-number* is the subslot of the SIP where the SPA is located.

The following example displays the console output of a recovery upgrade operation:

```

Router# upgrade hw-module subslot 0/1 fpd bundled

```

```

% Cannot get FPD version information from SPA-4XOC3-POS in subslot 0/1.

```

If a previous upgrade attempt on the target card was interrupted, then the corruption of FPD image might have prevented the card from coming online. If this is the case, then a recovery upgrade would be required to fix the failure.

```

(Hit ENTER to proceed with recovery upgrade operation) [confirm]

```

```

% The following FPD will be upgraded for SPA-4XOC3-POS (H/W ver = 1.0) in subslot 0/1:

```

```

=====
Field Programmable   Current      Upgrade      Estimated
Device: "ID-Name"     Version      Version      Upgrade Time
=====
1-I/O FPGA           ??          3.4          00:00:50
=====

```

```

% NOTES:

```

- Use 'show upgrade fpd progress' command to view the progress of the FPD upgrade.
- Since the target card is currently in disabled state, it will be automatically reloaded after the upgrade operation for the changes to take effect.

```

% Do you want to perform the recovery upgrade operation? [no]: y

```

```

% Starting recovery upgrade operation in the background ...

```

```

(Use "show upgrade fpd progress" command to see upgrade progress)

```

```

Router#

```

```

*Nov 28 17:46:10.191: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
SPA-4XOC3-POS card in subslot 0/1 = 00:00:50.

```

```

*Nov 28 17:46:10.233: %FPD_MGMT-6-UPGRADE_START: I/O FPGA (FPD ID=1) image upgrade in
progress for SPA-4XOC3-POS card in subslot 0/1. Updating to version 3.4. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:00:50) ...
*Nov 28 17:46:55.948: %FPD_MGMT-6-UPGRADE_PASSED: I/O FPGA (FPD ID=1) image in the
SPA-4XOC3-POS card in subslot 0/1 has been successfully updated from version ?? to
version 3.4. Upgrading time = 00:00:45.715
*Nov 28 17:46:55.948: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for SPA-4XOC3-POS card in subslot 0/1. Number of
successful/failure upgrade(s): 1/0.
*Nov 28 17:46:55.949: %FPD_MGMT-5-CARD_POWER_CYCLE: SPA-4XOC3-POS card in subslot 0/1 is
being power cycled for the FPD image upgrade to take effect.

```

Verifying a Successful Upgrade

After the upgrade process is complete, you can use the **show hw-module all fpd** command to verify that the FPD image has been successfully upgraded:

```
Router# show hw-module all fpd
```

```

=====
Slot Card Type                H/W   Field Programmable   Current   Min. Required
Ver.   Device: "ID-Name"   Version   Version
=====
0/0 SPA-4XOC3-POS             1.0    1-I/O FPGA           3.4       3.4
-----
0/1 SPA-4XOC3-POS             1.0    1-I/O FPGA           3.4       3.4
-----
0/2 SPA-1X10GE-L-V2           1.0    1-10GE I/O FPGA      1.9       1.9
-----
0/3 SPA-1X10GE-L-V2           1.0    1-10GE I/O FPGA      1.9       1.9
=====

```



PART 8

Quality-of-Service (QoS)



CHAPTER 27

Classifying and Scheduling Packets for ASR 1000 Series

This chapter provides an overview of the release history, prerequisites, restrictions, overview of classification and scheduling and configuring the classification and scheduling for ingress packets on the Cisco ASR 1000 Series Aggregation Services Routers.

This chapter includes the following sections:

- [Release History, page 27-1](#)
- [Overview of the Ingress Classification and Scheduling, page 27-2](#)
- [Prerequisites for Ingress Classification and Scheduling, page 27-2](#)
- [Classification and Scheduling Restrictions, page 27-3](#)
- [Information About Ingress Classification, page 27-3](#)
- [Information About Ingress Scheduling, page 27-16](#)

Release History

Table 27-1 Ingress Classification and Scheduling Release History

Release	Modification
Cisco IOS XE Software, Release 3.1S	Classification and scheduling for ingress packets was introduced on the Cisco ASR 1000 Series Aggregation Services Routers to resolve the oversubscription of bandwidth on ingress side.

Overview of the Ingress Classification and Scheduling

The ASR 1000 Series Routers contain a variety of SIPs and SPAs with a combination of low and high speed interfaces ranging from DS1 to 10 Gbps. Due to a variety of SPAs inserted in the ASR 1000 Series Router, both the Carrier Card (CC) and the SPA get oversubscribed in the ingress or egress direction. Currently, all the existing components of the ASR 1000 Series Router such as CC and ESP, prioritize the traffic in the egress direction. To resolve the oversubscription issue on the ingress side, ingress classification and scheduling have been introduced in Cisco IOS XE Software, Release 3.1S.

This technology provides the following advantages:

- Classifies and schedules the packets marked as high priority.
- Reduces the latency and jitters for packets (example video and voice) classified as high priority.

Prerequisites for Ingress Classification and Scheduling

Table 27-2 shows the hardware and software compatibility prerequisites for the ingress classification and scheduling feature.

Table 27-2 Hardware and Software Compatibility Matrix for Ingress Classification and Scheduling

Platform	Processor Engine	Forwarding Processors, Carrier Cards, and SPA Types Supported	New and Modified Commands
Cisco ASR 1000 Series Router	Cisco IOS XE Release 3.1S <ul style="list-style-type: none"> • Route Processor 1 (RP1) • Route Processor 2 (RP2) 	Forwarding Processors supported <ul style="list-style-type: none"> • ESP 5, ESP 10, ESP 20, ESP 40 SIPs supported <ul style="list-style-type: none"> • CC 10 • CC 40 SPAs supported <ul style="list-style-type: none"> • POS SPA: OC3, OC12, OC48, and OC192 flavors • Channelized SPA: ChT1/E1, ChT3/DS0, ChSTM1/OC3, and ChOC12/DS0 SPAs • Clear Channel SPA: T3/E3 and 12-in-1 SPAs • Ethernet SPAs: FE, 1 GE, 10 GE SPAs. • ATM SPAs: OC-3 and OC-12 flavour SPAs. 	Following is the list of new and modified commands: <ul style="list-style-type: none"> • ingress-class-map • map ip all queue • map ip dscp-based • map ip dscp • map ip precedence-based • map ip precedence • map ipv6 all queue • map ipv6 tc • map mpls all queue • map mpls exp • plim qos input class-map • show ingress-class-map • plim qos input map cos {enable inner-based outer-based {inner outer} {cos-value cos-range} queue {strict-priority 0}} • hw-module subslot {slot/subslot} qos input {weight weight}

**Note**

The above listed new commands for ingress classification and scheduling are documented in the *Cisco IOS Quality of Service Solutions Command Reference guide* at the URL http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html.

