CONTENTS

CHAPTER 1

Getting Started With the Cisco ASR 920 Series Router 1
  Overview 1
  Restrictions 3
  Interface Naming 3
  Interface Speed Based on Port Type 6
  VCoP Optics Support 7

CHAPTER 2

Using Cisco IOS XE Software 9
  Understanding Command Modes 9
  Accessing the CLI Using a Router Console 11
  Using Keyboard Shortcuts 11
  Using the History Buffer to Recall Commands 11
  Getting Help 12
    Finding Command Options Example 12
  Using the no and default Forms of Commands 15
  Saving Configuration Changes 16
  Managing Configuration Files 16
  Filtering Output from the show and more Commands 17
  Powering Off the Router 18
  Password Recovery 18
  Finding Support Information for Platforms and Cisco Software Images 19
    Using Cisco Feature Navigator 19
    Using Software Advisor 19
    Using Software Release Notes 19

CHAPTER 3

Using Zero Touch Provisioning 21
Common Ethernet Management Tasks  44
   Viewing the VRF Configuration  44
   Viewing Detailed VRF Information for the Management Ethernet VRF  45
   Setting a Default Route in the Management Ethernet Interface VRF  45
   Setting the Management Ethernet IP Address  45
   Telnetting over the Management Ethernet Interface  46
   Pinging over the Management Ethernet Interface  46
   Copy Using TFTP or FTP  46
   NTP Server  46
   SYSLOG Server  47
   SNMP-related services  47
   Domain Name Assignment  47
   DNS service  47
   RADIUS or TACACS+ Server  47
   VTY lines with ACL  48

CHAPTER 7

Out of Band Management Through USB Modem  49
   Prerequisites for the OOB Management Through USB Modem  49
   Restrictions for the OOB Management Through USB Modem  49
   Information About the OOB Management Through USB Modem  50
   Configuring the Management Interface on the MAG  51
      Configuration Example: MAG Configuration with Dynamic IP Address on Logical MN Interface  53
   Configuration Example: MAG Configuration with Static IP Address on Logical MN Interface  53
   Configuring the LMA  54
      Configuration Example  55
   Verifying the Configuration  56
      MAG Call Setup  56
      MAG Data Path  56
      Debug Commands  57
      Related Documents  57

CHAPTER 8

Power Over Ethernet  59
   Prerequisites for PoE  59
Example: CRC Configuration  82
Example: Facility Data Link Configuration  82
Example: Invert Data on the T1/E1 Interface  83

CHAPTER 10  Installing and Upgrading Software  85
Upgrading Field Programmable Hardware Devices  85
File Systems on the Cisco ASR 920 Series Router  85
Restrictions  86
System Requirements  86
Memory Recommendations  86
ROMmon Version Requirements  86
Bootflash Space Requirements  86
Determining the Software Version  87
Cisco IOS XE 3S to Cisco IOS Version Number Mapping  87
Autogenerated Files and Directories  87
Upgrading the Router Software  88
  Downloading an Image  88
  Upgrading the ROMMON on router  90
Verifying the Upgrade  92
Software Upgrade Example  92

CHAPTER 11  Activating or Deactivating Interface Module  95
Overview  95
Prerequisites for Activating an IM  96
Restrictions for Activating an IM  96
Activating an IM  97
Prerequisites for Deactivating an IM  97
Restrictions for Deactivating an IM  98
Deactivating an IM  98
Sample Configuration and Verification Examples for Activation or Deactivation of IMs  99
  Sample Configuration and Verification of Activating an 8-port 1G Cu IM (A900-IMA8T)  99
  Sample Configuration and Verification for Deactivating an 8-port 1G Cu IM (A900-IMA8T)  101
  Sample Configuration and Verification of Activating 8-port T1/E1 IM (A900-IMA8D)  103
  Sample Configuration and Verification of Deactivating 8-port T1/E1 IM (A900-IMA8D)  106
CHAPTER 12 Configuring Ethernet Interfaces 111
   Configuring an Interface 111
   Specifying the Interface Address on an Interface 113
   Modifying the Interface MTU Size 113
      Interface MTU Configuration Guidelines 114
      Interface MTU Configuration Task 114
   Verifying the MTU Size 115
   Configuring the Encapsulation Type 115
   Configuring Autonegotiation on an Interface 115
      Enabling Autonegotiation 116
      Disabling Autonegotiation 116
   Configuring Carrier Ethernet Features 116
   Saving the Configuration 116
   Shutting Down and Restarting an Interface 117
   Verifying the Interface Configuration 117
      Verifying Per-Port Interface Status 117
   Verifying Interface Status 118
   Configuring LAN/WAN-PHY Controllers 120
      Configuring the LAN-PHY Mode 120
      Configuring WAN-PHY Signal Failure and Signal Degrade Bit Error Rates 121
   Configuration Examples 122
      Basic Interface Configuration 122
      MTU Configuration 122
      VLAN Encapsulation 123

CHAPTER 13 Configuring Serial Interfaces 125
   Information About Serial Interface Module 125
   Restrictions 126
   How to Configure Serial Interface 127
      Required Configuration Tasks 127
      Configuring the Controller 127
   Optional Configurations 128
      Configuring Layer 1 on Sync and Async Interface Server 128
Setting a Dummy Pattern 152
Shutting Down a CEM Channel 153
Configuring Structure-Agnostic TDM over Packet (SAToP) 153
Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN) 154
Configuring an Ethernet over MPLS Pseudowire 156
Configuring Pseudowire Redundancy 157
Sample Configurations 159
  Example: CEM Configuration 159
  Example: Ethernet over MPLS 160
  Example: BGP PIC with TDM-PW Configuration 161
Adaptive Clock Recovery (ACR) 162
  Benefits of ACR for 8 T1/E1 Interface Module 163
  Prerequisites for ACR Configuration in 8 T1/E1 Interface Module 163
  Restrictions for ACR on 8 T1/E1 Interface Module 163
  Configuring ACR for T1 Interfaces for SAToP 164
  Verifying the ACR Configuration of T1 Interfaces for SAToP 164
  Associated Commands 166

CHAPTER 16 Configuring and Monitoring Alarm 167
Monitoring Alarms 167
  Network Administrator Checks Console or Syslog for Alarm Messages 168
    Enabling the Logging Alarm Command 168
    Examples of Alarm Messages 168
    ALARMS for Router 168
    Reviewing and Analyzing Alarm Messages 172
Configuring External Alarm Trigger 172
  Approaches for Monitoring Hardware Alarms 173
    Onsite Network Administrator Responds to Audible or Visual Alarms 173
  How to Configure External Alarms 173
    Example 174
Alarm Filtering Support 175
  Information About Alarm Filtering Support 175
    Overview of Alarm Filtering Support 175
    Prerequisites for Alarm Filtering Support 176
Restrictions for Alarm Filtering Support 176

How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications 177

Configuring Alarm Filtering for Syslog Messages 177

Configuring Alarm Filtering for SNMP Notifications 177

Configuration Examples for Alarm Filtering Support 177

Configuring Alarm Filtering for Syslog Messages: Example 177

Configuring Alarm Filtering for SNMP Notifications: Example 177

---

CHAPTER 17

**Tracing and Trace Management** 179

- Tracing Overview 179
- How Tracing Works 179
- Tracing Levels 180
- Viewing a Tracing Level 181
- Setting a Tracing Level 182
- Viewing the Content of the Trace Buffer 182

---

CHAPTER 18

**BCP Support on MLPPP** 185

- Finding Feature Information 185
  - Prerequisites for BCP Support on MLPPP 185
  - Restrictions for BCP Support on MLPPP 185
- Information About BCP Support on MLPPP 186
  - Supported Profiles and Protocols 187
  - Quality of Service 187
- How to Configure BCP Support on MLPPP 187
  - Configuring Multiple EFPs Bridged Through the Same Link 187
    - Configuring an EFP 187
      - Adding an EFP to a Multilink 188
  - Configuring Multiple Encapsulated VLANs Bridged Through Different Multilinks 190
    - Adding an Encapsulated VLAN to Multilinks 190
  - Configuring QoS for BCP Support on MLPPP 191
    - Defining a QoS Policy 191
    - Applying a QoS Policy on an MLPPP Interface 193
  - Verifying BCP Support on MLPPP 194
- Configuration Examples for BCP Support on MLPPP 195
Example: Configuring an EFP  195
Example: Multilink with a Single EFP  196
Example: Multilink with Multiple EFPs  196
Example: Multilink with QoS  197
Example: Multilink Between Cisco ASR 903 Series Routers and Cisco C7600 Series Routers  198
Example: Multilink with Maximum 10 Links  199

Additional References  203
Related Documents  203
MIBs  204
RFCs  204
Technical Assistance  204
Feature Information for BCP Support on MLPPP  204
Overview

Cisco ASR 920 families of routers include:

- **ASR 920-I (Indoor) [ASR-920-12CZ-A/ASR-920-12CZ-D]**—This sub-family has fixed ENET interfaces (12 x 1 GE + 2 x 10GE) and dual power supplies (AC or DC).

- **ASR 920-C (Compact) [ASR-920-4SZ-A/ASR-920-4SZ-D]**—This sub-family of routers have a compact form factor and configurable ports: 4 x 1 GE or 4 x 10 GE or any combinations of 1 GE and 10 GE among the four ports available. In addition, there are 2 x 1 GE copper ports available.

- **ASR 920-O (Outdoor) [ASR-920-10SZ-PD and ASR-920-8S4Z-PD]**—This sub-family is designed for deployment outdoors in an environment that is protected from rain and direct sunlight and provides cost optimized, and extended temperature range for business, residential, and mobile access services.

- **ASR 920-F (Fixed) [ASR-920-24SZ-M/ASR-920-24TZ-M]**—This sub-family with 1 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE Copper or SFP) and redundant modular power supplies (AC or DC).

- **ASR 920-M (Modular) [ASR-920-24SZ-IM]**—This sub-family with 1.5 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE Fiber), one modular interface, and redundant modular power supplies (AC or DC). The interface modules from ASR 900 family of routers can be leveraged for use with this model.

- **ASR-920-12SZ-IM**—Eight 1G copper ports, four SFP ports, and four 1G/10G Dual Rate ports one IM slot Power over Ethernet (PoE), and a global navigation satellite system (GNSS) port, with redundant AC or DC power supplies.
• ASR-920-12SZ-A/Cisco ASR-920-12SZ-D—This sub-family with 1 RU form factor has a single AC or DC fixed power supply with 12 (10G SFP+/1G SFP dual rate port) interfaces, Timing (1PPS/10MHz/ToD) interfaces, and a pluggable GNSS module.

• ASR-920-20SZ-M—This sub-family with 1 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE with four Copper ports) and redundant modular power supplies (AC or DC).

In addition to the 1G/10G interfaces, the Cisco ASR 920 Series Routers also have the following hardware interfaces for management, and timing and synchronization features:

• One Copper 10/100/1000Base-T LAN management port
• One BITS interface with RJ48 Connector
• One 1PPS or Time of Day port with RJ45 interface
• External Alarm interface with 4 Dry Contact Alarm inputs
• One RS-232 Console Port with USB A type connector

Due to the USB form factor, the flow control pins are not connected and the terminal server hosting the RS232 session must configure **no flow-control** or the console access to work correctly.

• One USB2.0 Console Port
• One USB2.0 Port for Mass Storage
• ZTP button for Zero Touch Provisioning

A short press of the ZTP button starts the provisioning of the router. Pressing this button for 8 seconds or more leads to Powering off the System Power.

• Various LEDs for system and interface status
• The Cisco ASR-920-12SZ-IM Router also supports:
  • Power over Ethernet (PoE) port
  • Global navigation satellite system (GNSS) port


All variants of the Cisco ASR 920 Series Router have 8MB of NOR flash, and 4GB of DRAM.

**Table 1: Feature Comparison for Cisco ASR 920 Series Routers**

|-----------------------|------------------|----------------|-----------------|---------------|---------------|---------------|
### Restrictions

- The Cisco ASR 920 Series Routers do not support the `hw-module slot/subslot reload` command.

### Interface Naming

The following table shows the interface naming of the Cisco ASR-920-12CZ-A/ASR-920-12CZ-D ports:

<table>
<thead>
<tr>
<th>1G SFP Only</th>
<th>1G Combo Port</th>
<th>10G SFP+/1G SFP²</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

---

**Feature/Functionality**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
</tr>
<tr>
<td>SD FLASH</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
<td>2GB</td>
</tr>
<tr>
<td>1G-10G Dual Rate Ports</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>BITS interface</td>
<td>Present</td>
<td>Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Present</td>
</tr>
<tr>
<td>Time of Day port</td>
<td>Present</td>
<td>Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Not Present</td>
<td>Present</td>
</tr>
<tr>
<td>Auto-Media-Select Combo Port</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Copper Ports</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>SFP Ports</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Smart SFP</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>SFP+ Ports</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Copper SFP</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>XFP Ports</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>ZTP Button</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>PoE</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>GNSS</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>NotSupported</td>
<td>NotSupported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
Ports 12 and 13 when operating in 1G Mode is operationally up only when the peer connecting interfaces are in Auto negotiation mode.

• Interfaces 0–3 are Gigabit Ethernet SFP only ports.

• Interfaces 4X–11X-Gigabit Ethernet are combo ports that support dual media—Copper and SFP. For more information, see the Configuring Auto Media Sense on Cisco ASR 920 Series Routers.

• Interfaces 0 to 11 are referred to as Gigabit Ethernet 0/0/0–GigabitEthernet 0/0/11 respectively.

• Interfaces 12 and 13 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

Dual-Rate functionality is supported only with the Supported SFPs, listed in the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

• Interfaces 12 and 13 are TenGigabitEthernet 0/0/12–TenGigabitEthernet 0/0/13. The interface name remains unchanged even if an SFP is installed in the port and the port is operating in 1G mode.

• Out of Band Management Network port is referred as interface Gig0.

The following table shows the interface naming of the Cisco ASR920-4SZ-A/ASR920-4SZ-D ports:

<table>
<thead>
<tr>
<th>1G Cu Port</th>
<th>10G SFP+/1GSFP²</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

² Ports 2, 3, 4, and 5 when operating in 1G Mode is operationally up only when the peer connecting interfaces are in Auto negotiation mode.

• Interfaces 0–1 are Copper only ports with RJ45 connector.

• Interfaces 0 and 1 are referred to as Gigabit Ethernet 0/0/0–GigabitEthernet 0/0/1 respectively.

• Interfaces 2 to 5 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

Dual-Rate functionality is supported only with the Supported SFPs, listed in the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

• Interfaces 2 to 5 are named as TenGigabitEthernet 0/0/2–TenGigabitEthernet 0/0/5 respectively. The interface name remains unchanged even if an SFP is installed in the port and the port is operating in 1G mode.

• Out of Band Management Network port is referred as interface Gig0.

The following table shows the interface naming of the Cisco ASR-920-10SZ-PD ports:
• Interfaces 0–1 are Copper only ports with RJ45 connector.

• Interfaces 2-9 are Gigabit Ethernet SFP ports.

• Interfaces 10-11 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

The following table shows the interface naming of the Cisco ASR-920-8S4Z-PD ports:

<table>
<thead>
<tr>
<th>1G Cu</th>
<th>1G SFP</th>
<th>10G SFP+</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1G Cu</th>
<th>1G SFP</th>
<th>10G SFP+</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

• Interfaces 0–1 are Copper only ports with RJ45 connector.

• Interfaces 2-7 are Gigabit Ethernet SFP ports.

• Interfaces 8-11 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

The following table shows the interface naming of the Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, ASR-920-24TZ-M ports:

<table>
<thead>
<tr>
<th>IM Slots (for Cisco ASR-920-24SZ-IM only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G SFP/Cu³</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

³ Ports 0-23 are Copper ports for ASR-920-24TZ-M

• Interfaces 0–23 are Gigabit Ethernet SFP ports for ASR-920-24SZ-IM, ASR-920-24SZ-M, and Copper port for ASR-920-24TZ-M.

• Interfaces 24-27 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

The following table shows the interface naming of the Cisco ASR-920-12SZ-IM:

<table>
<thead>
<tr>
<th>10G/1G SFP</th>
<th>1G SFP</th>
<th>1G Cu</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>—</td>
<td>7</td>
</tr>
<tr>
<td>15 14</td>
<td>13 12</td>
<td>11 10</td>
</tr>
</tbody>
</table>

The following table shows the interface naming of the Cisco ASR-920-12SZ-A/Cisco ASR-920-12SZ-D ports:
• Interfaces 0–11 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

The following table shows the interface naming of the Cisco ASR-920-20SZ-M ports:

<table>
<thead>
<tr>
<th>1G Cu port</th>
<th>1G SFP port</th>
<th>10G SFP port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

• Interfaces 0–3 are Copper only ports with RJ45 connector.
• Interfaces 4-23 are Gigabit Ethernet SFP ports.
• Interfaces 24-27 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

All Interfaces with CU SFP, flap twice during router boot up. This behaviour is applicable to the following variants that support CU SFP:
• ASR-920-12CZ-A/D
• ASR-920-4SZ-A/D
• ASR-920-10SZ-PD and ASR-920-8S4Z-PD
• ASR-920-24SZ-M
• ASR-920-24SZ-IM
• ASR-920-12SZ-IM
• ASR-920-20SZ-M

**Interface Speed Based on Port Type**

The following table shows the interface speed of the Cisco ASR-920-12SZ-A/Cisco ASR-920-12SZ-D:

<table>
<thead>
<tr>
<th>Category</th>
<th>Cu Ports</th>
<th>SFP ports (With Fiber SFP plugged in)</th>
<th>SFP ports (With Copper SFP plugged in)</th>
<th>SFP+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>10M</td>
<td>100M</td>
<td>1G</td>
<td>10M</td>
</tr>
<tr>
<td>10G Dual rate ports</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>No</td>
</tr>
</tbody>
</table>

Not Supported

Yes
The following table shows the interface speed of the Cisco ASR-920-20SZ-M:

<table>
<thead>
<tr>
<th>Category</th>
<th>Cu Ports</th>
<th>SFP ports (With Fiber SFP plugged in)</th>
<th>SFP ports (With Copper SFP plugged in)</th>
<th>SFP+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>1G</td>
<td>10M</td>
<td>100M</td>
<td>1G</td>
</tr>
<tr>
<td>1G Copper/SFP ports</td>
<td>Yes</td>
<td>Yes</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10G Dual rate ports</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

VCoP Optics Support

The following table indicates the GE/Dual rate ports that support VCoP optics.

<table>
<thead>
<tr>
<th>Chassis</th>
<th>1 GE Port</th>
<th>Dual Rate 1 GE/10 GE port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR-920-10SZ-PD</td>
<td>3, 5, 7, and 9</td>
<td>NA</td>
</tr>
<tr>
<td>ASR-920-24SZ-IM</td>
<td>1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23</td>
<td>NA</td>
</tr>
<tr>
<td>ASR-920-12SZ-IM</td>
<td>0 to 11</td>
<td>12 to 15</td>
</tr>
<tr>
<td>ASR-920-12CZ-A</td>
<td>0, 1, 10, and 11</td>
<td>NA</td>
</tr>
</tbody>
</table>

4 The Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M routers support a maximum of 12 VCoP smart SFPs and only on GE ports of the top row.
5 The Cisco ASR-920-12SZ-IM router supports a maximum of 8 VCoP smart SFPs and on all GE and 10 GE ports.
6 The Cisco ASR-920-12CZ-A/D supports a maximum of 4 VCoP smart SFPs on GE ports (0, 1, 10, and 11) with maximum ambient temperature of 65°C or it supports a maximum of 14 VCoP smart SFPs on all 12 GE + two 10 GE dual rate ports with maximum temperature of 55°C.
Using Cisco IOS XE Software

This chapter provides information to prepare you to configure the Cisco ASR 920 Series Router:

- Understanding Command Modes, on page 9
- Accessing the CLI Using a Router Console, on page 11
- Using Keyboard Shortcuts, on page 11
- Using the History Buffer to Recall Commands, on page 11
- Getting Help, on page 12
- Using the no and default Forms of Commands, on page 15
- Saving Configuration Changes, on page 16
- Managing Configuration Files, on page 16
- Filtering Output from the show and more Commands, on page 17
- Powering Off the Router, on page 18
- Password Recovery, on page 18
- Finding Support Information for Platforms and Cisco Software Images, on page 19

Understanding Command Modes

The command modes available in the traditional Cisco IOS CLI are exactly the same as the command modes available in Cisco IOS XE.

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.

The table below 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 2: Accessing and Exiting Command Modes

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Log in.</td>
<td>Router&gt;</td>
<td>Use the <code>logout</code> command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode, use the <code>enable</code> EXEC command.</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the <code>disable</code> command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC mode, use the <code>configure terminal</code> privileged EXEC command.</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the <code>exit</code> or <code>end</code> command.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an <code>interface</code> command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the <code>exit</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To return to privileged EXEC mode, use the <code>end</code> command.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>The router boots up or accesses diagnostic mode in the following scenarios:</td>
<td>Router(diag)#</td>
<td>If the IOS process failing is the reason for entering diagnostic mode, the IOS problem must be resolved and the router rebooted to get out of diagnostic mode.</td>
</tr>
<tr>
<td></td>
<td>• In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will reload.</td>
<td></td>
<td>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</td>
</tr>
<tr>
<td></td>
<td>• A user-configured access policy was configured using the <code>transport-map</code> command that directed the user into diagnostic mode. See the Console Port, Telnet, and SSH Handling chapter of this book for information on configuring access policies.</td>
<td></td>
<td>If the router is accessed through the Route Switch Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway.</td>
</tr>
<tr>
<td></td>
<td>• The router was accessed using a Route Switch Processor auxiliary port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A break signal (Ctrl-C, Ctrl-Shift-6, or the <code>send break</code> command ) was entered and the router was configured to go into diagnostic mode when the break signal was received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ROM monitor</td>
<td>From privileged EXEC mode, use the <code>reload</code> EXEC command. Press the <code>Break</code> key during the first 60 seconds while the system is booting.</td>
<td>&gt;</td>
<td>To exit ROM monitor mode, use the <code>continue</code> command.</td>
</tr>
</tbody>
</table>
Accessing the CLI Using a Router Console

**Note**
For more information about connecting cables to the router, see the *Connecting a Cisco ASR 920 Series Router to the Network* section in the *Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide*.

**Note**
For information about installing USB devices drivers in order to use the USB console port, see the *Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide*.

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.

The table below lists the keyboard shortcuts for entering and editing commands.

### Table 3: Keyboard Shortcuts

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or the Left Arrow key</td>
<td>Move the cursor back one character</td>
</tr>
<tr>
<td>Ctrl-F or the Right Arrow key</td>
<td>Move the cursor forward one character</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Move the cursor to the beginning of the command line</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Move the cursor to the end of the command line</td>
</tr>
<tr>
<td>Esc B</td>
<td>Move the cursor back one word</td>
</tr>
<tr>
<td>Esc F</td>
<td>Move the cursor forward one word</td>
</tr>
</tbody>
</table>

7 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.

The table below lists the history substitution commands.
Table 4: History Substitution Commands

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

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

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:

Table 5: Help Commands and Purpose

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

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.

The table below shows examples of how you can use the question mark ( `?` ) to assist you in entering commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; enable Password: &lt;password&gt; Router#</td>
<td>Enter the <strong>enable</strong> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a &quot;#&quot; from the &quot;&gt;&quot;; for example, Router&gt; to Router# .</td>
</tr>
<tr>
<td>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</td>
<td>Enter the <strong>configure terminal</strong> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)# .</td>
</tr>
<tr>
<td>Router(config)# gigabitethernet 0/0/1</td>
<td>Enter interface configuration mode by specifying the serial interface that you want to configure using the <strong>gigabitethernet</strong> or <strong>tengigabitethernet</strong> global configuration command.</td>
</tr>
</tbody>
</table>
### Command Options Example

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ?</td>
<td>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.</td>
</tr>
<tr>
<td>Interface configuration commands:</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>ip Interface Internet Protocol config commands</td>
<td></td>
</tr>
<tr>
<td>keepalive Enable keepalive</td>
<td></td>
</tr>
<tr>
<td>lan-name LAN Name command</td>
<td></td>
</tr>
<tr>
<td>llc2 LLC2 Interface Subcommands</td>
<td></td>
</tr>
<tr>
<td>load-interval Specify interval for load calculation for an interface</td>
<td></td>
</tr>
<tr>
<td>locaddr-priority Assign a priority group</td>
<td></td>
</tr>
<tr>
<td>logging Configure logging for interface</td>
<td></td>
</tr>
<tr>
<td>loopback Configure internal loopback on an interface</td>
<td></td>
</tr>
<tr>
<td>mac-address Manually set interface MAC address</td>
<td></td>
</tr>
<tr>
<td>mls mls router sub/interface commands</td>
<td></td>
</tr>
<tr>
<td>mpoa MPOA interface configuration commands</td>
<td></td>
</tr>
<tr>
<td>mtu Set the interface Maximum Transmission Unit (MTU)</td>
<td></td>
</tr>
<tr>
<td>netbios Use a defined NETBIOS access list or enable</td>
<td></td>
</tr>
<tr>
<td>name-caching no Negate a command or set its defaults</td>
<td></td>
</tr>
<tr>
<td>nrzi-encoding Enable use of NRZI encoding</td>
<td></td>
</tr>
<tr>
<td>ntp Configure NTP</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td></td>
</tr>
</tbody>
</table>

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ip ?</td>
<td>Enter the command that you want to configure for the interface. This example uses the ip command.</td>
</tr>
<tr>
<td>Interface IP configuration subcommands:</td>
<td></td>
</tr>
<tr>
<td>access-group Specify access control for packets</td>
<td></td>
</tr>
<tr>
<td>accounting Enable IP accounting on this interface</td>
<td></td>
</tr>
<tr>
<td>address Set the IP address of an interface</td>
<td></td>
</tr>
<tr>
<td>authentication authentication subcommands</td>
<td></td>
</tr>
<tr>
<td>bandwidth-percent Set EIGRP bandwidth limit</td>
<td></td>
</tr>
<tr>
<td>broadcast-address Set the broadcast address of an interface</td>
<td></td>
</tr>
<tr>
<td>cgp Enable/disable ICMP</td>
<td></td>
</tr>
<tr>
<td>directed-broadcast Enable forwarding of directed broadcasts</td>
<td></td>
</tr>
<tr>
<td>dvmrp DVMRP interface commands</td>
<td></td>
</tr>
<tr>
<td>hello-interval Configures IP-EIGRP hello interval</td>
<td></td>
</tr>
<tr>
<td>helper-address Specify a destination address for UDP broadcasts</td>
<td></td>
</tr>
<tr>
<td>hold-time Configures IP-EIGRP hold time</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip</td>
<td>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td>
</tr>
</tbody>
</table>
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 XE 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 XE 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#
```

This task saves the configuration to NVRAM.

Managing Configuration Files

On the router, the startup configuration file is stored in the nvram: file system and the running-configuration files are stored in the system: file system. This configuration file storage setup is not unique to the router and is used on several Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router’s other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

The `copy` command can be used to backup startup configuration files. Below are some examples showing the startup configuration file in NVRAM being backed up:

Example 1: Copying Startup Configuration File to Bootflash

```
Router# dir bootflash:
Directory of bootflash:/
  11 drwx 16384 Feb 2 2000 13:33:40 +05:30 lost+found
15105 drwx 4096 Feb 2 2000 13:35:07 +05:30 .ssh
45313 drwx 4096 Nov 17 2011 17:36:12 +05:30 core
75521 drwx 4096 Feb 2 2000 13:35:11 +05:30 .prst_sync
90625 drwx 4096 Feb 2 2000 13:35:22 +05:30 .rollback_timer
105729 drwx 8192 Nov 21 2011 22:57:55 +05:30 tracelogs
30209 drwx 4096 Feb 2 2000 13:36:17 +05:30 .installer
1339412480 bytes total (1199448064 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
3517 bytes copied in 0.647 secs (5436 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
  11 drwx 16384 Feb 2 2000 13:33:40 +05:30 lost+found
15105 drwx 4096 Feb 2 2000 13:35:07 +05:30 .ssh
45313 drwx 4096 Nov 17 2011 17:36:12 +05:30 core
75521 drwx 4096 Feb 2 2000 13:35:11 +05:30 .prst_sync
90625 drwx 4096 Feb 2 2000 13:35:22 +05:30 .rollback_timer
12 -rw- 0 Feb 2 2000 13:36:03 +05:30 traceslogs.878
```
Example 2: Copying Startup Configuration File to USB Flash Disk

Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 May 27 2008 14:10:20 -07:00
asr920-adventerprisek9.02.01.00.122-33.XNA.bin
2 55497216 bytes total (40194064 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
3172 bytes copied in 0.214 secs (14822 bytes/sec)
Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 May 27 2008 14:10:20 -07:00
asr920-adventerprisek9.02.01.00.122-33.XNA.bin 3172 Jul 2 2008 15:40:45
-07:00 startup-config255497216 bytes total (40186880 bytes free)

Example 3: Copying Startup Configuration File to a TFTP Server

Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)

For more detailed information on managing configuration files, see the Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S.

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 | {append | begin | exclude | include | redirect | section | tee} 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
Powering Off the Router

Before you turn off a power supply, make certain the chassis is grounded and you perform a soft shutdown on the power supply. Not performing a soft shutdown will often not harm the router, but may cause problems in certain scenarios.

To perform a soft shutdown before powering off the router, enter the `reload` command to halt the system and then wait for ROM Monitor to execute before proceeding to the next step.

The following screenshot shows an example of this process:

```plaintext
Router# reload
Proceed with reload? [confirm]
```

Place the power supply switch in the Off position after seeing this message.

Password Recovery

**Warning**

You will loose the startup configuration by using this Password Recovery procedure.

**Note**

The configuration register is usually set to 0x2102 or 0x102. If you can no longer access the router (because of a lost login or TACACS password), you can safely assume that your configuration register is set to 0x2102.

**Before you Begin:**

Make sure that the hyperterminal has the following settings:

- 9600 baud rate
- No parity
- 8 data bits
- 1 stop bit
- No flow control
- Use the power switch to turn off the router and then turn it on again.
- Press Break on the terminal keyboard within 60 seconds of power up to put the router into ROMMON. In some cases Ctrl+Break key combination can be used.
- Type `confreg 0x2142` at the ROMMON.