Classification and Scheduling Restrictions

Following are the restrictions pertaining to the classification feature:

- The maximum number of ingress class map templates configured per CC is 62 templates.
- Classification support is not enabled for logical interfaces such as multilink and tunnel interfaces.
- Packet classification CLI is disabled for multilink member links.
- Classification CLI cannot be enabled for frame relay subinterfaces.
- Classification is not supported for service SPAs such as WebEx.

Following are the restrictions pertaining to the scheduling feature:

- For clear-channel SPAs such as Ethernet, Serial, POS, and ATM SPAs, excess bandwidth settings are configured at the physical interface level. For channelized SPAs, the excess bandwidth settings can be set at the SPA level.
- Configurations built using high capacity CC or ESP, will be restored with best effort when a low-capacity CC or ESP replaces the high-capacity CC or ESP. Also, any per-CC minimum bandwidth configuration exceeding its ESI link capacity will be replaced with the corresponding ESI link's maximum capacity.
- When configuring the minimum CC bandwidth, the available range is 0 to the minimum carrier-card bandwidth and ESP bandwidth.

Information About Ingress Classification

The following sections provide details of the Ingress classification feature:

- [Ingress Classification Architecture, page 27-3](#)
- [Resolving Oversubscription, page 27-5](#)
- [Ingress Classification Overview, page 27-5](#)

Ingress Classification Architecture

The Cisco ASR 1000 Series Routers support ingress oversubscription. However, in case of oversubscription, it is important that the processing of the high-priority packets such as Internet control, L2 keepalives, signaling protocols, and high-priority data packets is done by the SIP or SPA over the low-priority packets. [Table 27-3](#) illustrates the various SPA, SIP, and ESP combinations that cause oversubscription.

Table 27-3 SIP-10 Oversubscription Details

ASR 1000 Chassis Type	ESP Type	Oversubscription State
<ul style="list-style-type: none"> ASR1000-SIP10G Incoming rate from SPAs. Maximum 4 multiplied by 11.2 Gbps Outgoing rate towards ESP 11.2 Gbps <p>Conclusion: SIP10G is always oversubscribed.</p>	ESP-2.5 G and ESP-5 G (Supported only on ASR-1002)	<p>No ESP oversubscription.</p> <p>ESPs interconnect device handles the entire 10G incoming traffic.</p>
	ESP-10G	<p>ESP is oversubscribed.</p> <p>Example:</p> <p>Input rate from (example) 3 carrier cards is 3 multiplied by 11.2Gbps</p> <p>Output rate towards QFP=12.8Gbps</p>
	ESP-20G	<p>ESP is oversubscribed.</p> <p>Example:</p> <p>Input rate from (example) 3 carrier cards is 3 multiplied by 11.2Gbps</p> <p>Output rate towards QFP=25.6 Gbps</p>
	ESP-40G	<p>No ESP oversubscription.</p> <p>Example:</p> <p>Input rate from (example) 3 carrier cards is 3 multiplied by 11.2Gbps</p> <p>Output rate towards QFP=2*25.6 Gbps</p>

Table 27-4 SIP-40 Oversubscription Details

ASR 1000 Chassis Type	ESP Type	Oversubscription State
<ul style="list-style-type: none"> ASR1000-SIP40G Incoming rate from SPAs. Maximum 4 multiplied by 11.2 Gbps Outgoing rate towards ESP depends on the ESP type <p>Conclusion: SIP40G oversubscription depends on the ESP type.</p>	ESP-2.5 G and ESP-5 G (Supported only on ASR-1002)	Not supported.
	ESP-10G	ASR1000-SIP40G operates as ASR1000-SIP10G. Example: Input rate from (example) 3 carrier cards is 3 multiplied by 11.2 Gbps Output rate towards QFP=12.8 Gbps ESP is oversubscribed.
	ESP-20G	ASR1000-SIP40G operates as ASR1000-SIP10G. Example: Input rate from (example) 3 carrier cards is 3 multiplied by 11.2 Gbps Output rate towards QFP=25.6 Gbps ESP is oversubscribed.
	ESP-40G	ASR1000-SIP40G operates as ASR1000-SIP40G. Example: Input rate from (example) 3 carrier cards is 3 multiplied by 23 Gbps Output rate towards QFP=51.2 Gbps ESP is oversubscribed.

Resolving Oversubscription

Following are the two high-level tasks which need to be performed to resolve the bandwidth oversubscription on the ingress side:

- Classifying the incoming traffic as high priority and low priority. Depending on the SPA type, the classification is done by either a SIP or a SPA.
- Scheduling the high-priority packets first and then processing the low-priority traffic. Depending on the scheduling configuration, weight can be assigned to low-priority packets.

Ingress Classification Overview

To solve the bandwidth oversubscription issue, packets must be classified as high-priority data traffic and control traffic, and guarantee their transmission to the QFP. Ingress Classification can be broadly divided into two:

- SPA-based classification—Some of the SPAs support the classification performed within the SPA hardware.

- SIP-based classification—SPAs rely on the classification performed inside the CC.

The SPAs supported on a Cisco ASR 1000 Series Router can be broadly classified into the following categories:

- Ethernet SPAs—Fast Ethernet (FE), 1-Gigabit Ethernet (GE), 10-Gigabit Ethernet SPAs
- ATM SPAs—OC3 and OC12 flavours
- Channelized SPAs—ChT1/ E1, ChT3/ DS0, ChSTM1/ OC3, and ChOC12/ DS0 SPAs
- Clear Channel SPAs—T3/ E3 and 12-in-1 SPAs
- POS SPAs—OC3, OC12, OC48, and OC192 flavors

**Note**

The Ethernet and ATM SPAs have classification capability at the SPA level, while the other types of SPAs rely on the SIP for ingress classification.

Table 27-5 shows the classification models followed by the various SPAs:

Table 27-5 SPA-Based Matrix for Ingress Classification at the SIP or SPA level

Classification at the SPA Level	Classification at the SIP Level
Ethernet SPAs <ul style="list-style-type: none"> • SPA-4X1FE-TX-V2 • SPA-8X1FE-TX-V2 • SPA-2X1GE-V2 • SPA-5X1GE-V2 • SPA-8X1GE-V2 • SPA-10X1GE-V2 • SPA-1X10GE-L-V2 	Serial and Channelized SPA <ul style="list-style-type: none"> • SPA-2XCT3/DS0 • SPA-4XCT3/DS0 • SPA-8XCHT1/E1 • SPA-1XCHSTM1/OC3 • SPA-1XCHOC12/DS0 • SPA-2xT3/E3 • SPA-4xT3/E3 • SPA-4xT-SERIAL
ATM SPAs <ul style="list-style-type: none"> • SPA-1XOC3-ATM-V2 • SPA-3XOC3-ATM-V2 • SPA-1XOC12-ATM-V2 	POS SPAs <ul style="list-style-type: none"> • SPA-2XOC3-POS • SPA-4XOC3-POS • SPA-1XOC12-POS • SPA-2XOC12-POS • SPA-4XOC12-POS • SPA-8XOC12-POS • SPA-8XOC3-POS • SPA-1XOC48POS/RPR • SPA-2XOC48POS/RPR • SPA-4XOC48POS/RPR • SPA-OC192POS-XFP

SPA-Based Classification

Ethernet and ATM SPAs perform classification at the SPA level. In the SPA-based classification model, the SPA performs both L2 and L3 classification, and decides on the priority of the packet. After classifying the packets into high priority and low priority, the SPA has unique SPI4 channels per priority, and all the high-priority packets are sent on separate SPI4 channels other than the low-priority SPI4 channel. In such a scenario, the SPA queues the packets on high SPI4 channels to high-priority buffers and low-SPI4 channels to low-priority buffers. After the packets are classified into high priority and low priority, the packets are sent to the ESP for further processing.

SIP-Based Classification

POS SPAs, channelized, and clear-channel SPAs support packet classification at SIP level. In SIP-based classification, the SIP does the classification for SPAs and classifies the packet into high-priority and low-priority.

Commands have been introduced in Release 3.1S to configure SIP based classification. To classify high-priority packets such as IPv4, IPv6, or MPLS, in a SIP or SPA, the classification template is defined using the **ingress-class map index** command. The classification template-specific details are defined inside the template, and the template is attached to an interface using the **plim qos class-map index** command.

Default Classification

Commands are used to configure the L3 packet classification criteria. If no L3 classification rule has been configured, the SIP classifies the packet with the following L3 settings as high priority by default:

- IPv4 DSCP-based— If no values are specified as high priority for IPv4 DSCP values, the system considers packets with DSCP EF as high priority.
- IPv4 precedence-based— If no values are specified as high priority for IPv4 precedence values, the system considers packets with precedence 6-7 as high priority.
- IPv6 TC-based— If no values are specified as high-priority for IPv6 DSCP values, the system considers packets with DSCP EF as high priority.
- MPLS EXP bits— If no values are specified as high-priority for MPLS EXP values, the system considers packets with EXP values 6-7 as high priority.

High Availability and Online Insertion and Removal

- CLI configured under an interface are retained after SPA online-insertion-and-removal (OIR). When one type of SPA is replaced by another type of the SPA, the interface configuration is not retained. However, if the earlier SPA type is reinserted, the configuration added on that SPA type is restored.
- All the configurations are synced to the standby route processor (RP). Hence, the router configuration is retained even after the RP switchover.

Configuring the Ingress Classification

The following section provides configuration details for classifying IPv4, IPv6, and MPLS packets for POS, serial, channelized, and clear-channel SPAs.

Defining the L3 Classification Template

To classify high-priority packets such as IPv4, IPv6, or MPLS in either a SIP or SPA, the classification template is defined using the **ingress-class map** *index* command. The classification rules are defined inside the template, and the template is attached to an interface using the **plim qos input class-map** *index-id* command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ingress-class-map** *{index-id}*
4. **interface** {POS | Serial} *interface-path-id*
5. **plim qos input class-map** *index-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters the global configuration mode.
Step 3	ingress-class-map <i>index-id</i> Example: Router(config)# ingress-class-map 1	Creates a classification template for L3 classification for POS, channelized, and clear-channel SPAs.
Step 4	interface {POS Serial} <i>interface-path-id</i> Example: Router(config)# interface POS 0/2/0	Enters the interface configuration mode and specifies the POS or Serial interface name with the notation <i>slot/sub-slot/interface-id</i> . Possible interface types for this procedure are: <ul style="list-style-type: none"> • POS • Serial Note The example indicates a 0 port in the POS SPA adapter at sub-slot 2 in the SIP at slot 0.
Step 5	plim qos input class-map <i>index-id</i> Example: Router(config-if)# plim qos input class-map 1	Attaches the ingress classification class-map template with the specified <i>index-id</i> to the POS or Serial interface.

Classifying IPv4 Packets

To configure and verify IPv4 packets as either high or low based on either the DSCP value or precedence value, execute the following set of commands in the Configuration ingress class map mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ingress-class-map index-id**
4. **map ip all queue strict-priority**
5. **map ip dscp-based**
6. **map ip dscp dscp-value queue 0**
7. **map ip precedence-based**
8. **map ip precedence precedence-value queue strict-priority**
9. **exit**
10. **interface {POS | Serial} *interface-path-id***
11. **plim qos input class-map *index-id***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ingress-class-map index-id Example: Router(config-ing-class-map)# ingress-class-map 1	Enters the ingress classification template settings for the specified template ID and enables the configuration of the classifications for IPv4, IPv6, or MPLS.
Step 4	map ip all queue strict-priority Example: Router(config-ing-class-map)# map ip all queue strict-priority	Sets the priority for all IPv4 packets as high.
Step 5	map ip dscp-based Example: Router(config-ing-class-map)# map ip dscp-based	Enables classification based on the DSCP value in IPv4.
Step 6	map ip dscp dscp-value queue 0 Example: Router(config-ing-class-map)# map ip dscp cs1 cs2 queue 0	Classifies IPv4 packets, with DSCP values cs1 and cs2 as low-priority packets.
Step 7	map ip precedence-based Example: Router(config-ing-class-map)# map ip precedence-based	Enables classification for IPv4 packets based on IP precedence.
Step 8	map ip precedence precedence-value queue strict-priority Example: Router(config-ing-class-map)# map ip precedence 5 7 queue strict-priority	Classifies the IPv4 packets, with precedence values 5 and 7 as strict priority.
Step 9	exit Example: Router(config-ing-class-map)# exit	Exits the ingress-class-map mode and goes back to the global configuration mode.