```
1> confreg 0x2142
1>sync
```

The router reboots, but ignores the saved configuration.
• The router will reload and prompt for configuration. Type no after each setup question, or press Ctrl-C to skip the initial setup procedure.

• Type enable at the Router> prompt.
  You are now in enable mode and should see the Router# prompt.

• Reset the config-register from 0x2142 to 0x2102. To do so, type the following:

  ```
  (config)# config-register configuration_register_setting
  Where, configuration_register_setting is 0x2102. For example,
  ```

```(config)# config-register 0x2102```

## 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 software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Using Software Advisor

To see if a feature is supported by a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE 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](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 3

Using Zero Touch Provisioning

Note
The Cisco ASR 920 Series Router (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M) do not have a ZTP or Reset button.

Note
Routers running ZTP must be able to connect to a DHCP server and TFTP server, download the configuration template, and begin operation, all at the press of a button.

• Prerequisites for Using ZTP, on page 21
• Restrictions for Using ZTP, on page 22
• Information About Using ZTP, on page 22
• Downloading the Initial Configuration, on page 24
• ZTP LED Behavior, on page 25
• Verifying the ZTP Configuration, on page 25

Prerequisites for Using ZTP

• The Cisco ASR 920 Series Router must be running Cisco IOS-XE Release 3.13.0S or later.

• The interface connected to the TFTP server must be turned green.

• DHCP server should be configured to ensure reachability to the TFTP server.

• Ports that are licensed through port licensing are disabled during the ZTP process. It is highly recommended that you connect to free ports that do not need a license to be enabled. For information on port licensing, see Licensing 1G and 10G Ports on the Cisco ASR 920 Series Router.

Caution
Do not change the ROMMON configuration register to 0x0.
Restrictions for Using ZTP

- ZTP is not supported on the LAN Management port—Gig0 on the router. ZTP is supported only on the Ethernet interfaces such as 1—Gige, 10—Gige ports, and so on.
- ZTP is not initialized if the ZTP button is pressed for more than eight seconds. In this case, the router goes through a normal reload process.
- ZTP is also not initialized when the router is already reloading or if the router is in ROMMON prompt.
- When the ZTP process is initialized all previous logs in the buffer are cleared.
- DHCP declines addresses when loading DHCP configuration through TFTP. It is strongly recommended to have only the CNS configuration present on the configuration file to avoid tampering with the ZTP BDI.
- ZTP is not initialized if bootflash has files named as 'router-config'.

Information About Using ZTP

Figure 1: Sample ZTP Topology

On the Cisco ASR 920 Series Routers, ZTP is triggered under any of the following conditions:

- A router without a start up configuration is powered on
- ZTP button is pressed (applicable on Cisco ASR 920 Series Router variants where the ZTP button is present on the front panel) or,
- The write erase and reload commands are executed (applicable on Cisco ASR 920 Series Router variants where the ZTP button is not present on the front panel)

Note

The Cisco ASR 920 Series Routers (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, and ASR-920-8S4Z-PD) have a ZTP button on the front panel.

The Cisco ASR 920 Series Routers (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M) do not have a ZTP or Reset button.

Router# write erase
System configuration has been modified. Save? [yes/no]: no
Router# reload

If you type yes at the prompt, the system configuration is saved in the nvRAM and the ZTP process terminates.

After the ZTP process initializes, the following sequence is initiated:

1. The router detects the management VLAN and waits for any of the following data packets.
   - Broadcast (Gratuitous ARP)
   - ISIS hello packets
   - OSPF hello packets
   - IPv6 router advertisement packets
   - VRRP

2. When the first packet on any VLAN is detected, the router initiates a DHCP session to a DHCP server over that VLAN.

3. After a DHCP session is established, the router must establish a connection with the TFTP server through DHCP option 43 or DHCP option 150.

4. When connectivity to the TFTP server is established, the bootup process starts.

When the ZTP process initiates, the Cisco ASR 920 Series Router creates an Ethernet flow point (EFP) and associates a bridge domain interface (BDI) on the detected management VLAN.

The router creates the following configuration to establish a connection with the DHCP server and the TFTP server. The BDI created for this purpose has description ZTP_BDI configured under the BDI interface.

Do not delete ZTP_BDI. Deleting this configuration results in loss of connectivity to the router and the ZTP process terminates.

Effective Cisco IOS-XE Release 3.14.0S, to stop the ZTP process when the ZTP button is accidently pressed, use the ztp disable command in global configuration mode. However, if you long press the ZTP button, (more than 8 sec) ZTP is still initialized reload even though ZTP is disabled through the ztp disable command.

Example ZTP Configuration

Let us assume that GigabitEthernet0/0/1 is connected to the DHCP server and is used to connect to the TFTP server. VLAN ID 1000 is used as the management VLAN.
Router# show running-config int gi0/0/1
Building configuration...
Current configuration : 216 bytes
!
interface GigabitEthernet0/0/1
  no ip address
  media-type auto-select
  no negotiation auto
  service instance 12 ethernet
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 12
!
end
!

interface BDI12
  description ZTP_BDI
  ip address dhcp
end

**Downloading the Initial Configuration**

After the VLAN discovery process is completed, the configuration download process begins. The following sequence of events is initiated.

1. The router sends DHCP discover requests on each Ethernet interface.
2. The DHCP server allocates and sends an IP address, TFTP address (if configured with option 150) and default router address to the router.
3. If the TFTP option (150) is present, the router requests a bootstrap configuration that can be stored in any of the following files: PID-<mac-address>, network-config, router-config, ciscortr.cfg, or cisconet.cfg.

**DHCP Server**

The following is a sample configuration to set up a Cisco router as a DHCP server:

```plaintext
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
  network 30.30.1.0 255.255.255.0
  option 150 ip 30.30.1.6
  default-router 30.30.1.6
```

This configuration creates a DHCP pool of 30.30.1.x addresses with 30.30.1.0 as the subnet start. The IP address of the DHCP server is 30.30.1.6. Option 150 specifies the TFTP server address. In this case, the DHCP and TFTP server are the same.

The DHCP pool can allocate from 30.30.1.1 to 30.30.1.19 with the exception of 30.30.1.6, which is the DHCP server itself.
**TFTP Server**

The TFTP server stores the bootstrap configuration file.

The following is a sample configuration (network– config file):

```
hostname test-router
! {ncs router-specific configuration content}
!
end
```

**ZTP LED Behavior**


<table>
<thead>
<tr>
<th>Process</th>
<th>PWR LED</th>
<th>STAT LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press ZTP button</td>
<td>Green</td>
<td>Blinking Amber</td>
</tr>
<tr>
<td>Loading image</td>
<td>Blinking Green/Red</td>
<td>OFF</td>
</tr>
<tr>
<td>Image loaded</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>ZTP process running</td>
<td>Green</td>
<td>Blinking Amber</td>
</tr>
<tr>
<td>ZTP process success and config-file download completes</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>ZTP process failure or aborted</td>
<td>Green</td>
<td>Red</td>
</tr>
</tbody>
</table>

On Cisco ASR 920 Series Routers (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M), using the `write erase` and `reload` commands:

<table>
<thead>
<tr>
<th>Process</th>
<th>PWR LED</th>
<th>STAT LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading image</td>
<td>Blinking Green/Red</td>
<td>OFF</td>
</tr>
<tr>
<td>Image loaded</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>ZTP process running</td>
<td>Green</td>
<td>Blinking Amber</td>
</tr>
</tbody>
</table>

**Verifying the ZTP Configuration**

To verify if the ZTP configuration is successful, use the following command:

- `show running-config`
Verifying the ZTP Configuration
Using Dual Rate Ports

Dual rate ports support both SFP and SFP+ optic modules.


Note
See the Supported SFP chapter in the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

- Restrictions for Dual Port, on page 27
- Prerequisites for Dual Port, on page 29
- Information About Dual Port, on page 29
- Verifying the Interface Mode, on page 30

Restrictions for Dual Port

For more information on licensing, see, Activating Port Upgrade and Bulk Port License on Cisco ASR 920 Series Router:

- When a dual rate port operates in 1G mode, autonegotiation is forced on the interface. For the link to be operationally up, ensure that the peer device is also configured with autonegotiation.

- If a 10G license is installed and activated for a dual rate port and an SFP is installed in that port, the interface comes up in 1G mode.

- If a 10G license is installed and activated for a dual rate port and an SFP+ is installed in that port, the interface comes up in 10G mode.

- If a 10G license is not installed for particular port but an SFP is installed on that port, the interface comes up in 1G mode.

- If sufficient 10G licenses or bulk port licenses are not available or activated for a port and an SFP+ is installed in that port, the 10G mode is not enabled and the interface will be in link down state. The following system warning message is displayed:

  Warning: SFP+ inserted at port 5 tengig license not in use

  - However, if the 10G license is installed and activated after the insertion of the SFP+ the interface comes up in 10G mode automatically.
Do not issue another license command until the previous license command is processed completely. As part of the license command, multiple dual port EEM scripts will be running. These scripts, in turn, copy the port configuration. After executing completely, the previous configuration is restored. However, if you change the port configuration while the command is still executing, changes will not be in effect.

- If an activated 10G license is uninstalled or deactivated for a port with SFP+, the interface is initialized to 1G mode and 10G interfaces is administratively down.

- Dual rate interfaces in 1G mode cannot be bundled with another 1G port under a port channel interface. However, two dual rate interfaces of the same bandwidth can be bundled together. For example,
  - Interface Te0/0/11 and Interface Gig0/0/3 cannot be bundled in a port channel interface even if interface Te 0/0/11 is operating in 1G mode
  - Interface Te0/0/11 and Interface Te0/0/12 can be bundled together under a port channel interface provided they have the same bandwidth (1G or 10G).

- After changing an SFP on a dual rate port, you must wait for approximately three minutes before inserting another SFP in that port.

- In case of ASR-920-10SZ-PD and ASR-920-12CZ-A:
  - The maximum default VTY lines supported by Cisco IOS XE is 5, and at least 2 VTY (VTY 0 and 1) lines must be kept free for the dual rate EEM script to work as stated in the general EEM configuration guidelines at Embedded Event Manager Configuration Guide.

- In case of ASR-920-4SZ-D, ASR-920-12SZ-A/Cisco ASR-920-12SZ-D, and ASR-920-12SZ-IM:
  - The maximum default VTY lines supported by Cisco IOS XE is 5, and at least 4 VTY lines must be kept free for the dual rate EEM script to work as stated in the general EEM configuration guidelines at Embedded Event Manager Configuration Guide.

- Copper SFPs are not supported in dual rate ports for ASR920-12SZ-IM.

- Dual rate EEM script triggers DHCP renegotiation. The dualrate_eem_policy.tcl script is triggered when there is a 10G to 1G optics change or vice versa in a dual rate front panel interface.
Prerequisites for Dual Port

When a dual rate port operates in 1G mode, auto negotiation is forced on the interface. For the link to be operationally up, ensure that the peer device is also configured with auto negotiation.

Whenever there is a physical swap of optics from 1G to 10G or vice-versa on Cisco ASR 920 Series Routers (ASR-920-12CZ-A, ASR-920-4SZ-A, ASR-920-12SZ-IM, and ASR-920-10SZ-PD), a system internal EEM script is triggered to program the hardware registers. However, configurations such as AAA/TACACS can cause the EEM script (dualrate_eem_policy) to timeout with following error.

%HA_EM-6-LOG: Mandatory.dualrate_eem_policy.tcl: 1Process Forced Exit- MAXRUN timer expired

Ensure the following procedure for the devices that are configured with AAA authentication for their VTY access:

1. AAA or TACACS server must authenticate the devices by ensuring:
   1. the reachability
   2. the correct username credentials configured for EEM (refer point-3 below)

Note

If the mentioned criteria fails, then the EEM script prompts MAXRUN Timeout Error.

2. Avoid MAXRUN timeout error by bypassing the authorization.
   1. Unconfigure the current policy using the following command.

   ```
   no event manager policy Mandatory.dualrate_eem_policy.tcl type system
   ```

   2. Reconfigure the policy with Authorization bypass using the following command.

   ```
   event manager policy Mandatory.dualrate_eem_policy.tcl type system authorization bypass
   ```

3. Ensure correct authorization of EEM with TACACS.

   Ensure EEM script can pick the username from the following command.

   ```
   event manager session cli username <Username privilege 15>
   ```

   Example:

   ```
   event manager session cli username Cisco_user1 privilege 15
   ```

   The matching username (here, Cisco_user1) should be configured in TACACS.

Information About Dual Port

This feature offers the flexibility of retaining the existing 1G connections, and upgrading to a 10G connection by installing the SFP+ modules when required. For more information, see Restrictions.

The router can detect the removal of an SFP and an insertion of an SFP+ module, or the removal of an SFP+ and an insertion of an SFP module, and trigger mode change events in the system. Depending on the event type, the events generate the following messages:
The above events in turn, trigger the following actions:

- Current running configuration is saved to a temporary file on the bootflash: on the router.

**Note**

Ensure that at least 10MB of free space is available on the bootflash:, else the script and dual rate functionality itself may fail.

- Configurations are changed to default values on the interface.
- Interface is shut down.
- Running configuration (stored in bootflash:) is re-applied.
- If the interface was previously in administratively up state, it is brought up.
- If the running configuration was the same as the start up configuration, the configuration is saved after the OIR of the SFP/SFP+.

**Note**

It is highly recommended that you wait for the interfaces to be administratively up before performing a subsequent OIR.

**Note**

Features such as, QoS that rely on the bandwidth of the interface for service policy configuration may need to be reconfigured as the previously-configured service policy may no longer be applicable. Perform a careful verification of such features and consider reconfiguring them as required.

**Note**

Since the configuration are reapplied on detection of change of SFP type, depending on the size of the configuration on the router, the reapplication of configuration may take some time. It is recommended that you wait for 60 seconds before verifying the configuration.

Use the following command to debug failures and collect EEM debug logs:

`debug event manager tcl cli_lib`

### Verifying the Interface Mode

To verify the mode change (1G/10G), interface speed and media type inserted, run the following command:

```
Router# show interface tenGigabitEthernet 0/0/5
```

```
TenGigabitEthernet0/0/5 is up, line protocol is up
  Hardware is 2xGE-4x10GE-FIXED, address is badb.adba.fb85 (bia badb.adba.fb85)
  Internet address is 10.1.3.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  reliability 255/255, txload 1/255, rxload 1/255
```
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
**Full Duplex, 10000Mbps, link type is force-up, media type is 10GBase-SR**
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:13:56, 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

Router# show interface GigabitEthernet 0/0/7
TenGigabitEthernet0/0/5 is up, line protocol is up
Hardware is 2xGE-4x10GE-FIXED, address is badb.adba.fb85 (bia badb.adba.fb85)
Internet address is 10.1.3.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
**Full Duplex, 1000Mbps, link type is force-up, media type is ZX**
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:13:56, 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
CHAPTER 5

Console Port and Telnet Handling

- Console Port Overview, on page 33
- Connecting Console Cables, on page 33
- Installing USB Device Drivers, on page 33
- Console Port Handling Overview, on page 34
- Telnet and SSH Overview, on page 34
- Persistent Telnet, on page 34
- Configuring a Console Port Transport Map, on page 34
- Configuring Persistent Telnet, on page 36
- Viewing Console Port, SSH, and Telnet Handling Configurations, on page 39
- Important Notes and Restrictions, on page 41

Console Port Overview

The console port on the router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the router and is located on the front panel of the router.

For information on accessing the router using the console port, see the Cisco ASR 920 Hardware Installation Guide.

Connecting Console Cables

For information about connecting console cables to the Cisco ASR 920 Series Router, see the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

Installing USB Device Drivers

For instructions on how to install device drivers in order to use the USB console port, see the ASR 920 Series Aggregation Services Router Hardware Installation Guide.
Console Port Handling Overview

Users using the console port to access the router are automatically directed to the IOS XE command-line interface, by default.

If a user is trying to access the router through the console port and sends a break signal (a break signal can be sent by entering `Ctrl-C` or `Ctrl-Shift-6`, or by entering the `send break` command at the Telnet prompt) before connecting to the IOS XE command-line interface, the user is directed into diagnostic mode by default if the non-RPIOS sub-packages can be accessed.

These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

Telnet and SSH Overview

Telnet and Secure Shell (SSH) on the router can be configured and handled like in any other Cisco platforms. For information on traditional Telnet, see the `line` command in the Cisco IOS Terminal Services Command Reference guide.

For information on configuring traditional SSH, see the Secure Shell Configuration Guide.

The router also supports persistent Telnet. Persistent Telnet allows network administrators to more clearly define the treatment of incoming traffic when users access the router through the Management Ethernet port using Telnet. Notably, persistent Telnet provides more robust network access by allowing the router to be configured to be accessible through the Ethernet Management port using Telnet even when the IOS XE process has failed.

Persistent Telnet

In traditional Cisco routers, accessing the router using Telnet is not possible in the event of an IOS failure. When Cisco IOS fails on a traditional Cisco router, the only method of accessing the router is through the console port. Similarly, if all active IOS processes have failed on a router that is not using persistent Telnet, the only method of accessing the router is through the console port.

With persistent Telnet however, users can configure a transport map that defines the treatment of incoming Telnet traffic on the Management Ethernet interface. Among the many configuration options, a transport map can be configured to direct all traffic to the IOS command-line interface, diagnostic mode, or to wait for an IOS vty line to become available and then direct users into diagnostic mode when the user sends a break signal while waiting for the IOS vty line to become available. If you use Telnet to access diagnostic mode, the Telnet connection will be usable even in scenarios when no IOS process is active. Therefore, persistent Telnet introduces the ability to access the router via diagnostic mode when the IOS process is not active.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.
**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `transport-map type console transport-map-name`
4. `connection wait [allow interruptible | none]`
5. `banner [diagnostic | wait] banner-message`
6. `exit`
7. `transport type console console-line-number input transport-map-name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transport-map type console transport-map-name</td>
<td>Creates and names a transport map for handling console connections, and enter transport map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# transport-map type console consolehandler</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> connection wait [allow interruptible</td>
<td>none]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# connection wait none</td>
<td>• allow interruptible—The console connection waits for an IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a console connection waiting for the IOS vty line to become available. This is the default setting.</td>
</tr>
<tr>
<td><strong>Note</strong> Users can interrupt a waiting connection by entering <code>Ctrl-C</code> or <code>Ctrl-Shift-6</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• none—The console connection immediately enters diagnostic mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> banner [diagnostic</td>
<td>wait] banner-message</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. <strong>--Welcome to Diagnostic Mode--X</strong> Router(config-tmap)#</td>
<td>• diagnostic—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
- **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.
- **banner-message**—The banner message, which begins and ends with the same delimiting character.

#### Step 6
**exit**
**Example:**
```
Router(config-tmap)# exit
```
Exits transport map configuration mode to re-enter global configuration mode.

#### Step 7
**transport type console console-line-number input**
**transport-map-name**
**Example:**
```
Router(config)# transport type console 0 input consolehandler
```
Applies the settings defined in the transport map to the console interface.
The **transport-map-name** for this command must match the **transport-map-name** defined in the **transport-map type console** command.

### Examples

In the following example, a transport map to set console port access policies is created and attached to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to diagnostic mode X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

### Configuring Persistent Telnet

This task describes how to configure persistent Telnet on the router.

#### Before you begin

For a persistent Telnet connection to access an IOS vty line on the router, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access IOS using a Telnet connection into the Management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
Consoles Port and Telnet Handling

**Configuring Persistent Telnet**

3. `transport-map type persistent telnet transport-map-name`
4. `connection wait [allow {interruptible}] | none {disconnect}]`
5. `banner [diagnostic | wait] banner-message`
6. `transport interface gigabitethernet 0`
7. `exit`
8. `transport type persistent telnet input transport-map-name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transport-map type persistent telnet</td>
<td>Creates and names a transport map for handling persistent Telnet</td>
</tr>
<tr>
<td><strong>transport-map-name</strong></td>
<td>connections, and enters transport map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# transport-map type persistent</td>
<td></td>
</tr>
<tr>
<td>telnet telnethandler</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> connection wait [allow {interruptible}]</td>
<td>Specifies how a persistent Telnet connection will be handled using</td>
</tr>
<tr>
<td><strong>none {disconnect}]</strong></td>
<td>this transport map:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-tmap)# connection wait none</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Users can interrupt a waiting connection by</td>
<td></td>
</tr>
<tr>
<td>entering <strong>Ctrl-C</strong> or <strong>Ctrl-Shift-6</strong>.</td>
<td></td>
</tr>
<tr>
<td>• none—The Telnet connection immediately enters</td>
<td></td>
</tr>
<tr>
<td>diagnostic mode.</td>
<td></td>
</tr>
<tr>
<td>• none disconnect—The Telnet connection does not wait</td>
<td></td>
</tr>
<tr>
<td>for the IOS vty line and does not enter diagnostic</td>
<td></td>
</tr>
<tr>
<td>mode, so all Telnet connections are rejected if no vty</td>
<td></td>
</tr>
<tr>
<td>line is immediately available in IOS.</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 5
**Example:**

```
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode-- X
Router(config-tmap)#
```

- **banner [diagnostic | wait] banner-message**
  - **Purpose**: (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the persistent Telnet configuration.
  - **diagnostic**—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.
  - **wait**—creates a banner message seen by users waiting for the vty line to become available.
  - **banner-message**—the banner message, which begins and ends with the same delimiting character.

#### Step 6
**Example:**

```
Router(config-tmap)# transport interface gigabitethernet 0
```

- **transport interface gigabitethernet 0**
  - **Purpose**: Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0).
  - Persistent Telnet can only be applied to the Management Ethernet interface on the router. This step must be taken before applying the transport map to the Management Ethernet interface.

#### Step 7
**Example:**

```
Router(config-tmap)# exit
```

- **exit**
  - **Purpose**: Exits transport map configuration mode to re-enter global configuration mode.

#### Step 8
**Example:**

```
Router(config)# transport type persistent telnet input transport-map-name
```

- **transport type persistent telnet input transport-map-name**
  - **Purpose**: Applies the settings defined in the transport map to the Management Ethernet interface.
  - The **transport-map-name** for this command must match the **transport-map-name** defined in the **transport-map type persistent telnet** command.

### Examples

In the following example, a transport map that will make all Telnet connections wait for an IOS vty line to become available before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnetethandler
Router(config-tmap)#
connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode-- X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
```
--Waiting for IOS Process-- X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the `show transport-map all name transport-map-name | type console telnet` EXEC or privileged EXEC command to view the transport map configurations.

In the following example, a console port and persistent Telnet transport are configured on the router and various forms of the `show transport-map` command are entered to illustrate the various ways the `show transport-map` command can be entered to gather transport map configuration information.

Router# `show transport-map all`
Transport Map:
  Name: consolehandler
  Type: Console Transport
  Connection:
    Wait option: Wait Allow Interruptable
    Wait banner: Waiting for the IOS CLI
    bshell banner: Welcome to Diagnostic Mode
  Interface:
    GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner: Waiting for IOS prompt
  Bshell banner: 

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
  Interface:
    GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner: Waiting for IOS process
  Bshell banner: 
  Welcome to Diagnostic Mode
Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
Connection:
  Wait option: Wait Allow

Router# `show transport-map type console`
Transport Map:
  Name: consolehandler
  Type: Console Transport
  Connection:
    Wait option: Wait Allow Interruptable
    Wait banner: Waiting for the IOS CLI
    Bshell banner: 
    Welcome to Diagnostic Mode

Router# `show transport-map type persistent telnet`
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
  Interface: GigabitEthernet0
  Connection:
    Wait option: Wait Allow Interruptable
    Wait banner:
  Waiting for IOS process
  Bshell banner:
  Welcome to Diagnostic Mode

Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
  Connection:
    Wait option: Wait Allow

Router# show transport-map name telnethandler

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
  Interface: GigabitEthernet0
  Connection:
    Wait option: Wait Allow Interruptable
    Wait banner:
  Waiting for IOS process
  Bshell banner:
  Welcome to Diagnostic Mode

Router# show transport-map name consolehandler

Transport Map:
  Name: consolehandler
  Type: Console Transport
  Connection:
    Wait option: Wait Allow Interruptable
    Wait banner:
  Waiting for the IOS CLI
  Bshell banner:
  Welcome to Diagnostic Mode

The **show platform software configuration access policy** command can be used to view the current configurations for the handling of incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection, as well as any information on the currently configured banners. Unlike **show transport-map**, this command is available in diagnostic mode so it can be entered in cases when you need transport map configuration information but cannot access the IOS CLI.

Router# show platform software configuration access policy

The current access-policies
Method : telnet
  Rule : wait
  Shell banner:
  Wait banner :
  Method : ssh
  Rule : wait
  Shell banner:
  Wait banner :
  Method : console
  Rule : wait with interrupt
  Shell banner:
  Wait banner :
The `show platform software configuration access policy` output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```
Router# show platform software configuration access policy

The current access-policies
Method   : telnet
Rule     : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
Wait banner :
Waiting for IOS Process
Method   : ssh
Rule     : wait
Shell banner:
Wait banner :
Method   : console
Rule     : wait with interrupt
Shell banner:
Wait banner :
```

**Important Notes and Restrictions**

- Persistent SSH is not supported on Cisco ASR 920 IOS XE release.
- The Telnet settings made in the transport map overrides any other Telnet settings when the transport map is applied to the Management Ethernet interface.
- Only local usernames and passwords can be used to authenticate users entering a Management Ethernet interface. AAA authentication is not available for users accessing the router through a Management Ethernet interface using persistent Telnet.
- Applying a transport map to a Management Ethernet interface with active Telnet sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet sessions.
- Configuring the diagnostic and wait banners is optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet or SSH attempts.
CHAPTER 6

Using the Management Ethernet Interface

The Cisco ASR 920 Series Router has one Gigabit Ethernet Management Ethernet interface on each Route Switch Processor.

The purpose of this interface is to allow users to perform management tasks on the router; it is basically an interface that should not and often cannot forward network traffic but can otherwise access the router, often via Telnet and SSH, and perform most management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when the interfaces are inactive.