	Command or Action	Purpose
Step 10	<pre>interface {POS Serial} interface-path-id</pre> <p>Example: Router(config)# interface POS 0/2/0</p>	<p>Enters the interface configuration mode and specifies the POS or Serial interface name with the notation <i>slot/sub-slot/interface-id</i>. Possible interface types for this procedure are:</p> <ul style="list-style-type: none"> • POS • Serial <p>Note The example indicates a 0 port in the POS SPA adapter at sub-slot 2 in the SIP at slot 0.</p>
Step 11	<pre>plim qos input class-map index-id</pre> <p>Example: Router(config-if)# plim qos input class-map 1</p>	<p>Attaches the ingress classification class-map template with the specified index-id to the POS or Serial interface.</p>

Classifying IPv6 Packets

To classify all the IPv6 packets as either high priority or low priority, or to classify the IPv6 packets with specific traffic class values such as high or low, execute the following set of commands in the Configuration ingress class map mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ingress-class-map index-id**
4. **map ipv6 all queue**
5. **map ipv6 tc af43 strict-priority**
6. **exit**
7. **interface {POS | Serial} interface-path-id**
8. **plim qos input class-map index-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ingress-class-map 1 Example: Router(config-ing-class-map)#	Enters the ingress classification template settings for the specified template ID and enables the configuration of the classifications for IPv4, IPv6, or MPLS.
Step 4	map ipv6 all queue strict-priority Example: Router(config-ing-class-map)# map ipv6 all queue strict-priority	Sets the priority for all IPv6 packets as high.
Step 5	map ipv6 tc tc-value queue strict-priority Example: Router(config-ing-class-map)# map ipv6 tc af43 queue strict-priority	Classifies IPv6 traffic class values with af43 as high priority.
Step 6	exit Example: Router(config-ing-class-map)# exit	Exits the ingress-class-map mode and goes back to the global configuration mode.
Step 7	interface {POS Serial} interface-path-id Example: Router(config)# interface POS 0/2/0	Enters the interface configuration mode and specifies the POS or Serial interface name with the notation <i>slot/sub-slot/interface-id</i> . Possible interface types for this procedure are: <ul style="list-style-type: none"> • POS • Serial Note The example indicates a 0 port in the POS SPA adapter at sub-slot 2 in the SIP at slot 0.
Step 8	plim qos input class-map index-id Example: Router(config-if)# plim qos input class-map 1	Attaches the ingress classification class-map template with the specified index-id to the POS or Serial interface.

Classifying MPLS Packets

To classify either all the MPLS packets or the MPLS packets based on EXP bits of the MPLS header as either high or low, execute the following set of commands in the Configuration ingress class map mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ingress-class-map index-id**
4. **map mpls all queue**
5. **map mpls exp exp-value queue strict-priority**
6. **exit**
7. **interface {POS | Serial} interface-path-id**
8. **plim qos input class-map index-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ingress-class-map 1 Example: Router(config-ing-class-map)#	Enters the ingress classification template settings for the specified template ID and enables configuration of the classifications for IPv4, IPv6, or MPLS.
Step 4	map mpls all queue strict-priority Example: Router(config-ing-class-map)# map mpls all queue strict-priority	Sets the priority for all MPLS packets as high priority.
Step 5	map mpls exp exp-value queue strict-priority Example: Router(config-ing-class-map)# map mpls exp 1 queue strict-priority	Classifies MPLS packets with EXP value 1 as high.
Step 6	exit Example: Router(config-ing-class-map)# exit	Exits the ingress-class-map mode and goes back to the global configuration mode.

	Command or Action	Purpose
Step 7	interface {POS Serial} interface-path-id Example: Router(config)# interface POS 0/2/0	Enters the interface configuration mode and specifies the POS or Serial interface name with the notation <i>slot/sub-slot/interface-id</i> . Possible interface types for this procedure are: <ul style="list-style-type: none"> • POS • Serial Note The example indicates a 0 port in the POS SPA adapter at sub-slot 2 in the SIP at slot 0.
Step 8	plim qos input class-map index-id Example: Router(config-if)# plim qos input class-map 1	Attaches the ingress classification class-map template with the specified index-id to the POS or Serial interface.

Classifying Inner or Outer VLAN COS Values

To enable packet classification based on VLAN COS values for Inner or Outer VLAN of a 802.1Q subinterface or qinq subinterface, execute the following set of commands from QinQ subinterface configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitEthernet 0/0/0.1**
4. **plim qos input map cos inner-based**
5. **plim qos input map cos inner 5 6 queue strict-priority**
6. **plim qos input map cos outer-based**
7. **plim qos input map cos outer 4 queue strict-priority**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface gigabitEthernet 0/0/0.1 Example: Router(config)# interface gigabitEthernet 0/0/0.1	Enters the subinterface mode for Gigabit Ethernet 0/0/0.1.
Step 4	plim qos input map cos inner-based Example: Router(config-subif)# plim qos input map cos inner-based	Enables and allows configuration for inner VLAN COS values. Note The VLAN COS values can be enabled by default by executing the plim qos input map enable command.
Step 5	plim qos input map cos inner 5 6 queue strict-priority Example: Router(config-subif)# plim qos input map cos inner 5 6 queue strict-priority	Configures the COS values or the range of the inner VLAN of a qinq subinterface to high priority.
Step 6	plim qos input map cos outer-based Example: Router(config-subif)# plim qos input map cos outer-based	Enables configuration for outer VLAN COS values. Note The VLAN COS values can be enabled by default by executing the command plim qos input map enable .
Step 7	plim qos input map cos outer 4 queue strict-priority Example: Router(config-subif)# plim qos input map cos outer 4 queue strict-priority	Configures the COS values or range for outer-vlan of a qinq sub-interface to high-priority.

Information About Ingress Scheduling

The following sections provide details regarding the Ingress Scheduling feature:

- [Scheduling Overview, page 27-17](#)
- [Intra-CC Scheduling, page 27-17](#)

- [Inter-CC Scheduling, page 27-17](#)
- [Behavioral Changes in Scheduling, page 27-17](#)
- [Configuring Intra-CC Scheduling, page 27-18](#)
- [Configuring Inter-CC Scheduling, page 27-20](#)

Scheduling Overview

The ASR 1000 Series Routers support ingress oversubscription. After the ingress packets are classified as high priority and low priority, the packets are scheduled according to the priority. The ingress classification and scheduling features have to work in conjunction to handle oversubscription. Bandwidth oversubscription occurs at two levels, the SIP level (intra carrier card scheduling) and at ESP (inter carrier card scheduling) level. The decision to configure scheduling at the SIP level is based on the number of SPAs within a SIP and the scheduling decision to configure the scheduling at either SIP or ESP level is based on the number of SIPs in a router. The following section describes intra-CC scheduling and inter-CC scheduling.