The following aspects of the Management Ethernet interface should be noted:

- Each router has a Management Ethernet interface.
- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The interface provides a method of access to the router even if the interfaces or the IOS processes are down.
- The Management Ethernet interface is part of its own VRF. This is discussed in more detail in the Gigabit Ethernet Management Interface VRF, on page 44.
- Gigabit Ethernet Port Numbering, on page 43
- IP Address Handling in ROMmon and the Management Ethernet Port, on page 44
- Gigabit Ethernet Management Interface VRF, on page 44
- Common Ethernet Management Tasks, on page 44

Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

The port can be accessed in configuration mode like any other port on the router.

```bash
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```
IP Address Handling in ROMmon and the Management Ethernet Port

On the router, IP addresses can be configured in ROMmon (the `IP_ADDRESS=` and `IP_SUBNET_MASK=` commands) and through the use of the IOS command-line interface (the `ip address` command in interface configuration mode).

Assuming the IOS process has not begun running on the router, the IP address that was set in ROMmon acts as the IP address of the Management Ethernet interface. In cases where the IOS process is running and has taken control of the Management Ethernet interface, the IP address specified when configuring the Gigabit Ethernet 0 interface in the IOS CLI becomes the IP address of the Management Ethernet interface. The ROMmon-defined IP address is only used as the interface address when the IOS process is inactive.

For this reason, the IP addresses specified in ROMmon and in the IOS CLI can be identical and the Management Ethernet interface will function properly.

Gigabit Ethernet Management Interface VRF

The Gigabit Ethernet Management interface is automatically part of its own VRF. This VRF, which is named “Mgmt-intf,” is automatically configured on the router and is dedicated to the Management Ethernet interface; no other interfaces can join this VRF. Therefore, this VRF does not participate in the MPLS VPN VRF or any other network-wide VRF.

Placing the management ethernet interface in its own VRF has the following effects on the Management Ethernet interface:

• Many features must be configured or used inside the VRF, so the CLI may be different for certain Management Ethernet functions on the router than on Management Ethernet interfaces on other routers.
• Prevents transit traffic from traversing the router. Because all of the interfaces and the Management Ethernet interface are automatically in different VRFs, no transit traffic can enter the Management Ethernet interface and leave an interface, or vice versa.
• Improved security of the interface. Because the Mgmt-intf VRF has its own routing table as a result of being in its own VRF, routes can only be added to the routing table of the Management Ethernet interface if explicitly entered by a user.

The Management Ethernet interface VRF supports both IPv4 and IPv6 address families.

Common Ethernet Management Tasks

Because users can perform most tasks on a router through the Management Ethernet interface, many tasks can be done by accessing the router through the Management Ethernet interface.

Viewing the VRF Configuration

The VRF configuration for the Management Ethernet interface is viewable using the `show running-config vrf` command.

This example shows the default VRF configuration:
Router# show running-config vrf
Building configuration...
Current configuration : 351 bytes
vrf definition Mgmt-intf
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
(some output removed for brevity)

**Viewing Detailed VRF Information for the Management Ethernet VRF**

To see detailed information about the Management Ethernet VRF, enter the `show vrf detail Mgmt-intf` command.

Router# show vrf detail Mgmt-intf
VRF Mgmt-intf (VRF Id = 4085); default RD <not set>; default VPNID <not set>
  Interfaces:
  Gi0
  Address family ipv4 (Table ID = 4085 (0xFF5)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
  Address family ipv6 (Table ID = 503316481 (0x1E000001)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

**Setting a Default Route in the Management Ethernet Interface VRF**

To set a default route in the Management Ethernet Interface VRF, enter the following command

```bash
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 next-hop-IP-address
```

**Setting the Management Ethernet IP Address**

The IP address of the Management Ethernet port is set like the IP address on any other interface.

Below are two simple examples of configuring an IPv4 address and an IPv6 address on the Management Ethernet interface.

**IPv4 Example**

```bash
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address
A.B.C.D A.B.C.D
```
IPv6 Example

Router(config)# interface GigabitEthernet 0
Router(config-if)# ipv6 address X::X::X::X

Telnetting over the Management Ethernet Interface

Telnetting can be done through the VRF using the Management Ethernet interface.

In the following example, the router telnets to 172.17.1.1 through the Management Ethernet interface VRF:

Router# telnet 172.17.1.1 /vrf Mgmt-intf

Pinging over the Management Ethernet Interface

Pinging other interfaces using the Management Ethernet interface is done through the VRF.

In the following example, the router pings the interface with the IP address of 172.17.1.1 through the Management Ethernet interface.

Router# ping vrf Mgmt-intf 172.17.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Copy Using TFTP or FTP

To copy a file using TFTP through the Management Ethernet interface, the `ip tftp source-interface GigabitEthernet 0` command must be entered before entering the `copy tftp` command because the `copy tftp` command has no option of specifying a VRF name.

Similarly, to copy a file using FTP through the Management Ethernet interface, the `ip ftp source-interface GigabitEthernet 0` command must be entered before entering the `copy ftp` command because the `copy ftp` command has no option of specifying a VRF name.

**TFTP Example**

Router(config)# ip tftp source-interface gigabitethernet 0

**FTP Example**

Router(config)# ip ftp source-interface gigabitethernet 0

NTP Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server over the Management Ethernet interface, enter the `ntp server vrf Mgmt-intf` command and specify the IP address of the device providing the update.
The following CLI provides an example of this procedure.

Router(config)# ntp server vrf Mgmt-intf 172.17.1.1

**SYSLOG Server**

To specify the Management Ethernet interface as the source IP or IPv6 address for logging purposes, enter the `logging host ip-address vrf Mgmt-intf` command.

The following CLI provides an example of this procedure.

Router(config)# logging host <ip-address> vrf Mgmt-intf

**SNMP-related services**

To specify the Management Ethernet interface as the source of all SNMP trap messages, enter the `snmp-server source-interface traps gigabitEthernet 0` command.

The following CLI provides an example of this procedure:

Router(config)# snmp-server source-interface traps gigabitEthernet 0

**Domain Name Assignment**

The IP domain name assignment for the Management Ethernet interface is done through the VRF.

To define the default domain name as the Management Ethernet VRF interface, enter the `ip domain-name vrf Mgmt-intf domain` command.

Router(config)# ip domain-name vrf Mgmt-intf cisco.com

**DNS service**

To specify the Management Ethernet interface VRF as a name server, enter the `ip name-server vrf Mgmt-intf IPv4-or-IPv6-address` command.

Router(config)# ip name-server vrf Mgmt-intf IPv4-or-IPv6-address

**RADIUS or TACACS+ Server**

To group the Management VRF as part of a AAA server group, enter the `ip vrf forward Mgmt-intf` command when configuring the AAA server group.

The same concept is true for configuring a TACACS+ server group. To group the Management VRF as part of a TACACS+ server group, enter the `ip vrf forwarding Mgmt-intf` command when configuring the TACACS+ server group.
Radius Server Group Configuration

Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf

Tacacs+ Server Group Example

outer(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf

VTY lines with ACL

To ensure an access control list (ACL) is attached to vty lines that are and are not using VRF, use the vrf-also option when attaching the ACL to the vty lines.

Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
CHAPTER 7

Out of Band Management Through USB Modem

Effective Cisco IOS XE Release 3.15.0S, the Cisco ASR 920 Series Router provides out-of-band connectivity to manage remotely-deployed cell site routers using the 3G or 4G cellular network through the USB modem (also called the dongle). This OOB connectivity gives the service providers the ability to securely manage their remote cell site routers at anytime from anywhere. This feature also eliminates the need for the onsite or remote IT staff to handle outages.

Out of Band Management feature is not supported in Cisco IOS XE Everest 16.5.1.

- Prerequisites for the OOB Management Through USB Modem, on page 49
- Restrictions for the OOB Management Through USB Modem, on page 49
- Information About the OOB Management Through USB Modem, on page 50
- Configuring the Management Interface on the MAG, on page 51
- Configuring the LMA, on page 54
- Verifying the Configuration, on page 56

Prerequisites for the OOB Management Through USB Modem

- The Local Mobility Anchor (LMA) must be a Cisco ASR 1000 Series Router.
- The Mobile Access Gateway (MAG) must be the Cisco ASR 920 Series Router (ASR-920-12CZ-A/D, ASR-920-4SZ-A/D, ASR 920-10SZ-PD, or ASR-920-8S4Z-PD).
- The dongle can be inserted only in the USB Memory port of the Cisco ASR 920 Series Router.

Restrictions for the OOB Management Through USB Modem

For Cisco IOS-XE Release 3.15.0S:

- Multi-VRF is not supported on the Cisco ASR 1000 Series Router.
- Only UDP PMIPv6 tunnels are supported between the LMA and MAG.
- Only the following dongle are supported:
  - Reliance (ZTE: model- AC2739)
  - Airtel 4G (Huawei: model-E3272)
  - TATA DoCoMo (ZTE: model-MF190)
• OOB Management using USB Modem works only when the advance metro ip access license is enabled.
• Starting from Cisco IOS-XE 3.15.0S release, you cannot configure or remove an virtual interface, virtualPPP-4001, manually.

## Information About the OOB Management Through USB Modem

By default, the management interface remains in administratively down state until the dongle in inserted and the feature is enabled.

In the above topology, the LMA assigns an IP address to the LMN. The USB modem receives its IP address from the Service Provider. A UDP tunnel is established between the LMA and MAG through the proxy mobile IPv6 (PMIPv6) protocol.

- Proxy Mobile IPv6 technology—Provides network-based IP mobility management to a mobile node without requiring the participation of the mobile node in any mobility-related signaling. The network is responsible for managing IP mobility on behalf of the host.
- MAG—Manages mobility-related signaling for a mobile node attached to its access link. It is the first layer 3 attachment node for the mobile clients.

The major functions of MAG are:

- Assigning an IP address to the loopback address given by the LMA (when LMA assigns an IP address dynamically)
- Assigning an IP address to the loopback address and sending an update to LMA (in case of static IP address)
- Tunneling the traffic to the corresponding LMA.
• LMA—is the topological anchor point for the MAG

The LMA is responsible for assigning addresses to MAG and managing it.

In Cisco IOS-XE 3.15.0S, LMA is hosted on the Cisco ASR1000 Series Router.

### Configuring the Management Interface on the MAG

#### SUMMARY STEPS

1. platform usb modem username password
2. interface loopback loopback-id
3. ip route prefix mask {ip-address} virtualPPP-4001
4. exit
5. ipv6 unicast-routing
6. ipv6 mobile pmipv6-domain domain-name
7. encap updtunnel
8. lma lma-id
9. ipv4-address ip-address
10. exit
11. nai user@realm
12. lma lma-id
13. ipv6 mobile pmipv6-mag mag-id domain-name
14. address {ipv4 ipv4-address | ipv6 ipv6-address | dynamic}
15. roaming interface type number priority priority-value egress-att access-tech-type label egress-label
16. interface loopback loopback-id
17. interface GigabitEthernet slot/subslot
18. lma lma-id domain-name
19. ipv4-address ipv4-address
20. auth-option spi {spi-hex-value | decimal spi-decimal-value} key {ascii ascii-string | hex hex-string}
21. logical-mn network-access-identifier
22. address {ipv4 ipv4-address | ipv6 ipv6-address | dynamic}
23. home interface type

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables the dongle on the MAG. The <em>username</em> and <em>password</em> are the mobile numbers of the dongle (without the zero prefix).</td>
</tr>
<tr>
<td>platform usb modem username password</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates an interface loopback.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a route to reach the LMA through the dongle interface (virtual pp interface).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits the interface.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>ipv6 unicast-routing</td>
</tr>
<tr>
<td>Step 6</td>
<td>ipv6 mobile pmipv6-domain domain-name</td>
</tr>
<tr>
<td>Step 7</td>
<td>encap udptunnel</td>
</tr>
<tr>
<td>Step 8</td>
<td>lma lma-id</td>
</tr>
<tr>
<td>Step 9</td>
<td>ipv4-address ip-address</td>
</tr>
<tr>
<td>Step 10</td>
<td>exit</td>
</tr>
<tr>
<td>Step 11</td>
<td>nai user@realm</td>
</tr>
<tr>
<td>Step 12</td>
<td>lma lma-id</td>
</tr>
<tr>
<td>Step 13</td>
<td>ipv6 mobile pmipv6-mag mag-id domain domain-name</td>
</tr>
<tr>
<td>Step 14</td>
<td>address {ipv4 ipv4-address</td>
</tr>
<tr>
<td>Step 15</td>
<td>roaming interface type number priority priority-value egress-att access-tech-type label egress-label</td>
</tr>
<tr>
<td>Step 16</td>
<td>interface loopback loopback-id</td>
</tr>
<tr>
<td>Step 17</td>
<td>interface GigabitEthernet slot/subslot</td>
</tr>
<tr>
<td>Step 18</td>
<td>lma lma-id domain-name</td>
</tr>
<tr>
<td>Step 19</td>
<td>ipv4-address ipv4-address</td>
</tr>
<tr>
<td>Step 20</td>
<td>auth-option spi {spi-hex-value</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>This authentication should match that at the LMA side, otherwise the UDP tunnel will not be established.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 21** logical-mn network-access-identifier

Enables the mobile router functionality in MAG.

**Step 22** address {ipv4 ipv4-address | ipv6 ipv6-address | dynamic}

Configures an IPv4, an IPv6, or dynamic address for a MAG or LMA.

**Step 23** home interface type

Enables the MAG service on the specified interface.

### Configuration Example: MAG Configuration with Dynamic IP Address on Logical MN Interface

```
Router(config)# platform usb modem 1234567890
1234567890
Router(config)# interface loopback 1
Router(config-if)# exit
Router(config)# ipv6 unicast-routing
Router(config)# ip route 0.0.0.0 0.0.0.0 Virtual-PPP4001
Router(config)# ipv6 mobile pmipv6-domain D1
Router(config-ipv6-pmipv6-domain)# encap udptunnel
Router(config-ipv6-pmipv6-domain)# lma LMA1
Router(config-ipv6-pmipv6-domain-lma)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6-domain-lma)# exit
Router(config-ipv6-pmipv6-domain-mn)# lma LMA1
Router(config-ipv6-pmipv6-domain-mn)# exit
Router(config-ipv6-pmipv6-domain)# ipv6 mobile pmipv6-mag M1 domain D1
Router(config-ipv6-pmipv6-mag)# address dynamic
Router(config-ipv6-pmipv6-mag-addr-dyn)# roaming interface Virtual-PPP4001 priority 1 egress-att 3g label etyr
Router(config-ipv6-pmipv6-mag-addr-dyn)# interface loopback1
Router(config-ipv6-pmipv6-mag-intf)# interface GigabitEthernet0/0/1
Router(config-ipv6-pmipv6-mag-intf)# lma LMA1 D1
Router(config-ipv6-pmipv6-mag-intf)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6-mag-intf)# auth-option spi 67 key ascii key1
Router(config-ipv6-pmipv6-mag-intf)# logical-mn MN5@cisco.com
Router(config-ipv6-pmipv6-mag-logicalmn)# address dynamic
Router(config-ipv6-pmipv6-mag-logicalmn)# home interface loopback1
```

### Configuration Example: MAG Configuration with Static IP Address on Logical MN Interface

```
Router(config)# platform usb modem 1234567890
1234567890
Router(config)# interface loopback 1
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)# exit
Router(config)# ipv6 unicast-routing
Router(config)# ip route 0.0.0.0 0.0.0.0 Virtual-PPP4001
Router(config)# ipv6 mobile pmipv6-domain D1
Router(config-ipv6-pmipv6-domain)# encap udptunnel
```
Configuring the LMA

**SUMMARY STEPS**

1. **ip local pool**  
   `pool-name low-ip-address high-ip-address`
2. **ipv6 mobile pmipv6-domain**  
   `domain-name`
3. **auth-option spi**  
   `{spi-hex-value | decimal spi-decimal-value}`  
   **key**  
   `{ascii ascii-string | hex hex-string}`
4. **encap udptunnel**
5. **nai**  
   `user@realm`
6. **network**  
   `network-name`
7. **ipv6 mobile pmipv6-lma**  
   `lma-id domain-name [force]`
8. **address ipv4 ipv4-address | ipv6 ipv6-address | dynamic**
9. **dynamic mag learning**
10. **network**  
    `network-name`
11. **pool ipv4 name pfxlen length**
12. **ip route**  
    `prefix mask interface-name`
13. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
  `ip local pool pool-name low-ip-address high-ip-address` | Configures a pool of IP addresses from which the LMA assigns an IP address to the MAG. |
| **Step 2**  
  `ipv6 mobile pmipv6-domain domain-name` | Creates a PMIPv6 domain. |
| **Step 3**  
  `auth-option spi {spi-hex-value | decimal spi-decimal-value}`  
  **key**  
  `{ascii ascii-string | hex hex-string}` | Configures authentication for the PMIPv6 domain. |
  | **Note** | This authentication should match that at the MAG side, otherwise the UDP tunnel will not be established. |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>encap udptunnel</code></td>
<td>Configures the UDP tunnel encapsulation between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA).</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>nai user@realm</code></td>
<td>Configures a network access identifier (NAI) for the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain mobile node configuration mode. <strong>Note</strong> Multiple MAGs can be added in the LMA.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>network network-name</code></td>
<td>Associates a network, to which an IPv4 or IPv6 pool can be configured, with an LMA.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>ipv6 mobile pmipv6-lma lma-id domain domain-name [force]</code></td>
<td>Enables the LM) service on the router and configures the Proxy Mobile IPv6 (PMIPv6) domain for the LMA.</td>
</tr>
<tr>
<td>Step 8</td>
<td>`address ipv4 ipv4-address</td>
<td>ipv6 ipv6-address</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>dynamic mag learning</code></td>
<td>Enables the LMA to accept PMIPv6 signaling messages from any MAG that is not locally configured.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>network network-name</code></td>
<td>Associates a network, to which an IPv4 or IPv6 pool can be configured, with an LMA.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>pool ipv4 name pfhlen length</code></td>
<td>Specifies the name of the IPv4 address pool, from which a home address is allocated to a mobile node (MN), in the LMA.</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>ip route prefix mask interface-name</code></td>
<td>Creates a route to reach the MAG through the dongle interface.</td>
</tr>
<tr>
<td>Step 13</td>
<td><code>exit</code></td>
<td>Exits the interface.</td>
</tr>
</tbody>
</table>

### Configuration Example

```plaintext
ip local pool v4pool 10.10.10.0 10.10.10.254
! ipv6 mobile pmipv6-domain D1
  auth-option spi 64 key ascii 100
  encap udptunnel
  nai MN5@cisco.com
  network net1 ipv6 mobile pmipv6-lma LMA1 domain D1
  address ipv4 173.39.88.101
dynamic mag learning
  network net1	pool ipv4 v4pool pfhlen 24
! ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/2
exit
```
Verifying the Configuration

MAG Call Setup

On the MAG:

```
ASR920-MAG# show ipv6 mobile pmipv6 mag binding
Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, NAI: MN5@cisco.com
    [Binding][MN]: State: ACTIVE
    [Binding][MN]: Interface: Loopback1
    [Binding][MN]: Hoa: 10.10.10.1, Att: 4, llid: MN5@cisco.com
    [Binding][MN]: HNP: 0
    [Binding][MN][LMA]: Id: LMA1
    [Binding][MN][LMA]: Lifetime: 3600
    [Binding][MN][PATH]: interface: Virtual-PPP4001, Label: etyr
        State: PATH_ACTIVE
        Tunnel: Tunnel0
        Refresh time: 300(sec), Refresh time Remaining: 272(sec)
----------------------------------------
```

On the LMA:

```
ASR1000-LMA# show ipv6 mobile pmipv6 lma binding
Total number of bindings: 1
----------------------------------------
[Binding][MN]: State: BCE_ACTIVE
[Binding][MN]: Domain: D1, NAI: MN5@cisco.com
[Binding][MN]: HOA: 10.10.10.1, Prefix: 24
[Binding][MN]: HNP: 0
[Binding][MN][PEER]: Default Router: 10.10.10.0
    [Binding][MN]: ATT: WLAN (4)
    [Binding][MN][PEER1]: llid: MN5@cisco.com
    [Binding][MN][PEER1]: Id: dynamic_mag165
    [Binding][MN][PEER1]: Lifetime: 3600(sec)
    [Binding][MN][PEER1]: Lifetime Remaining: 3538(sec)
    [Binding][MN][PEER1]: Tunnel: Tunnel0
    [Binding][MN][GREKEY]: Upstream: 1, Downstream: 0
----------------------------------------
```

Note

If the LMA has bindings to multiple MAGs, use the following command to view a specific MAG:
```
show ipv6 mobile pmipv6 LMA binding nai MN5@cisco.com.
```

MAG Data Path

- To verify the dynamic tunnel created between the MAG and the LMA:
  
  `show interface tunnel tunnel-number`

- To verify dongle interface status (virtual ppp interface) and tunnel status:
show ip interface brief

ASR920-MAG# show ip int brief | i Virtual-PPP4001
Virtual-PPP4001    106.216.155.17 YES unset up up
ASR920-MAG# show ip int brief | i Tunnel
Tunnel0            106.216.155.17 YES unset up up

Note
Addresses assigned to the MN should be from the local pool configured in the LMA.

• To verify dynamic route map created in MAG:

  show route-map dynamic

Debug Commands
The following debugs can be used to debug the call flow information and events.

• debug ipv6 mobile mag events
• debug ipv6 mobile mag info
• debug ipv6 mobile mag api

To view the packet level information messages, use

• debug ipv6 mobile packets

To clear the PMIPv6 bindings and statistics:

• clear ipv6 mobile pmipv6 mag binding all
• clear ipv6 mobile pmipv6 mag binding nai MN-nai

Related Documents
For more information on mobility commands, see the Cisco IOS IP Mobility Command Reference.
Power Over Ethernet

Effective Cisco IOS XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router supports Power over Ethernet (PoE). PoE is the ability for any LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint or powered device.

Prerequisites for PoE

- Cisco ASR-920-12SZ-IM Aggregation Services Router supports multiple variants of power supplies. When using the AC power supplies, approximately 180 watts is used for PoE functionality, which can be shared by all eight available copper Ethernet ports.
- PoE is applicable only on the following ports: Gi0/0/0 to Gi 0/0/7
- When using DC power supplies, PoE is supported only if the input feed to the power-supply is 48 volts.

Restrictions for PoE

- Configuring a port as a static port pre-provisions power for that port. This power is deducted from the central power pool. It is, therefore, advisable to configure a port as an auto port.
- PoE does not support interface modules (IMs).
- The system allocates 180 W of static power. However, if a component or device tries to draw power over 180 W, the Cisco ASR-920-12SZ-IM Router silently reloads.

Information About PoE

The Cisco ASR-920-12SZ-IM Router uses the inline power as well as a global pool of power to power the modules, fans and other subsystems in the router. This power is allotted to all the powered devices detected on a first-come-first-serve basis. However, if many devices are connected, and a new device is added to
the system, the system may run out of power to allot to the new device. Over-subscription of power could also result in tripping the power supplies and bringing down modules or even the entire router. In such cases, PoE can manage power allocation.

Note

In the Cisco ASR-920-12SZ-IM Router, the dual power supplies function in redundant power mode.

PoE supports the following two modes of operations:

- Automatic—The automatic mode supports POE, POE+, and UPoE power negotiations up to the maximum power specified by the these different standards. UPoE is a Cisco proprietary standard, which can draw up to 60 W of power and supports LLDP negotiations. To enable UPoE mode, ensure that LLDP is not only enabled globally but also at the port level.
- Four-Pair Forced—This mode is enabled through the command line interface and can be used for third-party PoE devices that may need more than 30 Watts of power, but are not expected to have the Layer-2 power negotiation protocol, such as LLDP.

PoE License

PoE can be enabled only through the PoE license. As the PoE ports are controlled by the Port License, you must enable the PoE Port License as well as the PoE license to use this feature. Once you install the PoE license and enable the feature, the router attempts to detect and classify PoE on those PoE ports that are in ADMIN_UP state and the link state in DOWN state.

Installing the PoE License

To install or upgrade a license by using the license install command, you must have already received the license file from the Cisco Product License Registration portal at www.cisco.com/go/license (or you already backed up the license by using the license save command).

```
Router# license install bootflash:upoe.lic
Installing licenses from “bootflash:upoe.lic”
Installing...Feature:UPOE...Successful:Not Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

For more information on installing licenses, see Configuring the Cisco IOS Software Activation Feature.

How to Configure the PoE

SUMMARY STEPS

1. In the global config mode, select the interface to configure.
2. To determine how inline power is applied to the device on the specified port, use the power inline command:
3. If the interfaces tries to draw more power than negotiated through LLDP, the power inline police action errdisable command sets the port to errdisables mode.
4. Exit the configuration mode by running:
DETAILED STEPS

Step 1
In the global config mode, select the interface to configure.
Example:

```
Router(config)# interface gigabitethernet 0/0/1
```

Step 2
To determine how inline power is applied to the device on the specified port, use the `power inline` command:
Example:

```
Router(config-if)# power inline
```

Use one of the following options with the above command:
- **auto**—Enables the device discovery protocol and applies power to the device, if found.
- **four-pair**—Enables the four-pair mode.
- **never**—Disables the device discovery protocol and stops supplying power to the device.
- **police**—Enables inline power policing; optional if entering the no form of the command. Default is disabled.
- **static**—High priority PoE interface. The Cisco ASR-920-12SZ-1M Router preallocates power to the interface, even when nothing is connected, guaranteeing that there will be power for the interface. You can specify the maximum wattage that is allowed on the interface using the `power inline static max value` command. If you do not specify a wattage, the switch preallocates the hardware-supported maximum value of 60 W. If the switch does not have enough power for the allocation, the command will fail, after which you must execute the `shutdown` command to initiate the detection of the powered device.
- **max**—(Optional) This parameter configures the maximum power that a powered device can draw.

Step 3
If the interface tries to draw more power than negotiated through LLDP, the `power inline police action errdisable` command sets the port to errdisable mode.
Example:

```
Router(config-if)# power inline police action errdisable
```

Step 4
Exit the configuration mode by running:
Example:

```
Router(config-if)# end
Router(config)# end
Router#
```

Verifying the PoE Configuration

- The following is a sample output of the `show power` command:

```
Router# show power
Power Summary Maximum
```
Verifying the PoE Configuration

(in Watts) Used Available
-------------------- ---- --------
Inline Power 0.0 180

• The following is a sample output of the show power inline command:

```
Router# show power inline
Available:180.0(w) Used:15.4(w) Remaining:164.6(w)

Interface Admin Oper Power Device Class Max
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0 auto on 15.4 Ieee PD 0 60.0
Gi0/0/1 auto off 0.0 n/a n/a 60.0
Gi0/0/2 auto off 0.0 n/a n/a 60.0
Gi0/0/3 auto off 0.0 n/a n/a 60.0
Gi0/0/4 auto off 0.0 n/a n/a 60.0
Gi0/0/5 auto off 0.0 n/a n/a 60.0
Gi0/0/6 auto off 0.0 n/a n/a 60.0
Gi0/0/7 auto off 0.0 n/a n/a 60.0
```

Router# show power inline gigabitethernet 0/0/0 detail

Interface: Gi0/0/0
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee
Police: off
Power Allocated
Admin Value: 60.0
Power drawn from the source: 0.0
Power available to the device: 0.0
Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0
Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

• The following is a sample output for port policing using the show power inline police commands:

```
Router# show power inline police
Available:180.0(w) Used:15.4(w) Remaining:164.6(w)
Interface Admin Oper Admin Oper Cutoff Oper Power Power
--------- ------ ------ ------ ---------- ------- ------- -------
Gi0/0/0 auto on none n/a n/a 0.0
Gi0/0/1 auto off none n/a n/a n/a
Gi0/0/2 auto off none n/a n/a n/a
Gi0/0/3 auto off none n/a n/a n/a
Gi0/0/4 auto off none n/a n/a n/a
Gi0/0/5 auto off none n/a n/a n/a
Gi0/0/6 auto off none n/a n/a n/a
Gi0/0/7 auto off none n/a n/a n/a
```

Totals:

0.0
Debugging the PoE Configuration

- Use the following command to troubleshoot the PoE Configuration

Router# debug inline power

- Use the following commands to verify if the PoE license is enabled:

Router# show license detail
Index: 1 Feature: UPOE Version: 1.0
License Type: Permanent
License State: Active, Not in Use
License Count: Non-Counted
License Priority: Medium
Store Index: 0
Store Name: Primary License Storage
Index: 2 Feature: advancedmetroipaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use, EULA accepted
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
Period used: 0 minute 0 second
License Count: Non-Counted
License Priority: Low
Store Index: 0
Store Name: Built-In License Storage
Index: 3 Feature: metroaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
Period used: 0 minute 36 seconds
License Count: Non-Counted
License Priority: Low
Store Index: 2
Store Name: Built-In License Storage
Index: 4 Feature: metroipaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
Period used: 0 minute 0 second
License Count: Non-Counted
License Priority: Low
Store Index: 1
Store Name: Built-In License Storage

Router# show license feature
Feature name Enforcement Evaluation Subscription Enabled RightToUse
advancedmetroipaccess yes yes no no no
metroipaccess yes yes no no no
metroaccess no yes no no no
atm yes yes no no no
oc3 yes yes no no no
oc12 yes yes no no no
1588 yes yes no no no
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3af</td>
<td>The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power to each device.</td>
</tr>
<tr>
<td>802.3at</td>
<td>The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• POWER-ETHERNET-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-POWER-ETHERNET-MIB</td>
<td></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no new RFCs for this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to install</td>
<td></td>
</tr>
<tr>
<td>and configure the software and to troubleshoot and resolve technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies. Access to most tools on the Cisco</td>
<td></td>
</tr>
<tr>
<td>Support and Documentation website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Power Over Ethernet

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 6: Feature Information for Phrase Based on Module Title

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Over Ethernet</td>
<td>Cisco IOS-XE Release 3.16.0S</td>
<td>In this release, this feature was introduced on the Cisco ASR-920-12SZ-IM Aggregation Services Router.</td>
</tr>
</tbody>
</table>
Configuring T1/E1 Interfaces

Effective Cisco IOS-XE Release 3.14.0S, the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Router supports the following types of interface modules (IMs):

- 8x1G Cu IM (A900-IMA8T)
- 8xT1/E1 IM (A900-IMA8D)
- 1x10G IM (A900-IMA1Z)
- 2x10G IM (A900-IMA2Z)

Effective Cisco IOS-XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router supports the following types of interface modules (IMs):

- A900-IMA8T
- A900-IMA8S
- A900-IMA8D
- A900-IMA16D
- A900-IMA1X

This chapter provides information about configuring the T1/E1 interface module on the Cisco ASR 920 Series Router. 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.