Intra-CC Scheduling

Under intra-CC scheduling, the high-priority packets that are already classified by the SIP or the SPA are scheduled and processed first. By default, all high-priority packets are processed first, and then the excess bandwidth is shared among the low-priority packets, based on either the weight assigned to the interface or the entire SPA. Configuring weights provides an option in distributing the excess bandwidth among different interfaces to schedule low priority packets. Intra-CC scheduling is supported in all SPAs, SIP-10, and SIP-40.

To assign excess weight to a clear-channel SPA (POS, ATM, Ethernet, or Serial SPAs), execute the **plim qos input [weight weight]** command from Main interface configuration mode. This command was earlier supported on only Ethernet SPAs. From Cisco IOS XE Release 3.1S onwards, the command is supported on all clear-channel SPA on Cisco ASR 1000 Series Router.

To assign excess weight to low-priority packets on channelized SPAs, execute the **hw-module subslot {slot/subslot} qos [weight weight]** command in Global configuration mode.

Inter-CC Scheduling

Oversubscription occurs at both the SIP level and the ESP level. Inter-CC scheduling has been introduced to handle the oversubscription at the ESP level. In this scenario, the traffic sent from all the SIPs to the ESP. It is not mandatory to configure scheduling at the ESP level. It depends on the number of SIPs connected to the ESP. Inter-CC scheduling is needed whenever an oversubscription situation is encountered or there is a need to prioritize certain traffic or there is a need to give different bandwidth allocation to different types of traffic. To configure the minimum bandwidth service for the SIP and distribute the excess weight to the low priority packets on the per ESI link per CC, execute the **hw-module slot slot-number qos input link link-index {bandwidth value | weight weight}** command from the Global configuration mode.

Behavioral Changes in Scheduling

In Cisco IOS XE Release 6.0 and earlier images, by default, the SIP-10 scheduler and the ESP scheduler ran in port-fairness and ESP-fairness mode where each buffer is scheduled at a rate proportional to its interface bandwidth. As a result, even high-priority packets were treated based on a rate that was

proportional to its interface bandwidth. In Cisco IOS XE Release 3.1S, the SIP-10 scheduler, SIP-40 scheduler, and ESP scheduler ran in strict-priority mode. In this mode, if the high-priority queues of either a participating SPA port or a participating SIP has data to send, these queues will be scheduled first. The remaining bandwidth, if any, will then be shared among the low-priority buffers at a weight that is proportional to the interface bandwidth or at a weight that is equal to the weight of all the SIPs.

The supported excess weight range from Cisco IOS XE Release 3.1S and onwards for intra-SIP scheduling is as follows:

- SIP-10— 40 to 10000
- SIP-40— 40 to 10000

The supported minimum bandwidth range from Cisco IOS XE Release 3.1S and onwards for Inter-SIP scheduling depends on the combination of SIP and ESP. Following is the range for minimum bandwidth configuration for various combination of SIP and ESP:

- SIP-10 with all ESP: 1 Mbps to 11.2 Gbps
- SIP-40 with ESP10/ESP20: 1 Mbps to 11.2 Gbps
- SIP-40 with ESP40: 1Mbps to 23 Gbps on each ESI link

The supported excess weight range for inter carrier card scheduling (ESP level) is as follows:

- All ESPs— 50 to 100

Configuring Intra-CC Scheduling

By default, ingress packets that are classified as high-priority by a SIP or SPA, are processed first, and then sent. After processing the high-priority packets, the available excess bandwidth can be shared by low-priority packets depending on the weight assigned to the interface or to the SPA. Execute the following commands to configure the weight on an interface or for the entire SPA:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet 0/0/2**
4. **plim qos input [weight weight]**
5. **hw-module subslot *slot/subslot* qos input [weight weight]**
6. **show platform hardware {*slot/subslot/port*} plim qos input bandwidth**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface gigabitEthernet 0/0/0 Example: Router(config-if)# interface gigabitEthernet 0/0/0	Enters the interface configuration mode for Gigabit-Ethernet 0/0/0.
Step 4	plim qos input weight 100 Example: Router(config-if)# plim qos input weight 100	Assigns excess weight of 100 for bandwidth distribution to the Gigabit Ethernet 0/0/0. Note The plim qos input weight command is applicable for only clear-channel SPAs.
Step 5	exit Example: Router(config-if)# exit	Exits from the interface configuration mode, and goes back to the configuration mode.
Step 6	hw-module subslot 0/1 qos input weight 150 Example: Router(config)# hw-module subslot 0/1 qos input weight 150	Assigns excess weight of 150 for bandwidth distribution to the channelized SPA at slot 0/1. Note The hw-module subslot 0/1 qos input weight 150 command is applicable for all the channelized SPAs. The excess weight is assigned to all the channelized SPAs, while for clear-channel SPAs, weight is assigned to the SPA interface.

	Command or Action	Purpose
Step 7	exit	Exits from the configuration mode and goes back to the privilege execution mode.
	Example: Router#	
Step 8	show platform hardware slot 0 plim qos input bandwidth	Displays the interface-level excess weight configured for all the interfaces of all the SPAs, present in Slot 0.
	Example: Router# show platform hardware slot 0 plim qos input bandwidth Ingress QOS Scheduling Mode: Strict Priority 0/0, SPA-5X1GE-V2 Interface 0/0/0 BW: 1000000 Kbps, Min BW: N/A , Excessive Weight: 100000 Kbps, HP Polices Interface 0/0/1 BW: 1000000 Kbps, Min BW: N/A , Excessive Weight: 1000000 Kbps, HP Polices Interface 0/0/2 BW: 1000000 Kbps, Min BW: N/A , Excessive Weight: 1000000 Kbps, HP Polices Interface 0/0/3 BW: 1000000 Kbps, Min BW: N/A , Excessive Weight: 1000000 Kbps, HP Polices Interface 0/0/4 BW: 1000000 Kbps, Min BW: N/A , Excessive Weight: 1000000 Kbps, HP Polices 0/1, SPA-1XCHOC12/DS0 BW: 619968 Kbps, Min BW: N/A , Excessive Weight: 150000 Kbps, HP Polices 0/2, SPA-2XCT3/DS0 BW: 88384 Kbps, Min BW: N/A , Excessive Weight: 88000 Kbps, HP Polices	

Configuring Inter-CC Scheduling

The ESP-level scheduling feature helps to assign minimum guaranteed bandwidth for the entire SIP, and to assign a specific weight to the SIP for distribution of the excess bandwidth. Execute the following commands to either assign the minimum guaranteed bandwidth or to configure the weight for the entire SIP for excess bandwidth distribution:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hw-module slot *slot-number* qos input link *link-index* bandwidth *value_in_Kbps***
4. **hw-module slot *slot-number* qos input link *link-index* weight *weight***
5. **show platform hardware slot f0 serdes qos**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	hw-module slot 1 qos input link A bandwidth 512 Example: Router(config)# hw-module slot 1 qos input link A bandwidth 512	Assigns a guaranteed minimum bandwidth of 512 Kbps for ESI link A.
Step 4	hw-module slot 1 qos input link A weight 50 Example: Router(config)# hw-module slot 1 qos input link A weight 50	Assigns excess weight of 50 to the ESI link A of the SIP.
Step 5	exit Example: Router(config-if)# exit	Exits from the configuration mode and goes back to the privilege execution mode.
Step 6	show platform hardware slot f0 serdes qos Example: Router# show platform hardware slot f0 serdes qos Qos Settings on FP: slot # Min BW (Kbps) Min BW Mode Slot Weight RP0 99975 HILO 256 SIP0 11199981 HI 50	Displays the minimum guaranteed bandwidth and weight configured for all the SIP slots.