The router does not support swapping of the TDM interface modules to Gigabit Ethernet modules. If the TDM interface module is swapped with the Gigabit Ethernet module in the same slot or vice-versa, the router must be reloaded.

- Configuration Tasks, on page 67
- Verifying the Interface Configuration, on page 81
- Configuration Examples, on page 81

Configuration Tasks

This section describes how to configure the T1/E1 interface module for the Cisco ASR 920 Series Router.
Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module on the Cisco ASR 920 Series Router.

- The Cisco ASR 920 Series Router does not support ATM and IMA on T1/E1 interface modules.
- The Cisco ASR 920 Series Router only supports the following BERT patterns: $2^{11}$, $2^{15}$, $2^{20}$-O153, and $2^{20}$-QRSS.
- When TDM is inserted in the Cisco ASR 920 Series Router, it should be activated by running the `hw-module subslot slot-number/subslot-number activate` command in EXEC mode.

This command removes the following ports from front panel and brings up the respective IMs:

- Slots 20–23 for T1E1 IMs
- Slot 16–23 for copper IMs

Once the TDM is activated, you must reload the router to bring up the T1/E1 interface module.

---

**Note**

The above command is not required to bring up the 8X1G Cu, 1x10G and 2x10G IMs.

- To recover the front panel ports from the IMs, run the `hw-module subslot slot-number/subslot-number deactivate` command in EXEC mode.
- The above activation and deactivation commands assume that the correct IM is inserted in its corresponding slot. If an IM inserted in a different slot than what is activated, the IM does not come up and the corresponding front panel interfaces are removed.
- front panel interfaces will be removed
- L2TPv3 encapsulation is not supported on the Cisco ASR 920 Series Router.
- CEM on access BDI in core is not supported.
- Any change in the card type requires a router reload. To change the card type, the current card type must be unconfigured, then the router must be reloaded, and then the new card type must be changed.
- The Payload calculation per unit for T1/E1 interface module is:
  - Framed E1 / T1 with no. of time slots less than 4 → Payload = 4 x no. of time slots
  - Framed E1 / T1 with no. of timeslots greater than or equal 4 → Payload = 2 x no. of time slots
  - Unframed T1, C11 → Payload = 48 (2 x 24 (all slots))
  - Unframed E1, C12 → Payload = 64 (2 x32 (all slots))
- Channelization is not supported for serial interfaces. However, channelization is supported for CEM at the DS0 level.

---

**Note**

A card type change cannot be applied when the interface module is booting up. You must wait until after the interface module is administratively up.
Required Configuration Tasks

This section lists the required configuration steps to configure the T1/E1 interface module. 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.

Activating the IMs

SUMMARY STEPS

1. Verify that the correct IM is inserted properly in IM slot
2. Shut down all interfaces that are active in system and which will be removed during the IM activation process.
3. Wait for a minute.
4. Default all interfaces that will be removed from the system.
5. Activate the correct IM type that is preset in the IM slot.

DETAILED STEPS

Step 1 Verify that the correct IM is inserted properly in IM slot
Step 2 Shut down all interfaces that are active in system and which will be removed during the IM activation process.
   • Slots 20–23 for T1E1 IMs
   • Slot 16–23 for copper IMs
Step 3 Wait for a minute.
Step 4 Default all interfaces that will be removed from the system.
Step 5 Activate the correct IM type that is preset in the IM slot.

Deactivating the IMs

SUMMARY STEPS

1. Verify that IM is in 'OK' state.
2. Using the no interface interface-name command, remove all the Virtual Interfaces associated with the IM. These include MPLS TP tunnels, TE tunnels, BDI interface, Port-Channel interface and so on.
3. Shut down all pluggable IM interfaces in system.
4. Wait for a minute.
5. Default all pluggable IM interfaces in the system.
6. Deactivate the pluggable IMs.

DETAILED STEPS

Step 1 Verify that IM is in 'OK' state.
### Setting the Card Type

The interface module is not functional until the card type is set. Information about the interface module 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 T1 and E1 interface types is not supported. All ports on the interface module must be of the same type.

To set the card type for the T1/E1 interface module, complete these steps:

**SUMMARY STEPS**

1. Router# **configure terminal**
2. Router(config)# **card type** \{e1 | t1\} slot subslot
3. Router(config)# **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router# <strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** Router(config)# **card type** \{e1 | t1\} slot subslot | Sets the serial mode for the interface module:  
  - t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default linecode 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.  
  - slot subslot — Specifies the location of the interface module. |
| **Step 3** Router(config)# **exit** | Exits configuration mode and returns to the EXEC command interpreter prompt. |

**Configuring the Controller**

To create the interfaces for the T1/E1 interface module, complete these steps:
SUMMARY STEPS

1. Router# configure terminal
2. Router(config)# controller {t1 | e1} slot/port
3. Router(config-controller)# clock source {internal | line}
4. Router(config-controller)# linecode {ami | b8zs | hdb3}
5. For T1 Controllers:
   6. cablelength {long | short}
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Router(config)# controller {t1</td>
<td>e1} slot/port</td>
</tr>
<tr>
<td></td>
<td>• t1—Specifies the T1 controller.</td>
</tr>
<tr>
<td></td>
<td>• e1—Specifies the E1 controller.</td>
</tr>
<tr>
<td></td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The slot number is always 0 and subslot number is always 1.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config-controller)# clock source {internal</td>
<td>line}</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• internal—Specifies that the internal clock source is used.</td>
</tr>
<tr>
<td></td>
<td>• line—Specifies that the network clock source is used. This is the default for T1 and E1.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config-controller)# linecode {ami</td>
<td>b8zs</td>
</tr>
<tr>
<td></td>
<td>• ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.</td>
</tr>
<tr>
<td></td>
<td>• b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines.</td>
</tr>
<tr>
<td></td>
<td>• hdb3—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.</td>
</tr>
<tr>
<td><strong>Step 5</strong> For T1 Controllers: <strong>Example:</strong></td>
<td>For E1 Controllers:</td>
</tr>
<tr>
<td></td>
<td>Selects the framing type.</td>
</tr>
<tr>
<td></td>
<td>• sf—Specifies Super Frame as the T1 frame type.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Router(config-controller)# framing {crc4</td>
</tr>
</tbody>
</table>

### Purpose

- **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.

### Step 6

| `cablelength {long | short}` |
| --- |
| Example: `Router(config-controller)# cablelength long` |

To fine-tune the pulse of a signal at the receiver for an E1 cable, use the `cablelength` command in controller configuration mode.

### Step 7

<table>
<thead>
<tr>
<th><code>exit</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: <code>Router(config)# exit</code></td>
</tr>
</tbody>
</table>

Exits configuration mode and returns to the EXEC command interpreter prompt.

---

### Verifying Controller Configuration

To verify the controller configuration, use the `show controllers` command:

```
Router# show controllers t1 0/1 brief
T1 0/1 is up.
  Applique type is A900-IMA16D
  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 Internal.
  Data in current interval (230 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0Errored 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
  Total Data (last 24 hours):
    136 Line Code Violations, 63 Path Code Violations,
    0 Slip Secs, 6 Fr Loss Secs, 4 Line Err Secs, 0 Degraded Mins,
    7Errored Secs, 1 Bursty Err Secs, 6 Severely Err Secs, 458 Unavail Secs
    2 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

---

### Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your T1/E1 interface module.

### 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.
SUMMARY STEPS

1. Router# configure terminal
2. Router(config)# controller {t1 | e1} slot/port
3. For T1 controllers
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# controller {t1</td>
</tr>
<tr>
<td></td>
<td>Selects the controller to configure.</td>
</tr>
<tr>
<td></td>
<td>• t1—Specifies the T1 controller.</td>
</tr>
<tr>
<td></td>
<td>• e1—Specifies the E1 controller.</td>
</tr>
<tr>
<td></td>
<td>• slot/port—Specifies the location of the controller.</td>
</tr>
<tr>
<td></td>
<td>Note The slot number is always 0 and subslot number is always 1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>For T1 controllers</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# framing {sf</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# framing {crc4</td>
</tr>
<tr>
<td></td>
<td>For E1 controllers</td>
</tr>
<tr>
<td></td>
<td>Sets the framing on the interface.</td>
</tr>
<tr>
<td></td>
<td>• sf—Specifies Super Frame as the T1 frame type.</td>
</tr>
<tr>
<td></td>
<td>• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.</td>
</tr>
<tr>
<td></td>
<td>• crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1.</td>
</tr>
<tr>
<td></td>
<td>• no-crc4—Specifies no CRC4 as the E1 frame type.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

Router# show controllers t1 0/1 brief
T1 0/1 is up.
Applique type is A900-IMA16D
Cable length 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 (740 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
### Setting an IP Address

To set an IP address for the serial interface, complete these steps:

**Note**
You can also set an IP address using an IMA or CEM configuration.

#### SUMMARY STEPS

1. `Router(config)# interface serial slot/port`
2. `Router(config-if)# ip address address mask`
3. `Router(config)# exit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>Router(config)# interface serial slot/port</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>Router(config-if)# ip address address mask</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>Router(config)# exit</code></td>
</tr>
</tbody>
</table>

**What to do next**

**Note**
IPV4 routing protocols, such as `eigrp`, `ospf`, `bgp`, and `rip`, are supported on serial interfaces.

### Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic.
L2TPv3 encapsulation is not supported on the Cisco ASR 920 Series Routers.

To set the encapsulation method, use the following commands:

**SUMMARY STEPS**

1. Router# configure terminal
2. Router(config)# interface serial slot/port
3. Router(config-if)# encapsulation encapsulation-type {hdlc | ppp}
4. Router(config)# exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Router(config)# interface serial slot/port</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• slot—Specifies the slot in which the T1/E1 interface module is installed.</td>
</tr>
<tr>
<td></td>
<td>• port—Specifies the location of the controller. The port range for T1 and E1 is 0 to 1.</td>
</tr>
<tr>
<td>Step 3 Router(config-if)# encapsulation encapsulation-type {hdlc</td>
<td>ppp}</td>
</tr>
<tr>
<td></td>
<td>• hdlc—High-Level Data Link Control (HDLC) protocol for a 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.</td>
</tr>
<tr>
<td></td>
<td>• ppp—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.</td>
</tr>
<tr>
<td>Step 4 Router(config)# exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

**Verifying Encapsulation**

Use the show interfaces serial command to verify encapsulation on the interface:

```
Router# show interfaces serial 0/1
Serial0/1 is up, line protocol is up
   Hardware is Multichannel T1
   MTU 1500 bytes, BW 1536 Kbit/sec, 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 00:00:01, output 00:00:02, 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
60 packets input, 8197 bytes, 0 no buffer
Received 39 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
64 packets output, 8357 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions

Configuring the CRC Size for T1 Interfaces

All T1/E1 serial 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.

To set the length of the cyclic redundancy check (CRC) on a T1 interface, use these commands:

**SUMMARY STEPS**

1. Router# configure terminal
2. Router(config)# interface serial slot/port
3. Router(config-if)# crc {16 | 32}
4. Router(config)# exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# interface serial slot/port</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# crc {16</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring T1/E1 Interfaces

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
</tbody>
</table>

#### Verifying the CRC Size

Use the `show interfaces serial` command to verify the CRC size set on the interface:

```
Router# show interfaces serial 0/1
Serial0/1 is up, line protocol is up
    Hardware is Multichannel T1
    MTU 1500 bytes, BW 1536 Kbit/sec, 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 00:00:01, output 00:00:02, 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
        60 packets input, 8197 bytes, 0 no buffer
        Received 39 broadcasts (0 IP multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        64 packets output, 8357 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 unknown protocol drops
        0 output buffer failures, 0 output buffers swapped out
        1 carrier transitions
```

#### Saving the Configuration

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

```
Router# copy running-config startup-config
```

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.

#### Troubleshooting E1 and T1 Controllers

You can use the following methods to troubleshoot the E1 and T1 controllers using Cisco IOS software:

---

**Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x**
Setting a Loopback on the E1 Controller

To set a loopback on the E1 controller, perform the first task followed by any of the following tasks beginning in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Select the E1 controller and enter controller configuration mode.</td>
<td>controller e1 slot/port</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>Set a diagnostic loopback on the E1 line.</td>
<td>loopback diag</td>
</tr>
<tr>
<td>Set a network payload loopback on the E1 line.</td>
<td>loopback network {line</td>
</tr>
<tr>
<td>Exit configuration mode when you have finished configuring the controller.</td>
<td>end</td>
</tr>
</tbody>
</table>

Setting a Loopback on the T1 Controller

You can use the following loopback commands on the T1 controller in global configuration mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the T1 controller and enter controller configuration mode.</td>
<td>controller t1 slot/port</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The slot number is always 0.</td>
</tr>
<tr>
<td>Sets a local loopback on the T1 line. You can select to loopback the line or the payload.</td>
<td>loopback local {line</td>
</tr>
<tr>
<td>Sets a remote loopback on the T1 line. This loopback setting will loopback the far end at line or payload, using IBOC (in band bit-orientated code) or the Extended Super Frame (ESF) loopback codes to communicate the request to the far end.</td>
<td>loopback remote iboc</td>
</tr>
<tr>
<td>Exits configuration mode when you have finished configuring the controller.</td>
<td>end</td>
</tr>
</tbody>
</table>

Note

To remove a loopback, use the **no loopback** command.

Table 7: Loopback Descriptions

<table>
<thead>
<tr>
<th>Loopback</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback local</td>
<td>Loops the incoming receive signal back out to the transmitter. You can specify whether to use the line or payload.</td>
</tr>
</tbody>
</table>
**Loopback**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>loopback network</strong></td>
</tr>
<tr>
<td><strong>loopback remote iboc</strong></td>
</tr>
<tr>
<td><strong>network line</strong></td>
</tr>
<tr>
<td><strong>network payload</strong></td>
</tr>
</tbody>
</table>

---

**Running Bit Error Rate Testing**

Bit error rate testing (BERT) is supported on each of the E1 or T1 links. The BERT testing is done only over a framed E1 or T1 signal and can be run only on one port at a time.

The interface modules contain onboard BERT circuitry. With this, the interface module software can send and detect a programmable pattern that is compliant with CCITT/ITU O.151, O.152, and O.153 pseudo-random and repetitive test patterns. BERTs allows you to test cables and signal problems in the field.

When running a BER test, your system expects to receive the same pattern that it is transmitting. To help ensure this, two common options are available:

- Use a loopback somewhere in the link or network
- Configure remote testing equipment to transmit the same BERT test pattern at the same time

To run a BERT on an E1 or T1 controller, perform the following optional tasks beginning in global configuration mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
</table>
| Selects the E1 or T1 controller and enters controller configuration mode. | Router(config)# controller {e1 | t1} slot/port  
Note The slot number is always 0. |
| Specifies the BERT pattern for the E1 or T1 line and the duration of the test in minutes. The valid range is 1 to 1440 minutes. | Router(config-controller)# bert pattern {2^15 | 2^23 | All 1's} interval minutes  
Note Only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported. |
| Exit configuration mode when you have finished configuring the controller. | Router(config-controller)# end |
| Displays the BERT results. | show controllers {e1 | t1} slot/port |
The following keywords list different BERT keywords and their descriptions.

Table 8: BERT Pattern Descriptions

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1s</td>
<td>Repeating pattern of ones (...111...).</td>
</tr>
<tr>
<td>$2^{15}$</td>
<td>Pseudo-random O.151 test pattern that is 32,768 bits in length.</td>
</tr>
<tr>
<td>$2^{23}$</td>
<td>Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.</td>
</tr>
</tbody>
</table>

Both the total number of error bits received and the total number of bits received are available for analysis. You can select the testing period from 1 minute to 24 hours, and you can also retrieve the error statistics anytime during the BER test.

**Note** To terminate a BERT test during the specified test period, use the `no bert` command.

**Note** BERT is supported only on controllers with channel-group configured. If CEM, IMA, or ATM are configured on controller, the BERT option is disabled.

**Note** When BERT is running, the serial interface of that controller will be made down till BERT is complete.

You can view the results of a BERT test at the following times:

- After you terminate the test using the `no bert` command
- After the test runs completely

### Monitoring and Maintaining the T1/E1 Interface Module

After configuring the new interface, you can monitor the status and maintain the interface module by using `show` commands. To display the status of any interface, complete any of the following tasks in **EXEC** mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the status of the E1 or T1 controller.</td>
<td>`show controllers {e1</td>
</tr>
<tr>
<td>Displays statistics about the serial information for a specific E1 or T1 channel group. Valid values are 0 to 30 for E1 and 0 to 23 for T1.</td>
<td><code>show interface serial slot/port</code></td>
</tr>
<tr>
<td>Clears the interface counters.</td>
<td><code>clear counters serial slot/port</code></td>
</tr>
</tbody>
</table>
To change the T1/E1 card type configuration, use the no card type command and reload the router.

Verifying the Interface Configuration

Besides using the `show running-configuration` command to display your Cisco ASR 920 Series Router 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 T1/E1 interface module.

Verifying Per-Port Interface Status

To view detailed interface information on a per-port basis for the T1/E1 interface module, use the `show interfaces serial` command.

```
Router# show interfaces serial 0/1/x
Serial0/1/x is up, line protocol is up
Hardware is ASR900-IMA8D
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
```

Configuration Examples

This section includes the following configuration examples:

Example: Framing and Encapsulation Configuration

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
```
Example: CRC Configuration

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
! Router(config)# interface serial 0/1/x
!
! 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
```

Example: Facility Data Link Configuration

The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
! Router(config)# controller t1 0/1/x
!
! Specify the FDL specification
! Router(config-controller)#
! fdl ansi
!
! Exit controller configuration mode and return to global configuration mode
```
Example: Invert Data on the T1/E1 Interface

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 0/1/x
! 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
Example: Invert Data on the T1/E1 Interface
Installing and Upgrading Software

This chapter describes how to update software on the Cisco ASR 920 Series Router.

- Upgrading Field Programmable Hardware Devices, on page 85
- File Systems on the Cisco ASR 920 Series Router, on page 85
- Restrictions, on page 86
- System Requirements, on page 86
- Autogenerated Files and Directories, on page 87
- Upgrading the Router Software, on page 88
- Verifying the Upgrade, on page 92
- Software Upgrade Example, on page 92

Upgrading Field Programmable Hardware Devices

Cisco IOS XE on Cisco ASR 920 Series Routers (ASR-920-24SZ-IM and ASR-920-12SZ-IM) support upgradeable firmware for field programmable hardware devices such as interface modules (IMs) and upgrades IM FPGA when ever there is an upgrade.

Cisco ASR 920 Series Router upgrades the HOFPGA when required and is indicated to the user through logs. Generally an upgrade is only necessary in cases where a system message indicates that an upgrade is required or a Cisco technical support representative suggests an upgrade.

The procedures in this chapter describe how to upgrade the firmware on Cisco ASR 920 Series Router.

File Systems on the Cisco ASR 920 Series Router

The table below provides a list of file systems that can be seen on the Cisco ASR 920 Series Router.

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>The boot flash memory file system.</td>
</tr>
<tr>
<td>cns:</td>
<td>The Cisco Networking Services file directory.</td>
</tr>
<tr>
<td>nvram:</td>
<td>Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.</td>
</tr>
</tbody>
</table>
### File System Description

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system:</td>
<td>The system memory file system, which includes the running configuration.</td>
</tr>
<tr>
<td>bin:</td>
<td>The archive file system.</td>
</tr>
<tr>
<td>tmpsys:</td>
<td>The temporary system files file system.</td>
</tr>
<tr>
<td>usb[0-1]:</td>
<td>The Universal Serial Bus (USB) flash drive file systems.</td>
</tr>
</tbody>
</table>

If you see a file system not listed in the table above, enter the `?` help option or see the `copy` command reference for additional information on that file system.

### Restrictions

When you migrate to Cisco IOS-XE Release 3.18 SP, HOFPGA upgrade is mandatory and not optional. The router works for few minutes after the first reboot is complete and starts a second reboot without a notice.

### System Requirements

The following sections describe the system requirements for the Cisco ASR 920 Series Router software:

#### Memory Recommendations

These are the recommendation for the routers for the Cisco IOS XE images and packages:

- **DRAM Memory**—4 GB
- **Software Image**—asr920-universalk9_npe.bin—420 MB (ASR 920-24SZ-IM)
- **Software Image**—asr920-universalk9_npe.bin—430 MB (ASR 920-12SZ-IM)

#### ROMmon Version Requirements

Following are the recommended release versions for all ROMmon upgradeable components. For more information about ROMmon images, see Release Notes.

- **ROMmon Release 15.6(24r)S** for router ASR-920-12SZ-IM

#### Bootflash Space Requirements

The dual-rate functionality requires a minimum of 10 MB available space in bootflash memory on Cisco ASR 920 Series Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, ASR-920-8S4Z-PD, and ASR-920-12SZ-IM).
Determining the Software Version

The Cisco IOS XE image is stored as a bin file in a directory that is named with the Cisco IOS XE release. The image is stored on the system board bootflash device (bootflash:).

If you try to copy or archive upgrade beyond the bootflash memory capacity, the action aborts.

You can use the `show version` privileged EXEC command to see the software version that is running on your router. The second line of the display shows the version.

You can also use the `dir bootflash:` privileged EXEC command to see the names of other software images that you might have stored in bootflash.

Cisco IOS XE 3S to Cisco IOS Version Number Mapping

Each version of Cisco IOS XE 3S has an associated Cisco IOS version. The table below lists these mappings for Release 3.13.0S and forward.

<table>
<thead>
<tr>
<th>Cisco IOS XE 3S Version</th>
<th>Cisco IOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.13.0S</td>
<td>15.4(3)S</td>
</tr>
<tr>
<td>3.14.0S</td>
<td>15.5(1)S</td>
</tr>
</tbody>
</table>

The Cisco ASR 920 Series Router does not support IOS XE versions prior to 3.13.0S.

Autogenerated Files and Directories

The table below provides a list and descriptions of autogenerated files on the router.

Do not alter any autogenerated file in the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by customer support; altering these files can have unpredictable consequences for system performance.

<table>
<thead>
<tr>
<th>File or Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo files</td>
<td>A crashinfo file may appear in the bootflash: file system. Crashinfo files are useful for tuning and troubleshooting, but are not related to router operations: you can erase them without impacting the router’s performance.</td>
</tr>
<tr>
<td>File or Directory</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>core files</td>
<td>The bootflash/core directory is the storage area for .core files.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> Do not erase or move the core directory.</td>
</tr>
<tr>
<td>lost+found directory</td>
<td>This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.</td>
</tr>
<tr>
<td>tracelogs files</td>
<td>The storage area for trace files is bootflash/tracelogs.</td>
</tr>
<tr>
<td></td>
<td>Trace files are useful for troubleshooting; you can access trace files using diagnostic mode to gather information related to the IOS XE failure.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> Do not erase or move the tracelog directory.</td>
</tr>
</tbody>
</table>

---

**Upgrading the Router Software**

**Downloading an Image**

Download the image to the bootflash. For information on downloading images see, Loading and Managing System Images Configuration Guide.

**Caution**

Ensure that you have chosen an upgrade image that is supported by your current software version.

**Note**

Before upgrading from Cisco IOS XE 3.13.0S to 3.14.0S, we recommend that you disable the following CLI on router: platform trace runtime slot 0 bay 0 process iomd module all-modules level info

The routers are shipped with the latest software image installed. Follow the instructions in this section if you need to reinstall or upgrade the software image.

Before installing your router software, make sure that you have archived copies of the current Cisco IOS XE release and the Cisco IOS XE release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS XE image and until you have verified that the new Cisco IOS XE image works properly in your network.


You can copy the software image file on the bootflash memory to the appropriate TFTP directory on a host by using the `copy bootflash: tftp: `privileged EXEC command. You can also configure the router as a TFTP server to copy files from one router to another without using an external TFTP server by using the `tftp-server` global configuration command. For more information about the `tftp-server` command, see the “Basic File Transfer Services Commands” section of the Cisco IOS Configuration Fundamentals Command Reference at this URL: [http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html).
This procedure is for copying the combined bin file to the router. You copy the file to the router from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

**SUMMARY STEPS**

1. Locate the software image file:
2. Download the image to a TFTP server and make sure that the server is properly configured.
3. Log into the router through the console port or a Telnet session.
4. If Gigabit Ethernet (GE) port 0 is used as management interface, check the connectivity to TFTP server using the following CLI:
5. Download the image file from the TFTP server to the router by entering this privileged EXEC command:
6. Set the image path in the boot variables and configure the router to autobooot as follows:
7. Verify the boot variables set on the router using the following CLI:
8. Save the configuration and reload the router.

**DETAILED STEPS**

**Step 1** Locate the software image file:

- a) If you are a registered customer, go to this URL and log in: [http://software.cisco.com/download/navigator.html](http://software.cisco.com/download/navigator.html).
- b) Navigate to **Routers > Service Provider Edge Routers**.
- c) Navigate to your router model.
- d) Click IOS XE Software, then select the latest IOS XE release.

**Note** When you select a cryptographic image, you must also accept the terms and conditions of using cryptographic images.

**Step 2** Download the image to a TFTP server and make sure that the server is properly configured.

**Step 3** Log into the router through the console port or a Telnet session.

**Step 4** If Gigabit Ethernet (GE) port 0 is used as management interface, check the connectivity to TFTP server using the following CLI:

```
Router# ping vrf Mgmt-intf tftp-server-address
```

For more information about assigning an IP address and default gateway to the router, refer to the software configuration guide for this release.

**Step 5** Download the image file from the TFTP server to the router by entering this privileged EXEC command:

```
Router# copy tftp://location/directory/filename.bin bootflash:
```

- For //location, specify the IP address of the TFTP server.
- For /directory/image-name.bin, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 192.0.2.1 and to overwrite the image on the router:

```
Router# copy tftp://192.0.2.1/image-name.bin bootflash:
```
The installation process extracts the bin file with all the files and the IOS XE image, and sets the BOOT directory to the created directory in bootflash memory. The process takes approximately 5 to 10 minutes, and at some stages might appear to have stopped.

**Step 6**
Set the image path in the boot variables and configure the router to autoboot as follows:

```
Router# configure terminal
Router(config)# config-register 0x2102 (! 0x2102 sets the router for autoboot)
Router(config)# boot system bootflash:image-name.bin (! sets the image to be loaded in the next reload)
```

**Step 7**
Verify the boot variables set on the router using the following CLI:

```
Router# show bootvar
BOOT variable = bootflash:asr920-universalk9_npe.bin ,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0 (! will be 0x2102 at next reload)
```

**Step 8**
Save the configuration and reload the router.

```
Router# reload
```

After the installation, the router is running the universal image. To install a purchased license with increased capabilities, see *Software Activation Configuration Guide*. To purchase a license, contact Cisco.

### Upgrading the ROMMON on router

The router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

⚠️ **Caution**

To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow the procedure to upgrade the ROMMON image:

#### SUMMARY STEPS

1. Check the router bootup ROMMON region (ROM0 or ROM1). The example, shows the router boots up from ROM0 region.
2. Copy the ROMMON image to the bootflash on the router.
3. Use the upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg R0 command to upgrade the version.
4. Reload the router.
5. Reload the router again to confirm bootup from upgraded ROMMON region ROM1.
6. Repeat Step 3 to Step 5 to update the other region on the RSP (ROM0) region in this procedure.
DETAILED STEPS

Step 1 Check the router bootup ROMMON region (ROM0 or ROM1). The example, shows the router boots up from ROM0 region.

Example:

Router# show rom-monitor r0
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.

Step 2 Copy the ROMMON image to the bootflash on the router.

Example:

Router# copy tftp://location/directory/asr920-rommon-15.4.3r.S4-upgrade.pkg bootflash:

Step 3 Use the upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg R0 command to upgrade the version.

R0 represents router in slot0 of the chassis. Step 3 upgrades the ROMMON region of the router that is not used (ROM1 region) as ROM 0 region is used (in this procedure) in Step 1 to boot up the router.

Step 4 Reload the router.

Example:

Router# upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg r0
Upgrade rom-monitor on Route-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 712184b6ef336f40263222175255f475
Burning upgrade partition...
1966080+0 records in
1966080+0 records out
CChecking upgrade partition...
1966080+0 records in
1966080+0 records out
Upgrade flash partition MD5 signature is 712184b6ef336f40263222175255f475
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.

Step 5 Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

Example:

Router# reload
System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Proceed with reload? [confirm]
24 15:27:03.205 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with reload chassis code
System Bootstrap, Version 12.2(20140211:085836) [pbalakan-sb_romver_16 130], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012 by cisco Systems, Inc.
Compiled Fri 28-Mar-14 18:57 by pbalakan-sb_romver_16
Verifying the Upgrade

Use the show platform command to verify the ROMMON upgrade.

```
Router# show platform
Chassis type: ASR-920-12CZ-A
Slot   Type State Insert time (ago)
------- ------------------- --------------------- -----------------
 0/0    12xGE-2x10GE-FIXED ok 00:18:41
  R0    ASR-920-12CZ-A ok, active 00:20:39
     F0    ok, active 00:20:39
     P0    ASR920-PSU0 ok never
     P1    ASR920-PSU1 ps, fail never
     P2    ASR920-FAN ok never
Slot   CPLD Version Firmware Version
------- ------------------- ---------------------------------------
  R0    14080701 15.4(3r)S4
     F0    14080701 15.4(3r)S4
```

Use the show rom-monitor r0 command to check the rommon version on the router.

```
Router# show rom-monitor r0
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
```

Software Upgrade Example

The following section provide a sample of software upgrade on the router.

```
Router# show bootvar
BOOT variable = bootflash:asr920-universalk9_npe.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0 (will be 0x2102 at next reload)
Router# reload
Proceed with reload? [confirm]
*Nov 14 04:29:15.051: %SYS-5-RELOAD: Reload requested by vmalshet on console. Reload Reason:
  Reload Command.Nov 14 04:29:38.446 R0/0: %PMAN-5-EXITACTION: Process manage
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
Compiled Fri 20-Jun-14 17:24 by alnguyen
```

Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
Boot image size = 266349176 (0xfe02a78) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
    calculated 424f2b4ea7da21d397ef55db10f40e7a6250e8
    expected 424f2b4ea7da21d397ef55db10f40e7a6250e8
Image validated
Passing control to the main image..
%IOSXEBOOT-4-DEBUG_CONF: (rp/0): File /bootflash/debug.conf is absent, ignoring

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version 15.5(20141015:140327) [v155_1_s_xe314_throttle-sourdutt-xe314_cortina 184]
Compiled Tue 28-Oct-14 13:46 by sourdutt
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
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:
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ASR-920-12CZ-A (Freescale P2020) processor (revision 1.0 GHz) with 687183K/6147K bytes
of memory.
Processor board ID CAT1748U1GQ
12 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:
Press RETURN to get started!
Router# show version
Cisco IOS Software, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
Software Upgrade Example

15.5(20141015:140327) [v155_1_s_xe314_throttle-sourdutt-xe314_cortina 184]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 28-Oct-14 13:46 by sourdutt
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON
StrikerI uptime is 21 minutes
Uptime for this control processor is 25 minutes
System returned to ROM by reload
System image file is "bootflash:asr920-universalk9_npe.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:
If you require further assistance please contact us by sending email to
export@cisco.com.
License Level: advancedmetroipaccess
License Type: Smart License
Next reload license Level: advancedmetroipaccess
cisco ASR-920-12CZ-A (Freescale P2020) processor (revision 1.0 GHz) with 687183K/6147K bytes
of memory.
Processor board ID CAT1748U1GQ
12 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
Configuration register is 0x2102
CHAPTER 11

Activating or Deactivating Interface Module

This chapter provides information about activating or deactivating interface module (IM) on the Cisco ASR-920-24SZ-IM and Cisco ASR-920-12SZ-IM Routers. For more information about the commands used in this chapter, see the Cisco IOS XE 3S Command References.

Note
The router does not support swapping of the TDM interface modules to Gigabit Ethernet modules on the Cisco ASR 920 Router and vice-versa. If the TDM interface module is swapped with the Gigabit Ethernet module in the same slot or vice-versa, the router must be reloaded.

Overview, on page 95
Prerequisites for Activating an IM, on page 96
Restrictions for Activating an IM, on page 96
Activating an IM, on page 97
Prerequisites for Deactivating an IM, on page 97
Restrictions for Deactivating an IM, on page 98
Deactivating an IM, on page 98
Sample Configuration and Verification Examples for Activation or Deactivation of IMs, on page 99

Overview

Cisco ASR-920-24SZ-IM Router supports the following IMs in Cisco IOS XE Release 3.14S:

- 8-port 10/100/1000 Ethernet Interface Module (A900-IMA8T)
- 1-port 10GE XFP Interface Module (A900-IMA1X)
- 2-port 10GE SFP+/XFP Interface Module (A900-IMA2Z)
- 8-port RJ48C T1/E1 Interface Module (A900-IMA8D)
- 16-port T1/E1 Interface Module (A900-IMA16D)
- 32-port T1/E1 Interface Module (A900-IMA32D)
- 4-port OC3/STM1 or 1 port OC12/STM4 Interface Module (A900-IMA4OS)
- Combo 8-port 10/100/1000 and 1 port 10GE Interface Module (A900-IMA8T1Z)
Cisco ASR-920-12SZ-IM Router supports the following IMs in Cisco IOS XE Release 3.14S:

- 8-port 10/100/1000 Ethernet Interface Module (A900-IMA8T)
- 8-port SFP Gigabit Ethernet Interface Module (A900-IMA8S)
- 8-port RJ48C T1/E1 Interface Module (A900-IMA8D)
- 16-port T1/E1 Interface Module (A900-IMA16D)
- 32-port T1/E1 Interface Module (A900-IMA32D)
- 1-port 10GE XFP Interface Module (A900-IMA1X)
- 2-port 10GE SFP+/XFP Interface Module (A900-IMA2Z)
- Combo 8-port 10/100/1000 and 1 port 10GE Interface Module (A900-IMA8T1Z)
- Combo 8 SFP GE and 1-port 10GE IM (A900-IMA8S1Z)
- 4-port OC3/STM1 or 1-port OC12/STM4 Interface Module (A900-IMA4OS)

For information on installing and removing the IMs, see the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Router Hardware Installation Guide.

The router does not support swapping of the TDM interface modules to Gigabit Ethernet modules. If the TDM interface module is swapped with the Gigabit Ethernet module in the same slot or vice-versa, the router must be reloaded.

### Prerequisites for Activating an IM

- IM must be installed in the router
- IM must not be in admin down mode
- To activate 8x1G Cu IM or 8xT1/E1 IM, you must give up the following ports on the router front panel:
  - 16 to 23 for Cu IM
  - 20 to 23 for T1/E1 IM
- To activate a TDM IM you must reload the router. Without reloading the router, the IM or associated front panel ports cannot be used. If reload is aborted, the ports 20 to 23 remain disabled and IM remains in Out-of-Service (OOS) state until the next reload.

### Restrictions for Activating an IM

- You cannot activate an IM when activate or deactivate commands are running in the background. The activate process usually completes in two minutes.
- Activating an incorrect IM type results in the IM OOS state.
- `write erase` does not disable activated IM. To disable the IM, you must use the `hw-module subslot` command.
Activating an IM

This section is not applicable to Cisco ASR-920-12SZ-IM Router for TDM IMs.

This section is applicable only to the 8x1G Cu IM or 8xT1/E1 IMs. There is no impact to the front panel ports to bring up or bring down the 1x10G and 2x10G IMs.

Before using the IM, you must activate the IM.

- Verify that the correct IM is inserted in the IM slot.
- Shut down all active interfaces to be removed in IM activation (8x1G Cu IM or 8xT1/E1 IM). See Prerequisites for Activating an IM, on page 96, for active interfaces to be shut down.
- Wait for a minute.
- Default all interfaces to be removed from the router.
- Execute the following command to activate the IM present in the IM slot.

```
hw-module subslot slot-number/subslot-number activate
```

- `slot-number`—Specifies the chassis slot number where the IM is installed.
- `subslot-number`—Specifies the chassis subslot number where IM is installed.

The activate CLI operations run in the background.

The following ports on the router are relinquished when activating 8x1G Cu IM or 8xT1/E1 IM:

- 16 to 23 for Cu IM
- 20 to 23 for T1/E1 IM

Prerequisites for Deactivating an IM

- IM must be installed in the router
- IM must not be in admin down mode
Restrictions for Deactivating an IM

- You cannot deactivate an IM when activate or deactivate commands are running in the background. The deactivation process usually completes in two minutes.
- You cannot use write erase to disable activated IM. To disable the activated IM, you must use CLI.
- Deactivating an IM by specifying an incorrect IM type or without an IM installed in the router can cause hardware or software resource issues. In this case, you must reload the router to reclaim the front panel ports and other ASIC related resources.
- You must reload the router to complete the activate/deactivate process.

**Note**

Activation or deactivation of 8x1G Cu IM does not require a router reload.

- The `hw-module subslot default` command is not supported on TDM and OC-3 interface module.

Deactivating an IM

**Note**

This section is applicable only to the 8-port 1G Cu IM or 8-port T1/E1 IMs. There is no impact to the front panel ports to bring up or bring down the 1-port 10G and 2-port 10G IMs.

Before removing the IM from the router, you must deactivate the IM.

- Verify that the correct IM is in OK state in the router.
- Remove all virtual interfaces (using the `no interface interface-name` command) that are associated with the IM. These interfaces include MPLS TP tunnels, TE tunnels, BDI interface, and Port-Channel interface.
- Shut down all pluggable IM interfaces in the router.
- Wait for a minute.
- Default all pluggable IM interfaces in the router.
- Execute the following command to deactivate the IM present in the IM slot:

  `hw-module subslot slot-number/subslot-number deactivate`

  - `slot-number`—Specifies the chassis slot number where the IM is installed.
  - `subslot-number`—Specifies the chassis subslot number where IM is installed.

**Note**

The deactivate CLI operations run in the background.
The following ports on the router are recovered when deactivating 8-port 1G Cu IM or 8-port T1/E1 IM:
- 16 to 23 for Cu IM
- 20 to 23 for T1/E1 IM

Sample Configuration and Verification Examples for Activation or Deactivation of IMs

The following sections provide sample configuration and verification example for activating or deactivating the following IMs:

Sample Configuration and Verification of Activating an 8-port 1G Cu IM (A900-IMA8T)

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
%Nov 20 09:31:44.532: %LINK-5-CHANGED: Interface GigabitEthernet0/0/19, changed state to administratively down
%Nov 20 09:31:44.536: %LINK-5-CHANGED: Interface GigabitEthernet0/0/20, changed state to administratively down
%Nov 20 09:31:44.541: %LINK-5-CHANGED: Interface GigabitEthernet0/0/21, changed state to administratively down
%Nov 20 09:31:44.542: %LINK-5-CHANGED: Interface GigabitEthernet0/0/22, changed state to administratively down
%Nov 20 09:31:44.547: %LINK-5-CHANGED: Interface GigabitEthernet0/0/23, changed state to administratively down
```

```
Router(config-if-range)# exit
Router(config)# exit
```

The following examples show how to activate an 8-port 1G Cu IM (A900-IMA8T) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module
*Nov 20 09:31:53.361: %SYS-5-CONFIG_I: Configured from console by consolesu
```

```
Router# hw-module subslot 0/1 activate A900-IMA8T
Command will disable & default configs in module 0 (16-23). Proceed ? [confirm]
```

```
Changed ACTIVATED IM: ASR900_IMA8T
```

```
Router# *Nov 20 09:32:11.112: %IOSXE-1-PLATFORM:kernel: Board info b500002
*Nov 20 09:32:11.359: %TRANSCEIVER-6-REMOVED:iomd: Transceiver module removed from GigabitEthernet0/0/23
```

```
*Nov 20 09:32:11.369: %IOSXE_RP_ALARM-6-INFO: ASSERT None GigabitEthernet0/0/23
```

```
*Nov 20 09:32:21.743: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA8T) online in subslot 0/1
```

```
*Nov 20 09:32:23.639: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to down
```

```
*Nov 20 09:32:23.652: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/1, changed state to down
```

```
*Nov 20 09:32:23.692: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/2, changed state to down
```

```
*Nov 20 09:32:23.697: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/3, changed state to down
```

```
*Nov 20 09:32:23.702: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/4, changed state to down
```
Activating or Deactivating Interface Module

Sample Configuration and Verification of Activating an 8-port 1G Cu IM (A900-IMA8T)

Activating or Deactivating Interface Module

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0/0 24xGE-4x10GE-FIXED ok 05:31:32
0/1 A900-IMA8T ok 00:00:39
R0 ASR-920-24SZ-IM ok, active 05:33:14
F0 ok, active 05:33:14
F0 ASR920-PSU0 ok 05:31:56
F1 ASR920-PSU1 N/A never
P2 ASR920-FAN ok 05:31:55
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM down down
GigabitEthernet0/0/1 unassigned YES NVRAM down down
GigabitEthernet0/0/2 unassigned YES NVRAM down down
GigabitEthernet0/0/3 unassigned YES NVRAM down down
GigabitEthernet0/0/4 unassigned YES NVRAM down down
GigabitEthernet0/0/5 unassigned YES NVRAM down down
GigabitEthernet0/0/6 unassigned YES NVRAM down down
GigabitEthernet0/0/7 unassigned YES NVRAM down down
GigabitEthernet0/0/8 unassigned YES NVRAM down down
GigabitEthernet0/0/9 unassigned YES NVRAM down down
GigabitEthernet0/0/10 unassigned YES NVRAM down down
GigabitEthernet0/0/11 unassigned YES NVRAM down down
GigabitEthernet0/0/12 unassigned YES NVRAM down down
GigabitEthernet0/0/13 unassigned YES NVRAM down down
GigabitEthernet0/0/14 unassigned YES NVRAM down down
GigabitEthernet0/0/15 unassigned YES NVRAM down down
Te0/0/24 unassigned YES NVRAM administratively down down
Te0/0/25 unassigned YES NVRAM administratively down down
Te0/0/26 unassigned YES NVRAM administratively down down
Te0/0/27 unassigned YES NVRAM administratively down down
GigabitEthernet0/1/0 unassigned YES unset down down
GigabitEthernet0/1/1 unassigned YES unset down down
GigabitEthernet0/1/2 unassigned YES unset down down
GigabitEthernet0/1/3 unassigned YES unset down down
GigabitEthernet0/1/4 unassigned YES unset down down
GigabitEthernet0/1/5 unassigned YES unset down down
GigabitEthernet0/1/6 unassigned YES unset down down
GigabitEthernet0/1/7 unassigned YES unset down down
GigabitEthernet0 7.23.21.156 YES NVRAM up up
BDI243 unassigned YES NVRAM down down
```

Router#
Sample Configuration and Verification for Deactivating an 8-port 1G Cu IM (A900-IMA8T)

The following example displays system environment information for system components for the Cisco ASR-920-24SZ-IM Router:

```
Router# show environment
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0
Slot Sensor Current State Reading
---- ------ ------------- -------
P0 PEM Iout Normal 7 A
P0 PEM Vout Normal 12 V DC
P0 PEM Vin Normal 230 V AC
P0 Temp: Temp 1 Normal 51 Celsius
P2 Temp: FC FWM Fan Speed 65% 38 Celsius
R0 VADM1: VX1 Normal 997 mV
R0 VADM1: VX2 Normal 1046 mV
R0 VADM1: VX3 Normal 997 mV
R0 VADM1: VP1 Normal 3283 mV
R0 VADM1: VP2 Normal 1796 mV
R0 VADM1: VP3 Normal 1197 mV
R0 VADM1: VP4 Normal 1768 mV
R0 VADM1: VH Normal 12317 mV
R0 VADM1: AUX1 Normal 3840 mV
R0 VADM1: AUX2 Normal 6958 mV
R0 Temp: CYLON Normal 60 Celsius
R0 Temp: FPGA Normal 49 Celsius
R0 Temp: Outlet Normal 47 Celsius
R0 VADM2: VX1 Normal 995 mV
R0 VADM2: VX2 Normal 973 mV
R0 VADM2: VX3 Normal 754 mV
R0 VADM2: VP1 Normal 2495 mV
R0 VADM2: VP2 Normal 1495 mV
R0 VADM2: VP3 Normal 1497 mV
R0 VADM2: VH Normal 12296 mV
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0/0 24xGE-4x10GE-FIXED ok 05:37:55
0/1 A900-IMA8T ok 00:07:02
R0 ASR-920-24SZ-IM ok, active 05:39:37
F0 ok, active 05:39:37
P0 ASR920-PSU0 ok 05:38:19
P1 ASR920-PSU1 N/A never
P2 ASR920-FAN ok 05:38:18
Slot CPLD Version Firmware Version
--------- ------------------- ---------------------------------------
R0 01491802 15.4(3r)34
F0 01491802 15.4(3r)34
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
--------- ----------- ------ ------ -------
```

Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
The following example shows how to deactivate 8x1G Cu IM (A900-IMA8T) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 deactivate
Command will default configs in module 1. Proceed ? [confirm]
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot    Type         State           Insert time (ago)
-------- --------------------------------------------------
 0/0     24xGE-4x10GE-FIXED   ok             05:40:54
 0/1     A900-IMA8T         stopped        00:01:55
 0       ASR-920-24SZ-IM   ok, active     05:42:36
 0       ok, active         05:42:36
 0       ok, active         05:41:19
 0       ASR920-PSU0        ok             05:41:18
 0       ASR920-PSU1        N/A           never
 0       ASR920-FAN         ok             05:41:18
 0       CPLD Version      Firmware Version
```

Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface       IP-Address OK? Method Status    Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM down     down
GigabitEthernet0/0/1 unassigned YES NVRAM down     down
GigabitEthernet0/0/2 unassigned YES NVRAM down     down
GigabitEthernet0/0/3 unassigned YES NVRAM down     down
GigabitEthernet0/0/4 unassigned YES NVRAM down     down
GigabitEthernet0/0/5 unassigned YES NVRAM down     down
GigabitEthernet0/0/6 unassigned YES NVRAM down     down
GigabitEthernet0/0/7 unassigned YES NVRAM down     down
GigabitEthernet0/0/8 unassigned YES NVRAM down     down
GigabitEthernet0/0/9 unassigned YES NVRAM down     down
GigabitEthernet0/0/10 unassigned YES NVRAM down    down
GigabitEthernet0/0/11 unassigned YES NVRAM down    down
GigabitEthernet0/0/12 unassigned YES NVRAM down    down
GigabitEthernet0/0/13 unassigned YES NVRAM down    down
GigabitEthernet0/0/14 unassigned YES NVRAM down    down
GigabitEthernet0/0/15 unassigned YES NVRAM down    down
GigabitEthernet0/0/16 unassigned YES NVRAM down    down
GigabitEthernet0/0/17 unassigned YES NVRAM down    down
GigabitEthernet0/0/18 unassigned YES NVRAM down    down
GigabitEthernet0/0/19 unassigned YES NVRAM down    down
GigabitEthernet0/0/20 unassigned YES NVRAM down    down
GigabitEthernet0/0/21 unassigned YES NVRAM down    down
GigabitEthernet0/0/22 unassigned YES NVRAM down    down
GigabitEthernet0/0/23 unassigned YES NVRAM down    down
Te0/0/24        unassigned    YES NVRAM administratively down administratively down down
Te0/0/25        unassigned    YES NVRAM administratively down administratively down down
Te0/0/26        unassigned    YES NVRAM administratively down administratively down down
Te0/0/27        unassigned    YES NVRAM administratively down administratively down down
GigabitEthernet0 7.23.21.156 YES NVRAM up     up
BDI243          unassigned    YES NVRAM down     down
```

Sample Configuration and Verification of Activating 8-port T1/E1 IM (A900-IMA8D)

The following example shows how to activate 8-port T1/E1 IM (A900-IMA8D) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 activate A900-IMA8D
Command will disable & default configs in module 0 (20-23). Proceed ? [confirm]
System reload is required for act/deact of TDM IMs. Proceed with reload ?[confirm]

Changed ACTIVATED IM: ASR900_IMA16D

*Nov 20 09:47:08.155: %TRANSCEIVER-6-REMOVED:iomd: Transceiver module removed from GigabitEthernet0/0/23
*Nov 20 09:47:08.875: %IOSXE_RP_ALARM-6-INFO: ASSERT None GigabitEthernet0/0/23 [OK]
Proceed with reload? [confirm]

Nov 20 09:47:56.304 R0/0:
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2014 by cisco Systems, Inc.
```
Compiled Fri 20-Jun-14 17:24 by alnguyen

PEX up stream Vendor ID [0x860610b5]
PEX down stream vendor ID [0x860610b5]
Boot ROM
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located asr920.bin
Image size 266457720 inode num 23, bks cnt 65054 blk size 8*512

Boot image size = 266457720 (0xfe1d278) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
expected 872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
Image validated
Passing control to the main image..

Restricted Rights Legend

Use, duplication, or disclosure by the Government is<
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
15.5(20141114:175558) [v155_1_s_xe314_throttle-hargurra-psu 104
Copyright (c) 1986-2014 by Cisco Systems, Inc.

Compiled Sat 15-Nov-14 00:09 by hargurra

Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License (&quot;GPL&quot;) Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or &quot;License Notice&quot; file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
Changed ACTIVATED IM: ASR900 IMA16D

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 ASR-920-24SZ-IM (Freescale P2020) processor (revision 1.2 GHz) with 687112K/6147K bytes of memory. Processor board ID CAT1707V01N
20 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:

Press RETURN to get started!

Authentication passed

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface    IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0  unassigned YES NVRAM down down
GigabitEthernet0/0/1  unassigned YES NVRAM down down
GigabitEthernet0/0/2  unassigned YES NVRAM down down
GigabitEthernet0/0/3  unassigned YES NVRAM down down
GigabitEthernet0/0/4  unassigned YES NVRAM down down
GigabitEthernet0/0/5  unassigned YES NVRAM down down
GigabitEthernet0/0/6  unassigned YES NVRAM down down
GigabitEthernet0/0/7  unassigned YES NVRAM down down
GigabitEthernet0/0/8  unassigned YES NVRAM down down
GigabitEthernet0/0/9  unassigned YES NVRAM down down
GigabitEthernet0/0/10 unassigned YES NVRAM down down
GigabitEthernet0/0/11 unassigned YES NVRAM down down
GigabitEthernet0/0/12 unassigned YES NVRAM down down
GigabitEthernet0/0/13 unassigned YES NVRAM down down
GigabitEthernet0/0/14 unassigned YES NVRAM down down
GigabitEthernet0/0/15 unassigned YES NVRAM down down
GigabitEthernet0/0/16 unassigned YES NVRAM down down
GigabitEthernet0/0/17 unassigned YES NVRAM down down
GigabitEthernet0/0/18 unassigned YES NVRAM down down
GigabitEthernet0/0/19 unassigned YES NVRAM down down
Te0/0/24         unassigned YES NVRAM administratively down down
Te0/0/25         unassigned YES NVRAM administratively down down
Te0/0/26         unassigned YES NVRAM administratively down down
Te0/0/27         unassigned YES NVRAM administratively down down
GigabitEthernet0 7.23.21.156 YES NVRAM up up
BDI243          unassigned YES NVRAM down down
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM

Slot  Type        State            Insert time (ago)
```
Sample Configuration and Verification of Deactivating 8-port T1/E1 IM (A900-IMA8D)

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```bash
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot Type State Insert time (ago)
--------- ------------------- --------------------- ----------------- 
0/0 24xGE-4x10GE-FIXED ok 00:15:26
0/1 A900-IMA8D ok 00:15:26
R0 ASR-920-24SZ-IM ok, active 00:17:14
F0 ok, active 00:17:14
P0 ASR920-PSU0 ok 00:15:52
P1 ASR920-PSUI N/A never
P2 ASR920-FAN ok 00:15:51
Slot CPLD Version Firmware Version
--------- ------------------- --------------------------------------- 
R0 01491802 15.4(3r)S4
F0 01491802 15.4(3r)S4
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```bash
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM down down
GigabitEthernet0/0/1 unassigned YES NVRAM down down
GigabitEthernet0/0/2 unassigned YES NVRAM down down
GigabitEthernet0/0/3 unassigned YES NVRAM down down
GigabitEthernet0/0/4 unassigned YES NVRAM down down
GigabitEthernet0/0/5 unassigned YES NVRAM down down
GigabitEthernet0/0/6 unassigned YES NVRAM down down
GigabitEthernet0/0/7 unassigned YES NVRAM down down
GigabitEthernet0/0/8 unassigned YES NVRAM down down
GigabitEthernet0/0/9 unassigned YES NVRAM down down
GigabitEthernet0/0/10 unassigned YES NVRAM down down
GigabitEthernet0/0/11 unassigned YES NVRAM down down
GigabitEthernet0/0/12 unassigned YES NVRAM down down
GigabitEthernet0/0/13 unassigned YES NVRAM down down
GigabitEthernet0/0/14 unassigned YES NVRAM down down
GigabitEthernet0/0/15 unassigned YES NVRAM down down
Te0/0/24 unassigned YES NVRAM administratively down down
Te0/0/25 unassigned YES NVRAM administratively down down
Te0/0/26 unassigned YES NVRAM administratively down down
Te0/0/27 unassigned YES NVRAM administratively down down
```
The following example shows how to deactivate 8-port T1/E1 IM (A900-IMA8D) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 deactivate

Command will default configs in module 1. Proceed ? [confirm]
System reload is required for act/deact of TDM IMs. Proceed with reload ?[confirm]
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED[OK]
Proceed with reload? [confirm]
Command
Nov 20 10:17:49.956 R0/0: %PMAN-5-EXITACTION: Process manager System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
```

Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
Compiled Fri 20-Jun-14 17:24 by alnguyen
PEX up stream Vendor ID [0x860610b5]
PEX down stream vendor ID [0x860610b5]
Boot ROM1
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located asr920.bin
Image size 266457720 inode num 23, bks cnt 65054 blk size 8*512

```
############################################################
Boot image size = 266457720 (0xfe1d278) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 872ac9f3:08808feb:9690e7e4:d68c5d0:18191823
expected 872ac9f3:08808feb:9690e7e4:d68c5d0:18191823
Image validated
Passing control to the main image..
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (i) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version 15.5(20141114:175558) [v155_1_a_xe314_throttle-hargurra-psu 104]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Sat 15-Nov-14 00:09 by hargurra
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED

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:

If you require further assistance please contact us by sending email to export@cisco.com.
cisco ASR-920-24SZ-IM (Freescale P2020) processor (revision 1.2 GHz) with 687112K/6147K bytes of memory.

Processor board ID CAT1707V01N
24 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash.
SETUP: new interface GigabitEthernet0/0/20 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/21 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/22 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/23 placed in "shutdown" state
Press RETURN to get started!

Authentication passed
*Nov 20 10:23:14.107: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM[OK]
*Nov 20 10:23:29.665: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent for Licensing.
*Nov 20 10:23:29.666: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco licensing cloud restored
*Nov 20 10:24:14.037: %SPA_OIR-6-ONLINECARD: SPA (24xGE-4x10GE-FIXED) online in subslot 0/0

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0/0 24xGE-4x10GE-FIXED ok 05:40:54
0/1 A900-IMA8T stopped 00:01:55
R0 ASR-920-24SZ-IM ok, active 05:42:36
P0 ok, active 05:42:36
P0 ASR920-PSU0 ok 05:41:19
P1 ASR920-PSU1 N/A never
P2 ASR920-FAN ok 05:41:18
Slot CPLD Version Firmware Version
--------- ------------------- ---------------------------------------
R0 01491802 15.4(3r)S4
```

Activating or Deactivating Interface Module
The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

Router# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/2</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/3</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/4</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/5</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/6</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/7</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/8</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/9</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/10</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/11</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/12</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/13</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/14</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/15</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/16</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/17</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/18</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/19</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/20</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/21</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/22</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0/23</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
<tr>
<td>Te0/0/24</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Te0/0/25</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Te0/0/26</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Te0/0/27</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0</td>
<td>7.23.21.156</td>
<td>YES</td>
<td>NVRAM up</td>
<td>up</td>
</tr>
<tr>
<td>BDI243</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM down</td>
<td>down</td>
</tr>
</tbody>
</table>
Sample Configuration and Verification of Deactivating 8-port T1/E1 IM (A900-IMA8D)
CHAPTER 12

Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface on the Cisco ASR 920 Series Router.