GLOSSARY

A

- ARPA** Advanced Research Projects Agency of the U.S. Department of Defense. ARPA funded research and experimentation with ARPANET, the predecessor to the Internet.
- ATM** Asynchronous Transfer Mode

B

- blank filler plate** An empty panel used to fill vacant subslots on a SIP. For proper operation, a SIP should be fully installed with either functional SPAs or blank filler plates.

F

- FPD** field-programmable device. General term for any hardware component implemented on router cards that supports separate software upgrades. SIPs and SPAs must have the correct FPD version to function properly; an FPD incompatibility will disable all interfaces on the SPA or all SPAs within the SIP.
- FPD image package** A software file used to upgrade FPD images. Whenever a Cisco IOS image is released that supports SPAs, a companion SPA FPD image package is also released for that Cisco IOS software release.

L

- LAN** local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

M

- MAC** media access control. Lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media.
- MIB** Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

O

- OIR** online insertion and removal. Feature supported by SIPs and SPAs allowing removal of the cards while the router and the cards are activated, without affecting the operation of other cards or the router. Although this removal can be done while the SIP or SPA is activated, it is generally recommended that you gracefully deactivate the hardware using the appropriate commands for your platform prior to removal of the hardware.

P

- PPP** Point-to-Point Protocol. A link-layer encapsulation method for dialup or dedicated circuits.

Q

- QoS** quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

S

- SFP** small form-factor pluggable optical transceiver. A type of fiber optic receptacle device that mounts flush with the front panel to provide network connectivity.
- single height** Describes the dimension of a SPA that occupies a single SIP subslot, or half of the SIP.

SIP	SPA interface processor. A SIP is a platform-specific carrier card that inserts into a router slot like a line card. A SIP can hold one or more SPAs in its subslots, depending on the SIP type. The SPA provides the network interface. The SIP provides the connection between the Route Processor (RP) and the SPA.
SNMP	Simple Network Management Protocol. The protocol governing network management and monitoring of network devices and their functions.
SPA	shared port adapter. A SPA is a modular, platform-independent port adapter that inserts into a subslot of a compatible SIP carrier card to provide network connectivity and increased interface port density. The SPA provides the interface between the network and the SIP.
subslot	Slot on a SIP where a SPA is installed. The primary slot is the chassis slot on the where the SIP is installed.

V

VLAN	Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. See also <i>LAN</i> .
-------------	---



INDEX

Symbols

<cr> [1-7](#)

? command [1-7](#)

Numerics

1-Port Channelized STM-1/OC-3 SPA

configuring

channelized DS3 mode [19-8](#)

DS1, channelized T3 mode [19-9](#)

E1, channelized T3/E3 mode [19-12](#)

SDH mode [19-6](#)

SONET mode [19-4](#)

creating the interface, SONET [19-4](#)

interface names [19-3](#)

SDH mode [19-3](#)

selecting the physical port [19-2](#)

SONET mode [19-3](#)

2-Port and 4-Port Channelized T3 SPA

configuring [16-1](#)

configuring data service unit mode [16-8](#)

configuring encapsulation [16-11](#)

configuring FDL [16-13](#)

configuring maintenance data link [16-9](#)

configuring scramble [16-15](#)

specifying interface address [16-7](#)

T3 framing [16-13](#)

verifying the configuration [16-16](#)

2-Port and 4-Port Clear Channel T3/E3 SPAs

configuring [17-1](#)

configuring cable length [17-13](#)

configuring data service unit mode [17-5](#)

configuring encapsulation [17-12](#)

configuring framing [17-11](#)

configuring maintenance data link [17-7](#)

configuring scramble [17-9](#)

interface addresses [17-5](#)

4-Port Serial Interface SPA

configuring [18-2](#)

show commands [18-3](#)

specifying interface address [18-7](#)

verifying configuration [18-2](#)

verifying the interface configuration [18-12](#)

8-Port Channelized T1/E1 SPA

configuring [15-1](#)

configuring CRC [15-10](#)

configuring FDL [15-11](#)

encapsulation [15-9](#)

framing [15-8](#)

setting IP address [15-6](#)

verifying the configuration [15-13](#)

A

activation

verifying for SIPs [5-4](#)

verifying for SPAs [5-8](#)

administratively down state [10-15](#)

Advanced Research Projects Agency. See ARPA.

associate application sccp command [25-4](#)

Asynchronous Transfer Mode. See ATM.

ATM

AIS [8-6](#)

FERF [8-6](#)

HCSE [8-6](#)



line coding errors [8-6](#)

LOF [8-6](#)

RAI [8-6](#)

SPA system messages [8-6](#)

ATMSPA system messages [8-6](#)

automatic SPA FPD image upgrade

(example) [26-7](#)

disabling [26-3](#)

re-enabling [26-4](#)

autonegotiation

configuring [10-10](#)

disabling on fiber interfaces [10-11](#)

enabling on fiber interfaces [10-12](#)

B

blank filler plate

for empty subslots in a SIP [2-1](#)

single-height size [2-3](#)

C

carriage return (<cr>) [1-7](#)

cautions, usage in text [i-xxviii](#)

CEF [6-1, 7-1, 8-1, 23-1](#)

CEF for PFC2

See CEF

channel group, changing configuration [15-12](#)

channelized DS3 mode, configuring [19-8](#)

Cisco ASR 1000 Series Routers

SIP description [3-2](#)

SIP features [3-2](#)

Cisco Discovery Protocol [10-12](#)

Cisco IOS configuration changes, saving [1-10](#)

Cisco MIB Locator [9-6](#)

CLI [1-1](#)

clock signal, inverting [18-9](#)

codec (DSP profile) command [25-3](#)

command-line interface. See CLI.

command line processing [1-5](#)

command modes [1-6](#)

command modes, understanding [1-6](#)

commands

context-sensitive help for abbreviating [1-7](#)

debug [5-1](#)

default form, using [1-10](#)

hardware module slot [4-3](#)

no form, using [1-10](#)

resetting a SIP [4-3](#)

show [5-2](#)

show interfaces serial

troubleshooting serial lines [20-4](#)

command syntax

conventions [i-xxvii](#)

displaying (example) [1-7](#)

conditions - status line, show interfaces serial
command [20-3](#)

configurations, saving [1-10](#)

configuration tasks, required

4-Port Serial Interface SPA [18-2](#)

for the Fast Ethernet SPA [10-2](#)

for the Gigabit Ethernet SPA [10-2](#)

configure terminal command [10-2](#)

configuring SPAs

Fast Ethernet [10-1](#)

copy command [10-15](#)

course wave division multiplexer (CWDM)



Optics Compatibility [2-7](#)

optics compatibility [2-7](#)

qualified optics modules [2-7](#)

CRC, configuring [15-10, 18-10](#)

CRC size, configuring [19-16](#)

cyclic redundancy checking. See CRC.

D

data service unit mode, configuring [16-8](#)

deactivation

 verifying for SIPs [5-4](#)

 verifying for SPAs [5-8](#)

debug atm errors command [8-2](#)

debug atm events command [8-2](#)

debug atm oam command [8-2](#)

debug command [5-1, 11-2](#)

debug hw-module subslot command [11-2](#)

dense wave division multiplexer (DWDM)

 optics compatibility [2-8](#)

 qualified optics modules [2-8](#)

description (DSP profile) command [25-3](#)

dot1q encapsulation [10-10](#)

 configuration (example) [10-35](#)

 configuring [10-12](#)

DS1, configuring [19-9](#)

dspfarm profile command [25-3, 25-5](#)

dsp services dspfarm command [25-3](#)

E

E1, channelized T3/E3, configuring [19-12](#)

encapsulation

 ARPA [10-10](#)

configuring [10-10, 19-15](#)

dot1q [10-10](#)

 configuration (example) [10-35](#)

 configuring [10-12](#)

SNAP [10-6, 10-10](#)

encapsulation, configuring [15-9, 16-11, 17-12, 18-10](#)

encapsulation dot1q command [10-13](#)

error messages [5-1](#)

event tracer feature [8-9, 23-15](#)

F

FDL, configuring [15-11, 16-13, 19-17](#)

field-programmable devices (FPDs)

 displaying image versions [26-5](#)

 manually upgrading SIP and SPA images [26-4](#)

 upgrades [26-1](#)

field-programmable devices. See FPD.

filtering output, show and more commands [1-10](#)

for [10-17](#)

FPD image packages

 displaying default information [26-6](#)

 overview [26-2](#)

FPD images

 displaying minimum and current versions [26-5](#)

 manually upgrading [26-4](#)

 troubleshooting upgrades [26-9 to 26-12](#)

 upgrade failure recovery (example) [26-10 to ??](#)

 upgrading in production [26-2 to 26-4](#)

 verifying successful upgrade [26-12](#)

 verifying upgrade progress [26-7](#)

FPD image upgrades [26-2](#)

 examples [26-7](#)



troubleshooting [26-9](#)

FPDs

- description [26-1](#)
- framing, configuring [15-8, 16-13, 17-11](#)

G

- giant packets [7-5](#)
- Gigabit Ethernet SPAs
 - configuring [10-1](#)
 - features supported [9-2](#)
 - MAC address [10-4](#)
 - modifying MTU [10-6](#)
 - QoS [10-7](#)
 - SPA automatic recovery [11-6](#)
 - troubleshooting [11-1](#)
 - using show commands [10-16](#)
 - VLAN [10-12](#)
- global configuration mode, summary of [1-6](#)

H

- hardware platforms
 - See* platforms, supported
- help command [1-7](#)
- Hot Standby Router Protocol . *See* HSRP.
- HSRP, verifying configuration [10-5](#)
- hw-module slot start command [5-4, 5-9](#)
- hw-module slot stop command [5-3](#)
- hw-module subslot start | stop | reload command [5-3](#)
- hw-module subslot command [10-15](#)
- hw-module subslot shutdown command [5-7, 5-8, 5-9](#)

I

- IEEE 802.1Q encapsulation [10-10](#)
 - configuration (example) [10-35](#)
 - configuring [10-12](#)
- images
 - FPD [26-2](#)
 - upgrading [26-2](#)
 - upgrading multiple FPD [26-2](#)
- interface
 - basic configuration (example) [10-33](#)
 - enabling [10-3](#)
 - restarting [10-15](#)
 - shutting down [10-15](#)
 - verifying configuration [10-15 to 10-16](#)
- interface address, specifying [10-4](#)
- interface configuration mode, summary of [1-6](#)
- interface gigabitethernet command [10-2, 10-13, 22-5](#)
- interface status line - states, show interfaces serial command [20-3](#)
- interface tengigabitethernet command [10-2, 10-13](#)
- invert the data stream [15-11](#)
- ip address command [10-2, 10-13](#)

K

- keyboard shortcuts [1-5](#)

L

- lines - interface status [20-3](#)
- lines - states, show interfaces serial command [20-3](#)
- loopback command [8-6](#)



loopback commands, using [18-6](#)

loopback diagnostic command [8-6, 8-8](#)

loopback line command [8-8](#)

M

MAC address

configuration (example) [10-33](#)

modifying [10-4](#)

verifying [10-4](#)

MAC address accounting, configuration example [10-34](#)

maintenance data link, configuring [16-9](#)

Management Information Base (MIB)

downloading [9-6](#)

supported on SIP [3-3](#)

supported on SPAs [9-6](#)

maximum sessions command [25-4](#)

MIB. See Management Information Base.

modes. *See* command modes

mpls mtu command [10-6, 13-2](#)

MTU (maximum transmission unit)

configuration (example) [10-34](#)

default size [10-6](#)

interface MTU

additional overhead [10-6](#)

configuration guidelines [10-6](#)

configuring [10-7](#)

description [10-6](#)

verifying [10-7](#)

IP MTU, description [10-6](#)

maximum size [10-6](#)

MPLS MTU, description [10-6](#)

tag MTU, description [10-6](#)

types [10-6](#)

mtu command [10-3, 10-7](#)

N

negotiation auto command [10-12](#)

no hw-module subslot shutdown command [5-9](#)

no negotiation auto command [10-11, 10-12](#)

non-return-to-zero inverted. See NRZI.

nonvolatile random-access memory. See NVRAM.