For more information about the commands used in this chapter, see the Cisco IOS XE 3S Command References.

Effective Cisco IOS-XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router was added to the Cisco ASR 920 Series Routers family.

Note
On the Cisco ASR-920-12SZ-IM Aggregation Services Router, ports from 12 through 15 can operate at either 1G or 10G, and operates in a mutually exclusive way. You cannot insert both 1G and 10G together. If you insert IG IMs (A900-IMA8T1Z, A900-IMA8S1Z, A900-IMA8T, A900-IMA8S), the dual rate port supports only 10G.

- Configuring an Interface, on page 111
- Specifying the Interface Address on an Interface, on page 113
- Modifying the Interface MTU Size, on page 113
- Configuring the Encapsulation Type, on page 115
- Configuring Autonegotiation on an Interface, on page 115
- Configuring Carrier Ethernet Features, on page 116
- Saving the Configuration, on page 116
- Shutting Down and Restarting an Interface, on page 117
- Verifying the Interface Configuration, on page 117
- Verifying Interface Status, on page 118
- Configuring LAN/WAN-PHY Controllers, on page 120
- Configuration Examples, on page 122

Configuring an Interface

This section lists the required configuration steps to configure Gigabit and Ten Gigabit Ethernet interfaces. Follow these steps to configure your interface:

Step 1  Router# configure terminal
Enters global configuration mode.

Step 2  Do one of the following:

- Router(config)# interface gigabitethernet slot/port
- Router(config)# interface tengigabitethernet slot/port

Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:

- slot/port — The location of the interface. See Specifying the Interface Address on an Interface, on page 113.

Note  The slot number is always 0.

Step 3  no negotiation auto

Example:

Router(config-if)# no negotiation auto

(Optional) Disables automatic negotiation.

Note  Use the speed command only when the mode is set to no negotiation auto.

Step 4  speed {10 | 100 | 1000}

Example:

Router(config-if)# speed 1000

(Optional) Specifies the speed for an interface to transmit at 10, 100, and 1000 Mbps (1 Gbps), where the default is 1000 Mbps.

Step 5  Router(config-if)# carrier-delay down msec value

(Optional) Sets the router to signal within the specified time delay, when an interface goes down, where:

- down — Time delay for signalling when the interface goes down.

Step 6  Router(config-if)# carrier-delay up msec value

(Optional) Sets the router to signal within the specified time delay, when an interface should be up again, where:

- up — Time delay before an interface should be up again.

You must wait for at least 2 msec before bring the interface up again, this is to protect against link flaps.

Step 7  Router(config-if)# ip address ip-address mask {secondary} | dhcp {client-id interface-name} {hostname host-name}]

Sets a primary or secondary IP address for an interface that is using IPv4, where:

- ip-address — The IP address for the interface.
- mask — 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 interface-name — Specifies the client identifier. The interface-name sets the client identifier to the hexadecimal MAC address of the named interface.
- hostname host-name — Specifies the hostname for the DHCP purposes. The host-name is the name of the host to be placed in the DHCP option 12 field.
Step 8  Router(config-if)# mtu bytes

(As Required) Specifies the maximum packet size for an interface, where:

• bytes—The maximum number of bytes for a packet.

The default is 1500 bytes; the range is from 1500 to 9216.

Step 9  Router(config-if)# no shutdown

Enables the interface.

---

Specifying the Interface Address on an Interface

To configure or monitor Ethernet interfaces, you need to specify the physical location of the interface in the CLI. The interface address format is slot/port, where:

• slot—The chassis slot number in the router of the interface.

Note

The interface slot number is always 0.

• subslot—The subslot of the interface. Interface subslots are always 0.

• port—The number of the individual interface port on an interface.

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

Modifying the Interface MTU Size

Note

The router supports only eight unique MTUs.

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

• Interface MTU—The interface checks the MTU value of incoming traffic. 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 specified on an interface. If an IP packet exceeds the IP MTU size, then the packet is fragmented.
• Tag or Multiprotocol Label Switching (MPLS) MTU—Can be specified on an interface and allows up to six different tag headers to be attached to a packet. The maximum number of tag headers (also referred to as labels) depends on your Cisco IOS software release.

**Note**

If the MTU interface configuration exceeds the maximum number of supported bytes, then the input errors are incremented. For packets with maximum size, the counter does not support increment by using CLI as the ASIC is unable to handle it. This is applicable on Cisco ASR 920-10SZ-PD (OD), ASR-920-8S4Z-PD, ASR-920-12SZ-IM, ASR-920U-12SZ-IM, ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M routers.

Encapsulation methods and 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 4-byte header, and each MPLS label adds a 4-byte header (n labels x 4 bytes).

For the Gigabit Ethernet interface on the router, the default MTU size is 1500 bytes. The maximum configurable MTU is 9216 bytes. The interface automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.

**Limitation**

The giants and input errors field counts are not incremented for both 1G and 10G ports on Cisco ASR 920 platforms.

### Interface MTU Configuration Guidelines

When configuring the interface MTU size, 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Router(config-if)# mtu bytes` | Configures the maximum packet size for an interface, where:
  - `bytes`— 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 that is shown in the “MTU” field.

The following example shows an MTU size of 1500 bytes for interface port 0 (the first port) on the Gigabit Ethernet interface in slot 0 of the router:

```
Router# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is down, line protocol is down
Hardware is 8xGE-4x10GE-FIXED, address is 6073.5cff.8080 (bia 6073.5cff.8080)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
```

**Configuring the Encapsulation Type**

The encapsulation supported by the interfaces is IEEE 802.1Q and IEEE 802.1ad encapsulation for virtual LANs (VLANs).

---

**Note**

VLANs are only supported on Ethernet Virtual Connection (EVC) service instances and Trunk Ethernet Flow Point (EFP) interfaces. For more information about how to configure these features, see the *Configuring Ethernet Virtual Connections* document.

---

**Configuring Autonegotiation on an Interface**

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 router, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

When enabling autonegotiation, consider these guidelines:

- 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.
- Flow control is enabled by default.
- Flow control will be on if autoneegotiation is disabled on both ends of the link.
Enabling Autonegotiation

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# negotiation auto</td>
<td>Enables autonegotiation on a Gigabit Ethernet interface. Advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

Disabling Autonegotiation

Autonegotiation is automatically enabled and can be disabled on Gigabit Ethernet interfaces. During autonegotiation, advertisement for flow control, speed, and duplex occurs, depending on the media (fiber or copper) in use.

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# no negotiation auto</td>
<td>Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs.</td>
</tr>
</tbody>
</table>

Configuring Carrier Ethernet Features

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S.

Saving the Configuration

To save your running configuration to NVRAM, use the following command in privileged EXEC configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# copy running-config startup-config</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>

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

You can shut down and restart any of the interface ports on an interface 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) of Gigabit Ethernet interfaces; you can remove them at any time.

If you are preparing for an OIR, it is not necessary to independently shut down each of the interfaces prior to deactivation of the module.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# shutdown</td>
<td>Restarts, stops, or starts an interface.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# shutdown</td>
<td>Disables an interface.</td>
</tr>
</tbody>
</table>

To enable traffic on an interface, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# no shutdown</td>
<td>Restarts a disabled interface.</td>
</tr>
</tbody>
</table>

Verifying the Interface Configuration

Besides using the `show running-configuration` command to display your router configuration settings, you can use the `show interfaces gigabitethernet` command to get detailed information on a per-port basis for your Gigabit Ethernet interface.

Verifying Per-Port Interface Status

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

The following example provides sample output for interface port 0 on the interface located in slot 1 of the router:

```
Router# show interface gigabitEthernet 0/0/7
GigabitEthernet0/0/7 is up, line protocol is up
Hardware is 8xGE-4x10GE-FIXED, address is 6073.5cff.8087 (bia 6073.5cff.8087)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 1000Mbps, link type is auto, media type is RJ45
```
output flow-control is off, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0 (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 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
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

## Verifying Interface Status

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

### Note

The `show interface transceiver` command is not supported on the router.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router# **show hw-module slot/subslot transceiver port idprom** | Displays information for the transceiver identification programmable read only memory (idprom).  
**Note** Transceiver types must match for a connection between two interfaces to become active. |
| Router# **show hw-module slot/subslot transceiver port idprom status** | Displays information for the transceiver initialization status.  
**Note** The transmit and receive optical power that is displayed by this command is useful for troubleshooting Digital Optical Monitoring (DOM). For interfaces to become active, optical power must be within required thresholds. |
| Router# **show hw-module slot/subslot transceiver port idprom dump** | Displays a dump of all EEPROM content that is stored in the transceiver. |

Following are sample output of several `show` commands for SFP Modules and SFP+ Modules.
The following show hw-module subslot command sample output is for SFP-GE-S:

Router# show hw-module subslot 0/0 transceiver 9 idprom
IDPROM for transceiver GigabitEthernet0/0/0:Description = SFP optics (type 3) Transceiver Type: = GE SX (19) Product Indentifier (PID) = FTRJ851P1BNL-C6Vendor Revision = ASerial Number (SN) = FNS1037R8DHVendor Name = CISCO-FINISARVendor OUI (IEEE company ID) = 00.90.65 (36965)CLEI code = IPUIALJRAACisco part number = 10-2143-01Device State = Enabled.Date code (yy/mm/dd) = 06/09/14Connector type = LC.Encoding = 8B10BNRZNominal bitrate = GE (1300 Mbits/s) Minimum bit rate as % of nominal bit rate = not specifiedMaximum 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 0/0 transceiver 2 idpromIDPROM for transceiver GigabitEthernet0/0/2:Description = SFP optics (type 3) Transceiver Type: = GE CWDM 1490 (28) Product Indentifier (PID) = FWDM-16217D49CSCVendor Revision = CSerial Number (SN) = FNS10500HA9Vendor Name = CISCO-FINISARVendor OUI (IEEE company ID) = 00.90.65 (36965)CLEI code = CNTRVX0FACisco part number = 10-1884-01Device State = Enabled.Date code (yy/mm/dd) = 06/12/12Connector type = LC.Encoding = 8B10BNRZNominal bitrate = (2700 Mbits/s) Minimum bit rate as % of nominal bit rate = not specifiedMaximum bit rate as % of nominal bit rate = not specified

The following show hw-module subslot command sample output is for an SFP+ module:

Router# show hw-module subslot 2/2 transceiver 9 idprom brief
IDPROM for transceiver TenGigabitEthernet0/0/9:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = SFP+ 10GBASE-SR (273)
Product Indentifier (PID) = SFP-10G-SR
Vendor Revision = 1
Serial Number (SN) = JUS1803G2FT
Vendor Name = CISCO-JDSU
Vendor OUI (IEEE company ID) = 00.01.9C (412)
CLEI code = COUIA8NCAA
Cisco part number = 10-2415-03
Device State = Enabled.
Date code (yy/mm/dd) = 14/01/18
Connector type = LC.
Encoding = 4b5b
NRZ
Manchester
Nominal bitrate = (10300 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 SFP+ module:

Router# show hw-module subslot 0/3 transceiver 9 status
The Transceiver in slot 0 subslot 0 port 9 is enabled.
Module temperature = +24.773 C
Transceiver Tx supply voltage = 3291.3 mVolts
Transceiver Tx bias current = 6024 uAmps
Transceiver Tx power = -2.3 dBm
Transceiver Rx optical power = -2.9 dBm

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

Router# show hw-module subslot 0/0 transceiver 9 idprom dump
IDPROM for transceiver GigabitEthernet0/0/0:Description = SFP optics (type 3) Transceiver
Configuring LAN/WAN-PHY Controllers

The LAN/WAN-PHY controllers are configured in the physical layer control element of the Cisco IOS XE software. Use the `hw-module subslot slot/subslot enable lan` command to configure the LAN-PHY mode.

WAN-PHY Mode is not currently supported on the Cisco ASR 920 Series Router.

Configuring the LAN-PHY Mode

This section describes how to configure the LAN-PHY mode on the Gigabit Ethernet interfaces.

Step 1  
`show controllers wanphy 0/0/1`

Example:

```
Router# show controllers wanphy 0/0/1
TenGigabitEthernet0/0/1
Mode of Operation: WAN Mode
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
WIS ALARMS
SER = 0 FELCDP = 0 FEAISP = 0
WLOS = 0 FLCD = 0
LFEBIP = 0 PBEC = 0
```
Active Alarms [All defects]: SWLOF LAIS PAIS SER
Active Alarms [Highest Alarms]: SWLOF
Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS

Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
S1SO = 00, C2 = 0x1A
PATH TRACE BUFFER: UNSTABLE
Remote J1 Byte :

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

Displays the configuration mode of the LAN/WAN-PHY controller. By default, prior to configuration of the LAN-PHY mode, the controller operates in the WAN-PHY mode.

Step 2 configure terminal

Example:

Router# configure terminal
Enters the global configuration mode.

Step 3 hw-module subslot slot/subslot enable LAN

Example:

Router(config)# hw-module subslot 0/1 enable LAN
Configures the LAN PHY mode for the 1-Port 10-Gigabit Ethernet LAN/WAN PHY SPA.

Step 4 exit

Example:

Router(config)# exit
Exits global-configuration (config) mode and enters privilege-exec mode.

Step 5 show controllers wanphy 0/0/1

Example:

Router# show controllers wanphy 0/0/1
TenGigabitEthernet0/0/1
Mode of Operation: LAN Mode

Displays the configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as LAN mode for the 1-Port 10-Gigabit Ethernet LAN/WAN PHY SPA.

---

**Configuring WAN-PHY Signal Failure and Signal Degrade Bit Error Rates**

**Note**

WAN-PHY Mode is not supported on the Cisco ASR 920 Series Router.
This section describes how to configure WAN-PHY Signal Failure (SF) and Signal Degrade (SD) Bit Error Rate (BER) reporting and thresholds.

A Signal Failure (SF) alarm is declared if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9).

A Signal Degrade (SD) alarm is declared if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9). If the B2 errors cross the SD threshold, a warning of link quality degradation is triggered. The WAN-PHY alarms are required for some users who are upgrading their Layer 2 core network from a SONET ring to a 10-Gigabit Ethernet ring.

**Note**
The controller must be in the WAN-PHY mode prior to configuring the SF and SD BER reporting and thresholds.

### Configuration Examples

This section includes the following configuration examples:

#### Basic Interface Configuration

The following example shows how to enter the global configuration mode to specify the interface that you want to configure, configure an IP address for the interface, and save the configuration.

```sql
! 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
```

#### MTU Configuration

The following example shows how to set the MTU interface to 9216 bytes.
The interface automatically adds an additional 38 bytes to the configured MTU interface 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 Encapsulation**

The following example shows how to configure the interface port 2 (the third port), and configure the first interface on the VLAN with the 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.
Router(config)# interface gigabitEthernet 0/0/5
!
! Specify the interface address
!
Router(config-if)# service instance 10 ethernet
!
! Configure dot1q encapsulation and specify the VLAN ID.
!
Router(config-if-srv)# encapsulation dot1q 268
```

VLANs are only supported on EVC service instances and Trunk EFP interfaces. For more information about how to configure these features, see the see the Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S.
Configuring Serial Interfaces

This chapter configures the serial interface module (PN: A900-IMASER14A/S) Async/Sync R232 serial data using Transparent Pseudowire (PW) over MPLS network and raw socket. It includes the following sections:

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.

• Information About Serial Interface Module, on page 125
• Restrictions, on page 126
• How to Configure Serial Interface, on page 127
• Verifying the Serial Interface Configuration, on page 137
• Configuration Examples, on page 139

Information About Serial Interface Module

The serial interface module supports pseudowire transport over MPLS and raw socket for Async and Sync traffic. The Serial IM interfaces monitor and detect cable connections, cable types and also monitors modem control signals periodically.
The A900-IMASER14A/S interface provides a direct connection between the Cisco ASR 920 router and external networks.

**Note**

We recommend that you use a smart serial or 4-port octopus cable to connect the A900-IMASER14A/S with the external network.

Out of 14 ports, 6 ports support sync interfaces and 8 ports support async interfaces. RS232 Async data is carried over Raw Socket and Transparent byte mode and RS232 Sync data is carried over Raw Socket.

## Restrictions

This section describes the port restrictions for Serial interface module:

- Ports 0-7 are Async ports on the 68-pin connector
- Ports 8-13 are Sync or Async on the 12-in-1 connector

**Note**

Sync is *not* supported in Cisco IOS XE Release 3.14S. Sync ports cannot be configured in Cisco IOS XE Release 3.14S.

- Maximum speed on all ports is 236Kbps.

This section describes the software limitations that apply when configuring the Serial interface module:
• The router can only be configured as data circuit-terminating equipment (DCE).
• Configuration of pseudowire between local and remote PE with different speed on Sync and Async ports is not supported.
• Sub-rate (below DS0 bandwidth) Async (R232) data over MPLS using T1/E1 CESoP is not supported.
• Pseudowire ping is not supported for the pseudowire configured on the serial interface module.
• Only two serial interface modules can come up on the router in release prior to Cisco IOS XE Release 3.14. Starting with Cisco IOS XE Release 3.14, all 6 bays on the router are available for insertion of interface modules simultaneously.
• Only Trans encapsulation is supported in Cisco IOS XE Release 3.14S.
• If you installed a new A900-IMASER14A/S or if you want to change the configuration of an existing interface, you must enter configuration mode to configure the new interfaces. If you replaced an A900-IMASER14A/S that was previously configured, the system recognizes the new interfaces and brings each of them up in their existing configuration.
• Pseudowire ping is not supported for cross-connect configured on A900-IMA14A/S interface module.
• A maximum speed of 64 kbps between PE and DTE is supported for RS232 Sync ports.
• PE can act only as DCE and provides the clock to DTE.
• Serial IM Sync signaling transport does not interoperable with the third party equipments. HLDC frames used for transport of these signals are Cisco-specific.

How to Configure Serial Interface

Required Configuration Tasks

Configuring the Controller

To create the interfaces for the Serial interface module, complete these steps:

SUMMARY STEPS

1. configure terminal
2. controller serial slot/subslot/port
3. physical-layer async | sync
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Selects the controller to configure and enters controller configuration mode.</td>
</tr>
</tbody>
</table>

**Step 2**

**controller serial slot/subslot/port**

*Example:*

```
Router(config)# controller serial 0/4/1
```

Selects the location of the interface.

**Note** The slot number is always 0.

**Step 3**

**physical-layer async | sync**

*Example:*

```
Router(config-controller)# physical-layer async
```

Configures the serial interface in async or sync mode.

- async—Specifies async interface.
- sync— Specifies sync interface. This is the default mode.

**Step 4**

**exit**

*Example:*

```
Router(config)# exit
```

Exits configuration mode and returns to the EXEC command interpreter prompt.

### Optional Configurations

**Configuring Layer 1 on Sync and Async Interface Server**

The RS232 which is enabled by default on the async interface, supports RS232 DCE cable with the DB-25 connector. The Cisco smart serial cable with the DB-25 connector supports RS232 and RS485. The RJ45 cable type supports only RS485.

**SUMMARY STEPS**

1. configure terminal
2. line slot/bay/port
3. databits \{5 | 6 | 7 | 8\}
4. stopbits \{1 | 1.5 | 2\}
5. speed speed-value
6. raw-socket tcp server port server ip address
7. raw-socket packet length packet length
8. flowcontrol \{none | software \{lock \| in \| out\} \| hardware \{in \| out\} \}

---

*Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x*
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> line slot/bay/port</td>
<td>Select the controller to configure and enters serial interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# <strong>line</strong> 0/4/1</td>
<td>• slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> databits {5</td>
<td>6</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# <strong>databits</strong> 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> stopbits {1</td>
<td>1.5</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# <strong>stopbits</strong> 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> speed speed-value</td>
<td>Specifies the serial interface speed. The valid range is from 300 to 230400. The default is 9600.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# <strong>speed</strong> 9600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> raw-socket tcp server port server ip address</td>
<td>Specifies raw-tcp server configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# <strong>raw-socket tcp server</strong> 5000 1.1.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> raw-socket packet length packet length</td>
<td>Specifies raw-tcp packet length configuration options.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# <strong>raw-socket packet-length</strong> 32</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 8    | `flowcontrol /none | Sets the flowcontrol.  
|      | software [lock | - none  
|      | in | out] | - software  
|      | hardware [in | out] | - hardware  
|      | Example: Router(config-line)# flowcontrol none |
| 9    | `parity {even | mark | none | odd | space} | Sets the parity.  
|      | Example: Router(config-line)# parity none |
| 10   | `sig-transport u-frame pattern pattern` | This step is specific to Sync mode only. Specifies the u-frame format used for internal signal transport.  
|      | Example: Router(config-line)#sig-transport u-frame pattern NR0 |
| 11   | `control-sig-transport [on | off] frequency frequency range` | Specifies if hardware control signals need to be sent to remote PE or not. Also specifies the frequency (period between successive control frames) in milliseconds. By default, control signal is OFF. Frequency needs to be configured only if the control signal is ON.  
|      | Example: Router(config-line)#control-sig-transport on frequency \(50\text{-}65535\) |
| 12   | `connection-topology [point-to-point | point-to-multipoint]` | This step is specific to Sync mode only. Specifies the type of topology.  
|      | Example: Router(config-line)#connection-topology point-to-multipoint |
| 13   | `dtr [used | not-used]` | (Optional) DTR is programmable when DTR pin in FPGA is not connected. By default, DTR is set as used.  
|      | Example: Router(config-line)# dtr not-used |
| 14   | `connection-timeout timeout` | (Optional) Specifies the connection timeout of the master and slave session. It should be configured 4 times higher than the frequency.  
|      | Example: Router(config-line)# connection-timeout \(<800\text{-}65535\) |
| 15   | `exit` | Exits configuration mode and returns to the EXEC command interpreter prompt.  
|      | Example: Router(config-line)# exit |

Example: Async Layer 1 Parameters

```
Router# configure terminal  
Router(config)# line 0/4/1
```
Configuring Layer 1 on Sync and Async Interface Client

**SUMMARY STEPS**

1. **configure terminal**
2. **line slot/bay/port**
3. **databits {5 | 6 | 7 | 8}**
4. **stopbits {1 | 1.5 | 2}**
5. **speed speed-value**
6. **raw-socket tcp client server ip address server port client ip address client port**
7. **raw-socket packet length packet length**
8. **flow-control /none | software [lock | in | out] | hardware [in | out]**
9. **parity {even | mark | none | odd | space}**
10. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select the controller to configure and enters serial interface configuration mode.</td>
</tr>
<tr>
<td>line slot/bay/port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# line 0/4/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the databit configuration. The default is 8.</td>
</tr>
<tr>
<td>databits {5</td>
<td>6</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# databits 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the stopbit configuration. The default is 2.</td>
</tr>
<tr>
<td>stopbits {1</td>
<td>1.5</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-line)# stopbits 2</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Serial Interfaces

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> speed speed-value</td>
<td>Specifies the serial interface speed. The valid range is from 300 to 230400. The default is 9600.</td>
</tr>
<tr>
<td>Example: Router(config-line)# speed 9600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> raw-socket tcp client server ip address server port client ip address client port</td>
<td>Specifies raw-tcp client configuration.</td>
</tr>
<tr>
<td>Example: Router(config-line)# raw-socket tcp client 1.1.1.1 5000 10.10.10.10 9000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> raw-socket packet length packet length</td>
<td>Specifies raw-tcp packet length configuration options.</td>
</tr>
<tr>
<td>Example: Router(config-line)# raw-socket packet-length 32</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> flowcontrol [none</td>
<td>software [lock</td>
</tr>
<tr>
<td>Example: Router(config-line)# flowcontrol none</td>
<td>• none</td>
</tr>
<tr>
<td>• software</td>
<td></td>
</tr>
<tr>
<td>• hardware</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> parity [even</td>
<td>mark</td>
</tr>
<tr>
<td>Example: Router(config-line)# parity none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>Example: Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Channel Group

#### SUMMARY STEPS

1. configure terminal
2. controller serial slot/bay/port
3. channel-group channel-group
4. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Serial Interfaces

### Example: Channel Group

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 controller serial slot/bay/port</td>
<td>Configures the controller.</td>
</tr>
<tr>
<td>Example: Router(config)# controller serial 0/4/1</td>
<td>slot/subslot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td>Step 3 channel-group channel-group</td>
<td>Configures the channel group with specified NxDS0 time slots.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# channel-group 0</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>Example: Router(config-controller)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic.

#### SUMMARY STEPS

1. configure terminal
2. interface serial slot/bay/port
3. encapsulation {ppp|raw-tcp | trans | sdmc}
4. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface serial slot/bay/port</td>
<td>Selects the interface to configure from global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config)# interface serial 0/4/1</code></td>
<td>- <code>slot/subslot/port</code>—Specifies the location of the interface.</td>
</tr>
</tbody>
</table>

**Step 3**

**encapsulation {ppp|raw-tcp | trans | sdmc}**

**Example:**

`Router(config-if)# encapsulation raw-tcp`

**Note**

- **ppp**—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.
- **trans**—Transparent encapsulation.
- **sdmc**—Switched Multimegabit Data Services (SDMC) for serial interface.

**Step 4**

**exit**

**Example:**

`Router(config)# exit`

Exits configuration mode and returns to the EXEC command interpreter prompt.

---

**Example: Encapsulation**

```
Router# configure terminal
Router(config)# interface serial 0/4/1
Router(config-if)# encapsulation raw-tcp
Router(config-if)# exit
```

**Configuring Transparent Pseudowire (PW) Cross-Connect**

Transparent PW mode provides a facility to configure the speed between 300 bps to 230400 bps.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface serial slot/bay/port`
3. `xconnect peer-router-id vcid encapsulation mpls`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

**configure terminal**

**Example:**

`Router# configure terminal` | Enters global configuration mode. |
### Purpose

**Command or Action**

**Step 2**

`interface serial slot/bay/port`

**Example:**

`Router(config)# interface serial 0/4/1`

**Purpose**

Selects the interface to configure from global configuration mode.

- `slot/subslot/port`—Specifies the location of the interface.

**Step 3**

`xconnect peer-router-id vcid encapsulation mpls`

**Example:**

`Router(config-if)# xconnect 1.1.1.1 1001 encapsulation mpls`

**Purpose**

Configures the VC to transport packets.

**Step 4**

`exit`

**Example:**

`Router(config)# exit`

**Purpose**

Exits configuration mode and returns to the EXEC command interpreter prompt.

---

### Example: Transparent Pseudowire on Cross Connect

```
Router# configure terminal
Router(config)# interface serial 0/4/1
Router(config-if)# xconnect 1.1.1.1 1001 encapsulation mpls
Router(config)# exit
```

### Configuring Invert Clock Signal

**SUMMARY STEPS**

1. `configure terminal`
2. `controller serial slot/bay/port`
3. `invert data`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>controller serial slot/bay/port</code></td>
<td>Configures the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# controller serial 0/4/1</code></td>
<td><code>slot/subslot/port</code>—Specifies the location of the interface.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>invert data</code></td>
<td>Configures the invert data clock signal.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-controller)# invert data</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits configuration mode and returns to the EXEC command interpreter prompt.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example: Invert Data on the Serial Interface**

The following example shows invert data configuration on the serial interface.

```
Router# configure terminal
Router(config)# controller serial 0/4/1
Router(config-controller)# invert data
Router(config-controller)# exit
```

**Configuring NRZI Formats**

**SUMMARY STEPS**

1. `configure terminal`
2. `interfaceserial slot/bay/port`
3. `nrzi-encoding`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>interfaceserial slot/bay/port</code></td>
<td>Select the controller to configure and enters serial interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface serial 0/4/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>nrzi-encoding</code></td>
<td>Enable NRZI encoding.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# nrzi-encoding</code></td>
<td>To disable NRZI encoding, use the no form of the command.</td>
</tr>
</tbody>
</table>
Saving the Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>Writes the new configuration to NVRAM.</td>
</tr>
</tbody>
</table>

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 Serial Interface Configuration

Use the following commands to verify the configuration the serial interface

- `show controllers serial slot/bay/port`

Use the `show controllers serial slot/bay/port` command to display serial interface configuration on the router.