no shut command [10-3](#)

notes, usage in text [i-xxviii](#)

no upgrade fpd auto command [26-3](#)

NRZI, configuring [18-9](#)

NVRAM [10-15](#)

O

OIR (online insertion and removal)

and shutting down or restarting interfaces [10-15](#)

event tracing for SPAs [8-9, 23-15](#)

for SIPs [2-1, 5-3](#)

for SPAs [2-3, 5-5](#)

troubleshooting [8-9, 23-15](#)

online insertion and removal. See OIR.

optics modules

qualified for SPAs (table) [2-5, 2-6, 2-7, 2-8](#)

P

packet flow, on Fast Ethernet or Gigabit Ethernet
SPA [9-7 to 9-8](#)

Packet over SONET (POS) SPAs [12-1](#)

alarm trigger delays [13-9](#)



architecture [12-6](#)

configuring [13-1, 22-1, 25-1](#)

framing [13-3](#)

interface address [13-1](#)

keepalive [13-5](#)

modifying CRC size [13-6](#)

payload scrambling [13-8](#)

restrictions [12-5](#)

supported features [12-3](#)

ping command [8-4, 23-15](#)

platforms, supported - release notes [1-11](#)

privileged EXEC mode, summary of [1-6](#)

prompts, system [1-6](#)

Q

question mark (?) command [1-7](#)

R

release history

Fast Ethernet SPAs [9-2](#)

Gigabit Ethernet SPAs [9-2](#)

SIP [3-1](#)

ROM monitor mode, summary of [1-6](#)

router console [1-1](#)

connecting [1-2](#)

running configuration, saving to NVRAM [10-15](#)

S

saving configuration changes [1-10](#)

scramble, configuring [16-15, 17-9](#)

SDH mode, configuring [19-6](#)

serial lines

troubleshooting

show interfaces serial command [20-4](#)

Serial SPAs

2-Port and 4-Port Channelized T3 SPA [16-1](#)

2-Port and 4-Port Clear Channel T3/E3 SPAs [17-1](#)

8-Port Channelized T1/E1 SPA [15-1](#)

release history [14-1](#)

restrictions [14-4](#)

serial SPAs

1-Port Channelized STM-1-OC-3 [19-1](#)

4-Port Serial Interface SPA [18-1](#)

SFP (small form-factor pluggable) optics

Cisco qualification check [2-5](#)

qualified for SPAs (table) [2-5, 2-6, 2-7, 2-8](#)

SFP-GE-T

speed and duplex configuration [10-11](#)

shared port adapter. See SPA.

show atm interface atm command [7-8](#)

show atm pvc command [7-11](#)

show atm pvc interface atm command [8-6](#)

show atm traffic shaping slot command [8-6](#)

show atm vc interface atm command [7-11](#)

show command [11-2](#)

show controllers atm command [6-6](#)

example [6-10](#)

show controllers command [6-9](#)

show diag slot command [4-2](#)

show diag sub-slot command [4-2](#)

show history command [1-5](#)

show hw-module subslot all oir command [5-8](#)

show hw-module subslot command [26-5](#)

show hw-module subslot fpd command [26-10](#)



show hw-module subslot service-engine status

example [21-6](#)

show hw-module subslot service-engine status
command [21-6](#)

show hw-module subslot transceiver idprom
command [10-16, 10-17](#)

show interface command [7-6](#)

show interfaces atm command [7-5](#)

example [6-10](#)

show interfaces command [6-9, 9-8, 11-2](#)

show interface serial command [19-14](#)

show interface service-engine command [21-6](#)

example [21-6](#)

show interfaces fastethernet [11-2](#)

show interfaces gigabitethernet command [10-4, 10-7, 11-2](#)

show interfaces serial command [20-4](#)

show interfaces tengigabitethernet command [9-8, 11-2](#)

show ip interface command [5-8, 7-6](#)

show module command [5-4](#)

show mpls interface command [7-6](#)

show platform command [4-2](#)

show standby command [10-5](#)

show upgrade package default command [26-6](#)

show upgrade progress command [26-7](#)

show vlans command [10-14](#)

shutdown command [10-15](#)

SIP (SPA interface processor)

activation (example) [5-9](#)

blank filler plates [2-1](#)

configuring [4-1](#)

deactivating [5-3](#)

deactivation (example) [5-8](#)

definition [2-1](#)

features supported [3-2](#)

general characteristics [2-1](#)

hardware type, displaying [?? to 3-3](#)

identifying slots and subslots [4-1](#)

reactivating [5-3](#)

release history [3-1](#)

SPA compatibility (table) [2-3, 2-4](#)

subslots

description [2-1](#)

numbering [4-2](#)

specifying location in CLI [4-2](#)

troubleshooting [5-1](#)

SNAP (Subnetwork Access Protocol) encapsulation [10-6, 10-10](#)

SONET mode, configuring [19-4](#)

SPA (shared port adapter)

activation (example) [5-9](#)

architecture, description [9-7](#)

automatic recovery [11-6](#)

deactivating [5-6](#)

deactivation (example) [5-9](#)

definition [2-2](#)

double-height description [2-2](#)

FPD image packages, overview [26-2](#)

Gigabit Ethernet [9-1](#)

interfaces [2-2](#)

online removal [5-5](#)

optics compatibility (table) [2-5, 2-6, 2-7, 2-8](#)

POS SPA architecture [12-6](#)

reactivating [5-7](#)

single-height description [2-2](#)

SIP compatibility (table) [2-3, 2-4](#)

SPA architecture

description [?? to 9-8](#)

POS SPA description [?? to 12-8](#)



SPA hardware type, displaying [9-8](#)

SPA interface processor. See SIP.

states - interface status line, show interfaces serial command [20-3](#)

subinterfaces, configuring [10-12 to 10-13](#)

Subnetwork Access Protocol. See SNAP.

subslots

- description [2-1](#)

- numbering [4-2](#)

- specifying location in CLI [4-2](#)

syntax [1-7](#)

configuring on a subinterface [10-12](#)

verifying configuration [10-14](#)

voice-card command [25-3](#)

T

Tab key, command completion [1-7](#)

telnet [1-3](#)

timing signals, configuring [18-7](#)

tips, usage in text [i-xxviii](#)

troubleshooting

- Fast Ethernet SPA [11-1](#)

- Gigabit Ethernet SPA [11-1](#)

U

unchannelized E3 serial interface, configuring [19-13](#)

upgrade fpd auto command [26-4, 26-7](#)

upgrade hw-module subslot command [26-4](#)

user EXEC mode, summary of [1-6](#)

V

virtual LAN. See VLAN.

VLANs (virtual LANs)

- configuration (example) [10-35](#)