```
Router# show controllers serial 0/1/0
Serial0/1/0 - (A900-IMASER14A/S) is up
Encapsulation : RAW-TCP
Cable type: RS-232 DCE
mtu 1500, max_buffer_size 1524, max_pak_size 1524 enc 84
loopback: Off, crc: 16, invert_data: Off
nrzi: Off, idle char: Flag
dce_terminal_timing_enable: Off ignore_dtr: Off
serial_clockrate: 64000bps, serial_clock_index: 14 serial_restartdelay:30000,
serial_restartdelay_def:30000
           DCD=up DSR=up DTR=up RTS=up CTS=up

- `show interfaces serial slot/bay/port`

Use the `show interfaces serial slot/bay/port` command to display serial interface packet status information, model control signal status information on the router.

```
Router# show interfaces serial 0/1/0
Serial0/1/0 is up, line protocol is up
    Hardware is A900-IMASER14A/S
    MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
        reliability 255/255, txload 47/255, rxload 103/255
    Encapsulation RAW-TCP, loopback not set
    Keepalive not supported
    Last input never, output 00:00:00, output hang never
    Last clearing of "show interface" counters 00:38:06
    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 26000 bits/sec, 69 packets/sec
    5 minute output rate 12000 bits/sec, 69 packets/sec
    157782 packets input, 7562229 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
    156062 packets output, 3460471 bytes, 0 underruns
```
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

• show running-config interface serial slot/bay/port

Use the show running-config interface serial slot/bay/port command to display serial interface IP address information, keep alive and cross-connect status information on the router.

Router# show running-config interface serial 0/1/0
Building configuration...
Current configuration : 107 bytes
!
interface Serial0/1/0
  no ip address
  encapsulation trans
  xconnect 1.1.1.1 1001 encapsulation mpls
End

• show xconnect all

Use the show xconnect all command to display all cross-connect status on the router.

Router# show xconnect all
Legend:  XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
        UP=Up  DN=Down  AD=Admin Down  IA=Inactive
        SB=Standby  HS=Hot Standby  RV=Recovering  NH=No Hardware
XC ST  Segment 1  S1  Segment 2  S2
-----+---------------------------------+--+---------------------------------+--
UP pri ac Se0/1/0(HDLC)  UP mpls 1.1.1.1:1001  UP

Use the show raw-socket tcp sessions and show raw-socket tcp statistic commands to display the raw socket status.

Router#show raw-socket tcp sessions
-------------------------------------------------- TCP Sessions
------------------------------------------------------
Interface  tty  vrf_name socket mode local_ip_addr  local_port
dest_ip_addr  dest_port  up_time  idle_time/timeout
0/3/12  154 0 server 20.20.20.20 5000
listening  ----  -----  ----
0/3/12  154 1 server 20.20.20.20 5000
10.10.10.10 9000 00:20:49 00:00:00/5 min

Router#show raw-socket tcp statistic
-------------------------------------------- TCP-Serial Statistics
-----------------------------------------
Interface  tty  vrf_name sessions tcp_in_bytes
tcp_out_bytes  tcp_to_tty_frames  tty_to_tcp_frames
tcp_in_bytes
0/3/12  154 1 1847204
4640310 87709 87671
Configuration Examples

This section includes the following configuration examples:

Example: Encapsulation Configuration

The following example sets encapsulation for the controller and interface:

PE1 CONFIG

ccontroller SERIAL 0/1/0
physical-layer async
channel-group 0
interface Serial0/1/0
  no ip address
  encapsulation trans
  xconnect 2.2.2.2 1001 encapsulation mpls

PE2 CONFIG

ccontroller SERIAL 0/2/0
physical-layer async
channel-group 0
interface Serial0/2/0
  no ip address
  encapsulation trans
  xconnect 1.1.1.1 1001 encapsulation mpls
Dying Gasp Support for Loss of Power Supply Through SNMP, Syslog and Ethernet OAM

Dying Gasp—One of the following unrecoverable condition has occurred:

- Power failure or removal of power supply cable

This type of condition is vendor specific. An Ethernet Operations, Administration, and Maintenance (OAM) notification about the condition may be sent immediately.

- Prerequisites for Dying Gasp Support, on page 141
- Restrictions for Dying Gasp Support, on page 141
- Example: Configuring SNMP Community Strings on a Router, on page 142
- Example: Configuring SNMP-Server Host Details on the Router Console, on page 142
- Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations, on page 143
- Message Displayed on the Peer Router on Receiving Dying Gasp Notification, on page 144
- Displaying SNMP Configuration for Receiving Dying Gasp Notification, on page 144

Prerequisites for Dying Gasp Support

You must enable Ethernet OAM before configuring Simple Network Management Protocol (SNMP) for dying gasp feature. For more information, see Enabling Ethernet OAM on an Interface.

Restrictions for Dying Gasp Support

- The dying gasp feature is not supported if you remove the power supply unit (PSU) from the system.
- SNMP trap is sent only on power failure or removal of power supply cable.
- The dying gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.
- In the case of power loss on the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Routers running Cisco IOS-XE Release 3.14.0S and the Cisco ASR-920-12SZ-IM running the Cisco IOS-XE Release 3.16.0S, dying gasp packets are sent to peer routers. However, the system state is not captured in the system logs (syslogs) or SNMP traps.
• The SNMP servers are configured in ascending order. The SNMP server host configured with the lowest IP address has precedence.

• The SNMP Dying Gasp trap via FPGA is not supported, when core MPLS interface is routed to the port on the Cisco ASR 920-10SZ-PD, ASR-920-8S4Z-PD, ASR-920-4SZ and ASR-920-12CZ routers in Cisco IOS-XE 16.9.x release.

• The SNMP Dying Gasp is supported on the following routers through FPGA:
  • Cisco ASR-920-24SZ-IM
  • Cisco ASR-920-24SZ-M
  • Cisco ASR-920-24TZ-M

The maximum number of supported SNMP servers for SNMP Dying Gasp is two. The maximum number of supported Link-OAMDying Gasp is six. This is applicable to releases starting from Cisco IOS XE 16.9.x release.

• Dying Gasp is not supported on default Mgmt-interface for the following routers:
  • Cisco ASR-920-24SZ-IM
  • Cisco ASR-920-24SZ-M
  • Cisco ASR-920-24TZ-M
  • Cisco ASR 920-10SZ-PD and ASR-920-8S4Z-PD
  • Cisco ASR-920-4SZ
  • Cisco ASR-920-12CZ-A
  • Cisco ASR-920-12CZ-D

This is applicable to releases starting from Cisco IOS XE 16.9.x release.

Example: Configuring SNMP Community Strings on a Router

Setting up the community access string to permit access to the SNMP:

Router> enable
Router# configure terminal
Router(config)# snmp-server community public RW
Router(config)# exit

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

Example: Configuring SNMP-Server Host Details on the Router Console

Specifying the recipient of a SNMP notification operation:
Router> enable
Router# configure terminal
Router(config)# snmp-server host X.X.X.XXX vrf mgmt-intf version 2c public udp-port 9800
Router(config)# exit

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations

**Note**
You can configure up to five different SNMP server host/port configurations.

Environmental Settings on the Network Management Server

```
setenv SR_TRAP_TEST_PORT=UDP port
setenv SR_UTIL_COMMUNITY=public
setenv SR_UTIL_SNMP_VERSION=v2c
setenv SR_MGR_CONF_DIR=Path to the executable snmpinfo.DAT file
```

The following example shows SNMP trap configuration on three hosts:

**Configuration example for the first host:**

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
```

**Configuration example for the second host:**

```
Router(config)#
Router(config)# snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
```

**Configuration example for the third host:**

```
Router(config)#
Router(config)# snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
```

After performing a power cycle, the following output is displayed on the router console:

```
Router#
System Bootstrap, Version 15.3(2r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Wed 17-Oct-12 15:00
Current image running: Boot ROM1
Last reset cause: PowerOn
UEA platform with 2097152 Kbytes of main memory
```
Dying Gasp Trap Received for the Power failure event:

---

**Trap on Host1**

snmp-server host = 7.0.0.149 (nms1-lnx) and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
---

**Trap on Host2**

snmp-server host = 7.0.0.152 (nms2-lnx) and SR_TRAP_TEST_PORT=9988
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
---

**Trap on Host3**

snmp-server host = 7.0.0.166 (erbusnmp-dc-lnx) and SR_TRAP_TEST_PORT=9800
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
---

**Message Displayed on the Peer Router on Receiving Dying Gasp Notification**

001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi4/2 has received a remote failure indication from its remote peer(failure reason = remote client power failure action = )

**Displaying SNMP Configuration for Receiving Dying Gasp Notification**

Use the show running-config command to display the SNMP configuration for receiving dying gasp notification:

```
Router# show running-config | i snmp
snmp-server community public RW
snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
```
snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router#
Displaying SNMP Configuration for Receiving Dying Gasp Notification
CHAPTER 15

Configuring Pseudowire

This chapter provides information about configuring pseudowire features on the Cisco ASR 920 Series Router.

- Pseudowire Overview, on page 147
- CEM Configuration, on page 148
- CEM Configuration Guidelines and Restrictions, on page 148
- Configuring a CEM Group, on page 149
- Using CEM Classes, on page 150
- Configuring CEM Parameters, on page 151
- Configuring Structure-Agnostic TDM over Packet (SAToP), on page 153
- Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 154
- Configuring an Ethernet over MPLS Pseudowire, on page 156
- Configuring Pseudowire Redundancy, on page 157
- Sample Configurations, on page 159

Pseudowire Overview

Effective Cisco IOS-XE Release 3.18S:

- BGP PIC with TDM Pseudowire is supported on the ASR 920 routers with RSP2 modules.
- BGP PIC for Pseudowires, with MPLS Traffic Engineering is supported on the ASR 920 router with RSP2 modules.

The following sections provide an overview of pseudowire support on the Cisco ASR 920 Series Router.

Limitations

If you are running Cisco IOS-XE Release 3.17S and later releases, the following limitations apply:

- Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules.
- BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
- BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
- BGP PIC is not supported for VPLS and H-VPLS.
- BGP PIC is not supported for IPv6.
- If BGP PIC is enabled, Multi-hop BFD should not be configured using the bfd neighbor fall-over bfd command.
• If BGP PIC is enabled, **neighbor ip-address weight** command should not be configured.
• If BGP PIC is enabled, **bgp nexthop trigger delay 6** under the **address-family ipv4** command and **bgp nexthop trigger delay 7** under the **address-family vpnv4** command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration.
• If BGP PIC is enabled and the targeted LDP for VPWS Xconnect services are established over BGP, perform the following tasks:
  • Configure Pseudowire-class (pw-class) with encapsulation “mpls”.
  • Configure no status control-plane route-watch under the pw-class.
  • Associate the pw-class with the VPWS xconnect configurations.

If you are running Cisco IOS-XE 3.18S, the following restrictions apply for BGP PIC with MPLS TE for TDM Pseudowire:

• MPLS TE over MLPPP and POS in the core is not supported.
• Co-existence of BGP PIC with MPLS Traffic Engineering Fast Reroute (MPLS TE FRR) is not supported.

### Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS (EoMPLS) PWs provide a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core network. EoMPLS PWs encapsulate Ethernet protocol data units (PDUs) inside MPLS packets and use label switching to forward them across an MPLS network. EoMPLS PWs are an evolutionary technology that allows you to migrate packet networks from legacy networks while providing transport for legacy applications. EoMPLS PWs also simplify provisioning, since the provider edge equipment only requires Layer 2 connectivity to the connected customer edge (CE) equipment. The Cisco ASR 920 Series Router implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

The Cisco ASR 920 Series Router supports VLAN rewriting on EoMPLS PWs. If the two networks use different VLAN IDs, the router rewrites PW packets using the appropriate VLAN number for the local network. For instructions on how to create an EoMPLS PW, see Configuring an Ethernet over MPLS Pseudowire.

### CEM Configuration

CEM provides a bridge between a time-division multiplexing (TDM) network and a packet network, such as Multiprotocol Label Switching (MPLS). The router encapsulates the TDM data in the MPLS packets and sends the data over a CEM pseudowire to the remote provider edge (PE) router. Thus, function as a physical communication link across the packet network.

**Note** Steps for configuring CEM features are also included in the Configuring Structure-Agnostic TDM over Packet (SAtOP) and Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), on page 154 sections.

### CEM Configuration Guidelines and Restrictions

Not all combinations of payload size and dejitter buffer size are supported. If you apply an incompatible payload size or dejitter buffer size configuration, the router rejects it and reverts to the previous configuration.
Configuring a CEM Group

The following section describes how to configure a CEM group on the Cisco ASR 920 Series Router.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. controller \{t1 | e1\} slot/port
4. cem-group group-number \{unframed | timeslots timeslot\}
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
Example:  
Router> enable  
- Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode.  
Example:  
Router# configure terminal |
| Step 3 | controller \{t1 | e1\} slot/port | Enters controller configuration mode.  
Example:  
Router(config)# controller t1 1/0  
- Use the slot and port arguments to specify the slot number and port number to be configured. |
| Step 4 | cem-group group-number \{unframed | timeslots timeslot\} | Creates a circuit emulation channel from one or more time slots of a T1 or E1 line.  
Example:  
Router(config-controller)# cem-group 6 timeslots 1-4,9,10  
- The **group-number** keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.  
- Use the **unframed** keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line.  
- Use the **timeslots** keyword and the **timeslot** argument to specify the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers. |
| Step 5 | end | Exits controller configuration mode and returns to privileged EXEC mode.  
Example: |
Using CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires. Follow these steps to configure a CEM class:

**Note**

The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.

**Note**

You cannot apply a CEM class to other pseudowire types such as ATM over MPLS.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class cem cem-class`
4. `Router(config-cem-class)# payload-size 512`
5. `Router(config-cem-class)# exit`
6. `Router(config)# interface cem 0/0`
7. `Router(config-if-cem)# exit`
8. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>class cem cem-class</code></td>
<td>Creates a new CEM class</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config)# class cem mycemclass</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring CEM Parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** | Router(config-cem-class)# **payload-size 512**  
**Example:** Router(config-cem-class)# **dejitter-buffer 10**  
**Example:** Router(config-cem-class)# **idle-pattern 0x55** | Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern. |
| **Step 5** | Router(config-cem-class)# **exit** | Returns to the config prompt. |
| **Step 6** | Router(config)# **interface cem 0/0**  
**Example:** Router(config-if)# **no ip address**  
**Example:** Router(config-if)# **cem 0**  
**Example:** Router(config-if-cem)# **cem class mycemclass**  
**Example:** Router(config-if-cem)# **xconnect 10.10.10.10 200 encapsulation mpls** | Configure the CEM interface that you want to use for the new CEM class.  
**Note** The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring. |
| **Step 7** | Router(config-if-cem)# **exit** | Exits the CEM interface. |
| **Step 8** | **exit**  
**Example:** Router(config)# **exit** | Exits configuration mode. |

**Note** The CEM parameters at the local and remote ends of a CEM circuit must match; otherwise, the pseudowire between the local and remote PE routers will not come up.
Configuring Payload Size (Optional)

To specify the number of bytes encapsulated into a single IP packet, use the pay-load size command. The size argument specifies the number of bytes in the payload of each packet. The range is from 32 to 1312 bytes.

Default payload sizes for an unstructured CEM channel are as follows:

- E1 = 256 bytes
- T1 = 192 bytes
- DS0 = 32 bytes

Default payload sizes for a structured CEM channel depend on the number of time slots that constitute the channel. Payload size (L in bytes), number of time slots (N), and packetization delay (D in milliseconds) have the following relationship: L = 8*N*D. The default payload size is selected in such a way that the packetization delay is always 1 millisecond. For example, a structured CEM channel of 16xDS0 has a default payload size of 128 bytes.

The payload size must be an integer multiple of the number of time slots for structured CEM channels.

Setting the Dejitter Buffer Size

To specify the size of the dejitter buffer used to compensate for the network filter, use the dejitter-buffer size command. The configured dejitter buffer size is converted from milliseconds to packets and rounded up to the next integral number of packets. Use the size argument to specify the size of the buffer, in milliseconds. The range is from 1 to 32 ms; the default is 5 ms.

Setting an Idle Pattern (Optional)

To specify an idle pattern, use the [no] idle-pattern pattern1 command. The payload of each lost CESoPSN data packet must be replaced with the equivalent amount of the replacement data. The range for pattern is from 0x0 to 0xFF; the default idle pattern is 0xFF.

Enabling Dummy Mode

Dummy mode enables a bit pattern for filling in for lost or corrupted frames. To enable dummy mode, use the dummy-mode [last-frame | user-defined] command. The default is last-frame. The following is an example:

```
Router(config-cem)# dummy-mode last-frame
```

Setting a Dummy Pattern

If dummy mode is set to user-defined, you can use the dummy-pattern pattern command to configure the dummy pattern. The range for pattern is from 0x0 to 0xFF. The default dummy pattern is 0xFF. The following is an example:

```
Router(config-cem)# dummy-pattern 0x55
```
Shutting Down a CEM Channel

To shut down a CEM channel, use the `shutdown` command in CEM configuration mode. The `shutdown` command is supported only under CEM mode and not under the CEM class.

Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco ASR 920 Series Router:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `controller [T1|E1] 0/4`
4. `cem-group group-number {unframed | timeslots timeslot }
5. Router(config)# interface CEM0/4
6. Router(config-if)# xconnect 30.30.30.2 304 encapsulation mpls
7. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>controller [T1</td>
<td>E1] 0/4</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# controller t1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cem-group group-number {unframed</td>
<td>timeslots timeslot }</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# cem-group 4 unframed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router(config)# interface CEM0/4</td>
<td>Defines a CEM group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Pseudowire

**Example:**

```
Router(config-if)# no ip address
```

**Purpose:**

Enables privileged EXEC mode.

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# cem 4</td>
</tr>
<tr>
<td>Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 30.30.2.304.</td>
</tr>
</tbody>
</table>

**Step 6**

```
Router(config-if)# xconnect 30.30.2 304 encapsulation mpls
```

**Step 7**

```
Router(config)# exit
```

**Purpose:**

Exits configuration mode.

### Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

Follow these steps to configure CESoPSN on the Cisco ASR 920 Series Router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `Router(config)# controller [e1|t1] 0/0`
4. `Router(config-controller)# cem-group 5 timeslots 1-24`
5. `Router(config-controller)# exit`
6. `Router(config)# interface CEM0/5`
7. `Router(config-if-cem)# xconnect 30.30.2 305 encapsulation mpls`
8. `Router(config-if-cem)# exit`
9. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters configuration mode for the E1 or T1 controller.</td>
</tr>
<tr>
<td>`Router(config)# controller [e1</td>
<td>t1] 0/0`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-controller)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the <em>timeslots</em> parameter to assign specific timeslots to the CEM channel.</td>
</tr>
<tr>
<td><code>Router(config-controller)# cem-group 5 timeslots 1-24</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits controller configuration.</td>
</tr>
<tr>
<td><code>Router(config-controller)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Defines a CEM channel.</td>
</tr>
<tr>
<td><code>Router(config)# interface CEM0/5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if-cem)# cem 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 5 to the remote peer 30.30.2.</td>
</tr>
<tr>
<td><code>Router(config-if-cem)# xconnect 30.30.2 305 encapsulation mpls</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as <code>ip route 30.30.30.2 255.255.255.255 1.2.3.4</code>.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits the CEM interface.</td>
</tr>
<tr>
<td><code>Router(config-if-cem)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring an Ethernet over MPLS Pseudowire

Ethernet over MPLS PWs allow you to transport Ethernet traffic over an existing MPLS network. The Cisco ASR 920 Series Router supports EoMPLS pseudowires on EVC interfaces.

For more information about Ethernet over MPLS Pseudowires, see Transportation of Service Using Ethernet over MPLS, on page 148. For more information about how to configure MPLS, see the Cisco IOS XE 3S Configuration Guides. For more information about configuring Ethernet Virtual Connections (EVCs), see Configuring Ethernet Virtual Connections on the Cisco ASR 920 Router.

Follow these steps to configure an Ethernet over MPLS Pseudowire on the Cisco ASR 920 Series Router.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `service instance number ethernet [name ]`
5. `encapsulation {default | dot1q | priority-tagged | untagged}`
6. `xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual] | mpls [manual]} | pw-class pw-class-name } [pw-class pw-class-name] [sequencing {transmit | receive | both}]`
7. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.</td>
</tr>
<tr>
<td>Example: Router(config)# interface gigabitethernet 0/0/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance number ethernet [name ]</td>
<td>Configure an EFP (service instance) and enter service instance configuration) mode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 2 ethernet [name ]</td>
<td>• The <em>number</em> is the EFP identifier, an integer from 1 to 4000.</td>
</tr>
</tbody>
</table>
### Purpose

- **(Optional) ethernet name** is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.

**Note** You can use service instance settings such as encapsulation, dot1q, and rewrite to configure tagging properties for a specific traffic flow within a given pseudowire session. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 920 Router.

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure encapsulation type for the service instance.</td>
</tr>
</tbody>
</table>
| `encapsulation {default | dot1q | priority-tagged | untagged}` | - **default**—Configure to match all unmatched packets.  
- **dot1q**—Configure 802.1Q encapsulation.  
- **priority-tagged**—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.  
- **untagged**—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation. |
| **Example:** | `Router (config-if-srv)# encapsulation dot1q 2` |

### Step 6

Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC.

**Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as `ip route 10.30.30.2 255.255.255.255 10.2.3.4`.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`xconnect peer-ip-address vc-id {encapsulation {l2tpv3 [manual]</td>
<td>mpls [manual]}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls</code></td>
</tr>
</tbody>
</table>

### Step 7

Exits configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# exit</code></td>
</tr>
</tbody>
</table>

---

### Configuring Pseudowire Redundancy

A backup peer provides a redundant pseudowire (PW) connection in the case that the primary PW loses connection; if the primary PW goes down, the Cisco ASR 920 Series Router diverts traffic to the backup PW. This feature provides the ability to recover from a failure of either the remote PE router or the link between the PE router and CE router.

The figure below shows an example of pseudowire redundancy.
You must configure the backup pseudowire to connect to a router that is different from the primary pseudowire.

Follow these steps to configure a backup peer:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `pseudowire-class [pw-class-name]`
4. `encapsulation mpls`
5. `gigabitethernet slot/port`
6. `Router(config)# backup delay enable-delay {disable-delay | never}`
7. `Router(config-if)# xconnect 1.1.1.2 101 encapsulation mpls`
8. `Router(config)# backup peer peer-router-ip-address vcid [pw-class pw-class name ]`
9. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Router&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td><code>pseudowire-class [pw-class-name]</code></td>
<td>Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config)# pseudowire-class mpls</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td>Specifies MPLS encapsulation.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-pw-class)# encapsulation mpls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>gigabitethernet slot/port</td>
<td>Enters configuration mode for the serial interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note</td>
</tr>
<tr>
<td>Router(config)# gigabitethernet 0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# backup delay enable-delay {disable-delay</td>
<td>Configures the backup delay parameters.</td>
</tr>
<tr>
<td>never}</td>
<td>Where:</td>
</tr>
<tr>
<td></td>
<td>• enable-delay — Time before the backup PW takes over for the primary PW.</td>
</tr>
<tr>
<td></td>
<td>• disable-delay — Time before the restored primary PW takes over for the backup PW.</td>
</tr>
<tr>
<td></td>
<td>• never — Disables switching from the backup PW to the primary PW.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# xconnect 1.1.1.2 101 encapsulation mpls</td>
<td>Binds the Ethernet port interface to an attachment circuit to create a pseudowire.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# backup peer peer-router-ip-address vcid</td>
<td>Defines the address and VC of the backup peer.</td>
</tr>
<tr>
<td>[pw-class pw-class name]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Configurations

The following sections contain sample pseudowire configurations.

#### Example: CEM Configuration

The following example shows how to add a T1 interface to a CEM group as a part of a SAToP pseudowire configuration.

This section displays a partial configuration intended to demonstrate a specific feature.

```plaintext
controller T1 0/0/0  
framing unframed  
clock source internal  
linemode b8zs  
cablelength short 110  
cem-group 0 unframed
```
interface CEM0/0/0
no ip address
cem 0
xconnect 18.1.1.1 1000 encapsulation mpls

Example: Ethernet over MPLS

PE 1 Configuration

!
mls label range 16 12000 static 12001 16000
mls label protocol ldp
mls ldp neighbor 10.1.1.1 targeted ldp
mls ldp graceful-restart
multilink bundle-name authenticated
!
!
redundancy
mode sso
!
!
ip tftp source-interface GigabitEthernet0
!
interface Loopback0
ip address 10.5.5.5 255.255.255.255
!
interface GigabitEthernet0/0/4
no ip address
negotiation auto
!
service instance 2 ethernet
encapsulation dot1q 2
xconnect 10.1.1.1 1001 encapsulation mpls
!
service instance 3 ethernet
encapsulation dot1q 3
xconnect 10.1.1.1 1002 encapsulation mpls
!
interface GigabitEthernet0/0/5
ip address 172.7.7.77 255.0.0.0
negotiation auto
mpls ip
mpls label protocol ldp
!
routing ospf 1
router-id 5.5.5.5
network 5.5.5.5 0.0.0.0 area 0
network 172.0.0.0 0.255.255.255 area 0
network 10.33.33.33 0.0.0.0 area 0
network 192.0.0.0 0.255.255.255 area 0
!
**Example: BGP PIC with TDM-PW Configuration**

This section lists the configuration examples for BGP PIC with TDM and TDM–Pseudowire. The below configuration example is for BGP PIC with TDM:

```
router bgp 1
neighbor 18.2.2.2 remote-as 1
neighbor 18.2.2.2 update-source Loopback0
neighbor 18.3.3.3 remote-as 1
neighbor 18.3.3.3 update-source Loopback0

address-family ipv4
```

---

### PE 2 Configuration

```
! mpls label range 16 12000 static 12001 16000
mpls label protocol ldp
mpls ldp neighbor 10.5.5.5 targeted ldp
mpls ldp graceful-restart
multilink bundle-name authenticated
!
 redundancy
mode sso
!
!
ip tftp source-interface GigabitEthernet0
!
interface Loopback0
ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0/4
no ip address
 negotiation auto
!
service instance 2 ethernet
 encapsulation dot1q 2
 xconnect 10.5.5.5 1001 encapsulation mpls
!
service instance 3 ethernet
 encapsulation dot1q 3
 xconnect 10.5.5.5 1002 encapsulation mpls
!
interface GigabitEthernet0/0/5
ip address 172.7.7.7 255.0.0.0
 negotiation auto
mpls ip
mpls label protocol ldp
!
router ospf 1
router-id 10.1.1.1
network 10.1.1.1 0.0.0.0 area 0
network 172.0.0.0 0.255.255.255 area 0
network 10.33.33.33 0.0.0.0 area 0
network 192.0.0.0 0.255.255.255 area 0
```
Adaptive Clock Recovery (ACR)

Adaptive Clock Recovery (ACR) is an averaging process that negates the effect of random packet delay variation and captures the average rate of transmission of the original bit stream. ACR recovers the original clock for a synchronous data stream from the actual payload of the data stream. In other words, a synchronous clock is derived from an asynchronous packet stream. ACR is a technique where the clock from the TDM domain is mapped through the packet domain, but is most commonly used for Circuit Emulation (CEM). ACR is supported on unframed and framed modes of SAToP.

Note

Framing type should be maintained same in all routers end to end.

Effective Cisco IOS XE Everest 16.5.1, ACR is supported on the 8-port T1/E1 interface module.
Benefits of ACR for 8 T1/E1 Interface Module

- Customer-edge devices (CEs) can have different clocks from that of the Provide-edge devices (PEs). Every T1/E1 interface module supports eight pseudowires (or the derived clocks).

Prerequisites for ACR Configuration in 8 T1/E1 Interface Module

- Ensure that CEM is configured before configuring the adaptive clock recovery.
- The following must be configured before configuring the ACR:
  - The remote Customer Equipment and the remote Provider Edge device. These can be configured by using the clock source internal and the clock source line commands under the T1/E1 controller.
  - The controller on the local Customer Equipment connected to the ACR router by using the `clock source line` command.
  - PRC or PRS reference clock from a GPS reference to the remote Customer Equipment or remote CEM Provider Edge device.

Restrictions for ACR on 8 T1/E1 Interface Module

- ACR is supported only on the 8-port T1/E1 interface module (A900-IMA8D). It is not supported on the 16-port T1/E1 interface module (A900-IMA16D), the 32-port T1/E1 interface module (A900-IMA32D), or the 4-port OC3 interface module (A900-IMA4OS).
- ACR is supported only for unframed and framed CEM (SAToP) and for fully-framed CEM (CESoPSN). Fully-framed refers to all the timeslots of T1 (1-24) or E1 (1-31) interfaces.
- ACR is supported only for CEM circuits with MPLS PW encapsulation. ACR is not supported for CEM circuits with UDP or IP PW encapsulation.
- The clock recovered by an ACR clock for a CEM circuit is local to that CEM circuit. The recovered clock cannot be introduced to another circuit and also cannot be introduced to the system clock as a frequency input source.
- The clock ID should be unique for the entire device.
- When a CEM group is configured, dynamic change in clock source is not allowed.
Physical or soft IOR causes the APS switchover time to be higher (500 to 600 ms). Shut or no shut of the port and removal of the active working or protect also cause the APS switchover time to be high.

To overcome these issues, force the APS switchover.

### Configuring ACR for T1 Interfaces for SAToP

To configure the clock on T1/E1 interfaces for SAToP in controller mode:

```
enable
configure terminal
controller t1 0/4/3
clock source recovered 15
cem-group 20 unframed
exit
```

To configure the clock recovery on T1/E1 interfaces in global configuration mode:

```
recovered-clock 0 4
clock recovered 15 adaptive cem 3 20
exit
```

---

**Note**
The clock source recovered configuration on the controller must be completed before configuring the clock recovery in global configuration mode.

---

**Note**
On the controller, the clock source should be configured before CEM group is configured.

---

**Note**
Follow a similar procedure to configure to configure CEM ACR for E1 Interfaces for SAToP. Also, follow a similar procedure to configure CEM ACR for T1 and E1 Interfaces for CESoPSN. Use `cem-group circuit-id timeslots <1-24> | <1-31>` command instead of `cem-group circuit-id unframed` command for the configuration depending on T1 or E1 controller.

To remove the clock configuration in ACR, you must remove the recovery clock configuration in global configuration mode, then remove the CEM circuit, and finally remove the clock source recovered configuration under the controller.

### Verifying the ACR Configuration of T1 Interfaces for SAToP

**Important Notes**

- When multiple ACR clocks are provisioned and if the core network or PSN traffic load primarily has fixed packet rate and fixed size packets, the states of one or more ACR clocks might flap between Acquiring and Acquired states and might not be stable in Acquired state.

  This happens because of the "beating" phenomenon and is documented in *ITU-T G.8261 - Timing and synchronization aspects in packet networks*.

  This is an expected behavior.
• After an ACR clock is provisioned and starts recovering the clock, a waiting period of 15-20 minutes is mandatory before measuring MTIE for the recovered clock.

This behavior is documented in ITU-T G.8261 Timing and synchronization aspects in packet networks Appendix 2.

• When the input stream of CEM packets from the core network or PSN traffic is lost or has many errors, the ACR clock enters the HOLDOVER state. In this state, the ACR clock fails to provide an output clock on the E1/T1 controller. Hence, during the HOLDOVER state, MTIE measurement fails.

This is an expected behavior.

• When the clock output from the clock master or GPS reference flaps or fails, the difference in the characteristics between the holdover clock at the source device and the original GPS clock may result in the ACR algorithm failing to recover clock for a transient period. The MTIE measurement for the ACR clock fails during this time. After this transient period, a fresh MTIE measurement is performed. Similarly, when the GPS clock recovers, for the same difference in characteristics, ACR fails to recover clock and MTIE fails for a transient period.

This is an expected behavior.

• When large-sized packets are received along with the CEM packets by the devices in the core network or PSN traffic, CEM packets may incur delay with variance in delay. As ACR is susceptible to delay and variance in delay, MTIE measurement may fail. This behavior is documented in ITU-T G.8261 section 10.

This is an expected behavior.

• For a provisioned ACR clock that is in Acquired state, if the ACR clock configuration under the recovered-clock global configuration mode is removed and then reconfigured, the status of the ACR clock may initially be ACQUIRED and not FREERUN and then move to Acquiring. This happens because the ACR clock is not fully unprovisioned until the CEM circuit and the controller clock source recovered configuration are removed. Hence, the clock starts from the old state and then re-attempts to recover the clock.

This is an expected behavior.

Use the `show recovered-clock` command to verify the ACR of T1 interfaces for SAToP:

Router#show recovered-clock
Recovered clock status for subslot 0/1
----------------------------------------
Clock Type Mode Port CEM Status Frequency Offset(ppb)
1 T1/E1 ADAPTIVE 3 1 ACQUIRED 100

Use the `show running-config` command to verify the recovery of adaptive clock of T1 interfaces:

Router#show running-config
controller T1 0/1/2
clock source recovered 1
cem-group 1 unframed
interface CEM0/1/3
cem 1
no ip address
xconnect 2.2.2.2 10
encapsulation mpls
## Associated Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Links</th>
</tr>
</thead>
</table>
CHAPTER 16

Configuring and Monitoring Alarm

This chapter describes monitoring alarms, alarms filtering support and configuring external alarms for fan tray alarm port.

This chapter includes the following sections:

- Monitoring Alarms, on page 167
- Configuring External Alarm Trigger, on page 172
- Alarm Filtering Support, on page 175

Monitoring Alarms

Once hardware is installed and operational, use alarms to monitor hardware status on a daily basis.

The routers are designed to send alarm notifications when problems are detected. Network administrators do not need to use show commands to poll devices on a routine basis and can monitor the network remotely. However, network administrators can perform onsite monitoring if they so choose.

Use `snmp-server enable traps alarms <severity>` command to enable the entity related Traps.

The default severity level is informational, which shows all alarms. Severity levels are defined as the following:

- 1—Critical. The condition affects service.
- 2—Major. Immediate action is needed.
- 3—Minor. Minor warning conditions.
- 4—Informational. No action is required. This is the default.

The entity notifications `ceAlarmAsserted` and `ceAlarmCleared` are used to report the condition for e.g. when a physical entity asserted or cleared an alarm.

Effective from Cisco IOS XE Everest 16.6.1, on RSP3 module, alarm notification is enabled on 900 watts DC power supply. There are 2 input feeds for 900 watts DC power supply, if one of the input voltage is lesser than the operating voltage, critical alarm is generated for that particular feed and clears (stops) once the voltage is restored but the power supply state remains in OK state as the other power supply is operationally up.
Network Administrator Checks Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a syslog.

Enabling the Logging Alarm Command

The logging alarm command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of alarm to log. All alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Examples of Alarm Messages

The following alarm messages are examples of alarm messages that are sent to the console when a SPA is removed without first doing a graceful deactivation of the SPA. The alarm is cleared when the SPA is re-inserted.

SPA REMOVED

*May 18 14:50:48.540: %TRANSCEIVER-6-REMOVED: SIP0: iomd: Transceiver module removed from TenGigabitEthernet0/0/1

*May 18 14:50:49.471: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled

*May 18 14:50:49.490: %SPA_OIR-6-OFFLINECARD: SPA (A900-IMA2Z) offline in subslot 0/0

SPA RE-INSERTED

*May 18 14:52:11.803: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0

*May 18 14:52:52.807: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA2Z) online in subslot 0/0

*May 18 14:52:53.543: %TRANSCEIVER-6-INSERTED: SIP0: iomd: transceiver module inserted in TenGigabitEthernet0/0/0

*May 18 14:52:53.551: %TRANSCEIVER-6-INSERTED: SIP0: iomd: transceiver module inserted in TenGigabitEthernet0/0/1

*May 18 14:52:54.780: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/0, changed state to down

*May 18 14:52:54.799: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to down

*May 18 14:53:06.578: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/1, changed state to up

*May 18 14:53:08.482: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to up

ALARMS for Router

To view the alarms on router, use the show facility-alarm status command. The example shows a critical alarm for Power supply along with the description:

SPA Removed
```markdown
Router# show facility-alarm status
System Totals Critical: 22 Major: 0 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>subslot 0/0 Alarm [0]</td>
<td>May 18 2016 14:50:49</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/1</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/2</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/6</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/7</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/3/1</td>
<td>May 11 2016 18:53:44</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/3/2</td>
<td>May 11 2016 18:53:44</td>
<td>INFO</td>
<td>Transceiver Missing [0]</td>
</tr>
<tr>
<td>xcvr container 0/4/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/1</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>GigabitEthernet0/4/3</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/4</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/5</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/6</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/4/7</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>TenGigabitEthernet0/4/8</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
</tbody>
</table>

SPA Re-Inserted

Router# show facility-alarm status
System Totals Critical: 22 Major: 0 Minor: 0

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet0/0/0</td>
<td>May 18 2016 14:53:02</td>
<td>CRITICAL</td>
<td>Physical Port Link Down</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/1</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/2</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/6</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>GigabitEthernet0/1/7</td>
<td>May 11 2016 18:53:36</td>
<td>CRITICAL</td>
<td>Physical Port Link Down [1]</td>
</tr>
<tr>
<td>xcvr container 0/2/0</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
<tr>
<td>xcvr container 0/2/2</td>
<td>May 11 2016 18:54:25</td>
<td>CRITICAL</td>
<td>Transceiver Missing - Link</td>
</tr>
</tbody>
</table>
```

To view critical alarms specifically, use the `show facility-alarm status critical` command:

```
Router# show facility-alarm status critical
System Totals Critical: 22 Major: 0 Minor: 0
Source Time Severity Description [Index]
----- ------ -------- -------------------
TenGigabitEthernet0/0/0 May 18 2016 14:53:02 CRITICAL Physical Port Link Down
GigabitEthernet0/1/0 May 11 2016 18:53:36 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/2/3 May 11 2016 18:54:25 CRITICAL Physical Port Link Down [1]
xcvr container 0/2/4 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/2/5 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
GigabitEthernet0/2/6 May 11 2016 18:54:25 CRITICAL Physical Port Link Down [1]
SONET 0/3/0 May 11 2016 18:54:25 INFO Physical Port Link Down [1]
xcvr container 0/3/1 May 11 2016 18:53:44 INFO Transceiver Missing [0]
xcvr container 0/3/2 May 11 2016 18:53:44 INFO Transceiver Missing [0]
xcvr container 0/3/3 May 11 2016 18:53:44 INFO Transceiver Missing [0]
xcvr container 0/4/0 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/4/1 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/4/2 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
GigabitEthernet0/4/3 May 11 2016 18:54:25 CRITICAL Physical Port Link Down [1]
xcvr container 0/4/4 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/4/5 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/4/6 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
xcvr container 0/4/7 May 11 2016 18:54:25 CRITICAL Transceiver Missing - Link
TenGigabitEthernet0/4/8 May 11 2016 18:54:25 CRITICAL Physical Port Link Down
```

Configuring and Monitoring Alarm

---

Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

170
To view the operational state of the major hardware components on the router, use the `show platform diag` command. This example shows the Power supply P0 has failed:

```plaintext
Router# show platform diag
Chassis type: ASR903
Slot: 1, A900-RSP2A-128
  Running state : ok
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time : 00:03:41 (00:56:24 ago)
  CPLD version : 15092360
  Firmware version : 15.4(3r)S2
Sub-slot: 0/0, A900-IMA2Z
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time : 00:04:46 (00:55:19 ago)
Sub-slot: 0/1, A900-IMA8T
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time : 00:04:46 (00:55:19 ago)
Sub-slot: 0/2, A900-IMA8S
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time : 00:04:46 (00:55:19 ago)
Sub-slot: 0/3, A900-IMA4OS
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time : 00:04:46 (00:55:18 ago)
Sub-slot: 0/4, A900-IMA8S1Z
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time : 00:04:46 (00:55:18 ago)
Sub-slot: 0/5, A900-IMASER14A/S
  Operational status : ok
  Internal state : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time : 00:04:46 (00:55:18 ago)
Slot: R0, A900-RSP2A-128
  Running state : ok, standby
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time : 00:31:28 (00:28:36 ago)
  CPLD version : 15092360
  Firmware version : 15.4(3r)S2
Slot: R1, A900-RSP2A-128
  Running state : ok, active
  Internal state : online
  Internal operational state : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time : 00:02:33 (00:57:31 ago)
```
Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

Configuring External Alarm Trigger

For Cisco ASR 902 Series Router, the fan tray includes an alarm port that maps to two (0 and 1) dry contact alarm inputs. For Cisco ASR 903 Series Router, the fan tray includes an alarm port that maps to four (0 - 3) dry contact alarm inputs.

The pins on the alarm port are passive signals and can be configured as Open (an alarm generated when current is interrupted) or Closed (an alarm is generated when a circuit is established) alarms. You can configure each alarm input as critical, major, or minor. An alarm triggers alarm LEDs and alarm messages. The relay contacts can be controlled through any appropriate third-party relay controller. The open/close configuration is an option controlled in IOS.
Approaches for Monitoring Hardware Alarms

Onsite Network Administrator Responds to Audible or Visual Alarms

An external element can be connected to a power supply using the DB-25 alarm connector on the power supply. The external element is a DC light bulb for a visual alarm and a bell for an audible alarm.

If an alarm illuminates the CRIT, MIN, or MAJ LED on the Cisco ASR 900 Series Route Processor (RP) faceplate, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector. The bell rings or the light bulb flashes.

Clearing Audible and Visual Alarms

To clear an audible alarm, do one of the following:

- Press the Audible Cut Off button on the RP faceplate.

To clear a visual alarm, you must resolve the alarm condition. For example, if a critical alarm LED is illuminated because an active SPA was removed without a graceful deactivation of the SPA, the only way to resolve that alarm is to replace the SPA.

Note

The clear facility-alarm command is not supported. The clear facility-alarm command does not clear an alarm LED on the RP faceplate or turn off the DC light bulb.

How to Configure External Alarms

SUMMARY STEPS

1. enable
2. configure
terminal
3. alarm-contact contact-number description string
4. alarm-contact {contact-number | all {severity {critical | major | minor} | trigger {closed | open}}} }}
5. exit
6. show facility-alarm status

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
| 2    | configure
terminal | Enters global configuration mode. |
|      | Example:         |         |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | `alarm-contact contact-number description string` | (Optional) Configures a description for the alarm contact number.  
- The contact-number can be from 1 to 4.  
- The description string can be up to 80 alphanumeric characters in length and is included in any generated system messages. |
| 4    | `alarm-contact {contact-number | all} {severity {critical | major | minor} | trigger {closed | open}}` | Configures the trigger and severity for an alarm contact number or for all contact numbers.  
- Enter a contact number (1 to 4) or specify that you are configuring all alarms.  
- For `severity`, enter `critical`, `major`, or `minor`. If you do not configure a severity, the default is `minor`.  
- For `trigger`, enter `open` or `closed`. If you do not configure a trigger, the alarm is triggered when the circuit is `closed`. |
| 5    | `exit` | Exits the configuration mode. |
| 6    | `show facility-alarm status` | Displays configured alarms status. |

### Example

```bash
Router>enable
Router#configure terminal
Router(config)#alarm-contact 2 description door sensor
Router(config)#alarm-contact 2 severity major
Router(config)#alarm-contact 2 trigger open
Router(config)#end
Router#show facility-alarm status
```

<table>
<thead>
<tr>
<th>Source</th>
<th>Time</th>
<th>Severity</th>
<th>Description [Index]</th>
</tr>
</thead>
<tbody>
<tr>
<td>subslot 0/0</td>
<td>Sep 21 2016 15:19:55</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
<tr>
<td>Alarm [0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/1</td>
<td>Sep 21 2016 15:19:12</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
<tr>
<td>Alarm [0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/2</td>
<td>Sep 21 2016 15:16:59</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
<tr>
<td>Alarm [0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/3</td>
<td>Sep 21 2016 15:18:10</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
<tr>
<td>Alarm [0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subslot 0/5</td>
<td>Sep 21 2016 15:16:11</td>
<td>CRITICAL</td>
<td>Active Card Removed OIR</td>
</tr>
</tbody>
</table>
The external alarm trigger and syslog support configuration is supported from Cisco IOS XE Release 3.13.0S.

Alarm Filtering Support

The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms.

Information About Alarm Filtering Support

Overview of Alarm Filtering Support

To configure alarm filtering in the Cisco Entity Alarm MIB, you should understand the following concepts:

CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB provides a management client with the capability to monitor alarms generated by physical entities in a network that are identified in the entPhysicalTable of the Entity-MIB (RFC 2737). Examples of these physical entities are chassis, fans, modules, ports, slots, and power supplies. The management client interfaces with an SNMP agent to request access to objects defined in the CISCO-ENTITY-ALARM-MIB.

ceAlarmGroup

The ceAlarmGroup is a group in the CISCO-ENTITY-ALARM-MIB that defines objects that provide current statuses of alarms and the capability to instruct an agent to stop (cut off) signaling for any or all external audible alarms.

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount
• ceAlarmMinorCount
• ceAlarmCutoff
• ceAlarmFilterProfile
• ceAlarmSeverity
• ceAlarmList

**ceAlarmFilterProfileTable**

The ceAlarmFilterProfileTable filters alarms according to configured alarm lists. The filtered alarms are then sent out as SNMP notifications or syslog messages, based on the alarm list enabled for each alarm type. This table is defined in the CISCO-ENTITY-ALARM-MIB and implemented in the group ceAlarmGroup.

**ceAlarmFilterProfile**

An alarm filter profile controls the alarm types that an agent monitors and signals for a corresponding physical entity. The ceAlarmFilterProfile object holds an integer value that uniquely identifies an alarm filter profile associated with a corresponding physical entity. When the value is zero, the agent monitors and signals all alarms associated with the corresponding physical entity.

**ceAlarmHistTable:**

This table contains the history of ceAlarmAsserted and ceAlarmCleared traps generated by the agent. Each entry to the table will have physical index from entPhysicalTable and the severity of the alarm. The ceAlarmAsserted and ceAlarmCleared trap varbinds are mostly from this table and the description from ceAlarmDescrTable.

**ceAlarmDescrTable:**

This table contains a description for each alarm type defined by each vendor type employed by the system. This table has the list of possible severity levels and the description for the physical entity, Object “ceAlarmDescrSeverity” indicates the severity of an alarm (1 to 4 as above).

**ceAlarmTable:**

This table specifies alarm control and status information related to each physical entity contained by the system, including the alarms currently being asserted by each physical entity capable of generating alarms.

**Prerequisites for Alarm Filtering Support**

- SNMP is configured on your routing devices.
- Familiarity with the ENTITY-MIB and the CISCO-ENTITY-ALARM-MIB.

**Restrictions for Alarm Filtering Support**

- The CISCO-ENTITY-ALARM-MIB supports reporting of alarms for physical entities only, including chassis, slots, modules, ports, power supplies, and fans. In order to monitor alarms generated by a physical entity, it must be represented by a row in the entPhysicalTable.
How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications

Configuring Alarm Filtering for Syslog Messages

This task describes how to configure the alarm severity threshold for generating syslog messages. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

```
enable
cfg-term
logging alarm 2
show facility-alarm status
```

Configuring Alarm Filtering for SNMP Notifications

This task describes how to configure the alarm severity threshold for generating SNMP notifications. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

```
enable
cfg-term
snmp-server enable traps alarms 2
show facility-alarm status
```

Configuration Examples for Alarm Filtering Support

Configuring Alarm Filtering for Syslog Messages: Example

The following example shows how to configure an alarm filter for syslog messages:

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps alarms 2
Router(config)#
Router(config)# exit
Router# show facility-alarm status
System Totals Critical: 2 Major: 1 Minor: 0
Source Time Severity Description [Index]
------ ------ -------- -------------------
Power Supply Bay 0 Jun 07 2016 13:36:49 CRITICAL Power Supply/FAN Module Missing [0]
xcvr container 0/5/0 Jun 07 2016 13:37:43 CRITICAL Transceiver Missing - Link Down [1]
```

Configuring Alarm Filtering for SNMP Notifications: Example

The following example shows how to configure an alarm filter for SNMP notifications:

```
```
```
Configuring Alarm Filtering for SNMP Notifications: Example

xcvr container 0/5/7       Jun 07 2016 13:37:43       INFO       Transceiver Missing [0]
Tracing Overview

Tracing is a function that logs internal events. Trace files are automatically created and saved to the tracelogs directory on the harddisk: file system on the router, which stores tracing files in bootflash:. Trace files are used to store tracing data.

The contents of trace files are useful for the following purposes:

- Troubleshooting—If a router is having an issue, the trace file output may provide information that is useful for locating and solving the problem. Trace files can almost always be accessed through diagnostic mode even if other system issues are occurring.
- Debugging—The trace file outputs can help users get a more detailed view of system actions and operations.

How Tracing Works

The tracing function logs the contents of internal events on the router. Trace files with all trace output for a module are periodically created and updated and are stored in the tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance.

The most recent trace information for a specific module can be viewed using the show platform software trace message privileged EXEC and diagnostic mode command. This command can be entered to gather trace log information even during an IOS failure because it is available in diagnostic mode.

Trace files can be copied to other destinations using most file transfer functions (such as FTP, TFTP, and so on) and opened using a plaintext editor.

Tracing cannot be disabled on the router. Trace levels, however, which set the message types that generate trace output, are user-configurable and can be set using the set platform software trace command. If a user...
wants to modify the trace level to increase or decrease the amount of trace message output, the user should set a new tracing level using the `set platform software trace` command. Trace levels can be set by process using the `all-modules` keyword within the `set platform software trace` command, or by module within a process. See the `set platform software trace` command reference for more information on this command, and the Tracing Levels, on page 180 section of this document for additional information on tracing levels.

## Tracing Levels

Tracing levels determine how much information about a module should be stored in the trace buffer or file. The table below shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

### Table 12: Tracing Levels and Descriptions

<table>
<thead>
<tr>
<th>Trace Level</th>
<th>Level Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>0</td>
<td>The message is regarding an issue that makes the system unusable.</td>
</tr>
<tr>
<td>Alert</td>
<td>1</td>
<td>The message is regarding an action that must be taken immediately.</td>
</tr>
<tr>
<td>Critical</td>
<td>2</td>
<td>The message is regarding a critical condition. This is the default setting.</td>
</tr>
<tr>
<td>Error</td>
<td>3</td>
<td>The message is regarding a system error.</td>
</tr>
<tr>
<td>Warning</td>
<td>4</td>
<td>The message is regarding a system warning</td>
</tr>
<tr>
<td>Notice</td>
<td>5</td>
<td>The message is regarding a significant issue, but the router is still working normally.</td>
</tr>
<tr>
<td>Informational</td>
<td>6</td>
<td>The message is useful for informational purposes only.</td>
</tr>
<tr>
<td>Debug</td>
<td>7</td>
<td>The message provides debug-level output.</td>
</tr>
<tr>
<td>Verbose</td>
<td>8</td>
<td>All possible tracing messages are sent.</td>
</tr>
<tr>
<td>Noise</td>
<td>-</td>
<td>All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.</td>
</tr>
</tbody>
</table>

Trace level settings are leveled, meaning that every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3(error) ensures that the trace file will contain all output for the 0(emergencies), 1(alerts), 2(critical), and 3(error) settings. Setting the trace level to 4(warning) will ensure that all trace output for the specific module will be included in that trace file.

The default tracing level for every module on the router is notice.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.
When setting trace levels, it is also important to remember that the setting is not done in a configuration mode, so trace level settings are returned to their defaults after every router reload.

⚠️ **Caution**

Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to this level or higher should be done with discretion.

⚠️ **Caution**

Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

**Viewing a Tracing Level**

By default, all modules on the router are set to notice. This setting will be maintained unless changed by a user.

To see the tracing level for any module on the router, enter the `show platform software trace level` command in privileged EXEC or diagnostic mode.

In the following example, the `show platform software trace level` command is used to view the tracing levels of the Forwarding Manager processes:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                  Trace Level
-----------------------------------------------
  acl                       Notice
  binos                     Notice
  binos/brand               Notice
  bipc                      Notice
  bsignal                   Notice
  btrace                    Notice
  cce                       Notice
  cdllib                    Notice
  cef                       Notice
  chasfs                    Notice
  chasutil                  Notice
  erspan                    Notice
  ess                       Notice
  ether-channel             Notice
  evlib                     Notice
  evutil                    Notice
  file_alloc                Notice
  fman_rp                   Notice
  fpm                       Notice
  fw                        Notice
  icmp                      Notice
  interfaces               Notice
  iosd                      Notice
  ipc                       Notice
  ipclog                    Notice
  iphc                      Notice
  ipsec                     Notice
  mgmte-acl                 Notice
  mlp                       Notice
```
Setting a Tracing Level

To set a tracing level for any module on the router, or for all modules within a process on the router, enter the `set platform software trace` privileged EXEC and diagnostic mode command.

In the following example, the trace level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 is set to info.

```
set platform software trace forwarding-manager F0 acl info
```

See the `set platform software trace` command reference for additional information about the options for this command.

Viewing the Content of the Trace Buffer

To view the trace messages in the trace buffer or file, enter the `show platform software trace message` privileged EXEC and diagnostic mode command.
In the following example, the trace messages for the Host Manager process in Route Switch Processor slot 0 are viewed using the `show platform software trace message` command:

Router# `show platform software trace message host-manager R0`
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in slot 0
BCP Support on MLPPP

This feature module describes how to configure Bridge Control Protocol (BCP) Support over Multilink PPP (MLPPP).

Note

This feature is only applicable for Cisco ASR 900 RSP2 Module.

- Finding Feature Information, on page 185
- Information About BCP Support on MLPPP, on page 186
- How to Configure BCP Support on MLPPP, on page 187
- Configuration Examples for BCP Support on MLPPP, on page 195
- Additional References, on page 203
- Feature Information for BCP Support on MLPPP, on page 204

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for BCP Support on MLPPP section.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for BCP Support on MLPPP

- Cisco IOS XE Everest 16.5.1 or a later release that supports the BCP Support on MLPPP feature must be installed previously on the Cisco ASR 900.

Restrictions for BCP Support on MLPPP

- IPv6 is not supported.
- Routing is not supported, hence, BDI is also not supported on BCP over MLPPP.
• Spanning Tree Protocol (STP) and Resilient Ethernet Protocol (REP) are not supported.
• Jumbo frames are not supported.
• Supports 16 T1/E1 and OC3 IM only. A maximum number of 16 (0-15) links per MLPPP bundle are supported, where traffic rate is not beyond MLPPP bandwidth. For E1 link, 16 E1 serial interfaces can be in one MLPPP bundle. For T1, 16 T1 links can be in one MLPPP bundle.
• The following encapsulations are not supported: QinQ, dot1ad, and dot1ad-dot1q.
• You cannot configure default or untagged encapsulations on two different multilinks. When default is configured on a multilink, you can configure another EFP as untagged on the same multilink. For untagged, the same multilink cannot have another EFP configured as untagged.
• Two different multilinks cannot bridge the same encapsulated VLAN.
• The same bridge domain cannot be configured twice on the same interface.
• Connectivity Fault Management (CFM), Y.1731, and Layer 2 protocol forward tagged are not supported.
• Set qos-group is not supported in the output policy of physical Gigabit interface and EVC of the multilink interface. Set qos-group on ASR 903 will not mark the packet. The scope of the set qos-group is limited to the router.
• QoS policy is not supported on multilink at the interface level. However, it is supported on different EVCs of the multilink interfaces.
• Qos-group classification will work only on the egress interface or EFP interface.
• The MLPPP interface bundle supports only a maximum of 64 EVCs.
• A maximum of 64 VLANs are supported across all the MLPPPs.
• Layer 3 traffic with default encapsulation is not supported.
• Multicast and IGMP is not supported.
• For ingress classification to work, it should be classified based on “match cos inner <>” or “match vlan inner <>”.
• Layer 2 QoS behavior is supported only on tagged/priority tagged packets. It is not supported for untagged packets.
• Only 1r2C policer is supported at the egress.
• With BCP on MLPPP, the COS bits in the payload are not preserved end to end.

Information About BCP Support on MLPPP

The BCP, as described in RFC 3518, is responsible for configuring, enabling and disabling the bridge protocol modules on both ends of the point-to-point link. The BCP feature enables forwarding of Ethernet frames over serial networks, and provides a high-speed extension of enterprise LAN backbone traffic through a metropolitan area.

When BCP is supported on MLPPP, it enables transport of Ethernet Layer 2 frames through MLPPP. In the following diagram, Bridge-A is connected to Bridge-B using MLPPP. The MLPPP bundle acts as a trunk link connecting Bridge-A and Bridge-B, transporting multiple VLANs. Using this feature, the hosts in VLAN 100, who are connected to Bridge-A, can talk to the hosts in VLAN 200, who are connected to Bridge-B.
Supported Profiles and Protocols

- Ethernet II frames
- 802.1Q tagged frames
- IPv4 packets
- Frame sizes from 64 to 1522 octets

Quality of Service

The Ethernet Layer 2 traffic is classified on the egress at the EVC of the Multilink interface based on IP DSCP or VLAN CoS bits. Based on this classification, egress policing (bandwidth percent or priority percent) is achieved. You can also re-mark the QoS field. The following table lists the options available for re-marking.

<table>
<thead>
<tr>
<th>IP DSCP</th>
<th>VLAN CoS or PCP Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set IP DSCP (re-mark IP DSCP)</td>
<td>Set IP DSCP</td>
</tr>
<tr>
<td>Set VLAN CoS or Priority Code Point (PCP) Bits</td>
<td>Set VLAN CoS Bits (re-mark VLAN CoS or PCP Bits)</td>
</tr>
<tr>
<td>Bandwidth Percent or Priority Percent</td>
<td>Bandwidth Percent or Priority Percent</td>
</tr>
</tbody>
</table>

How to Configure BCP Support on MLPPP

Configuring Multiple EFPs Bridged Through the Same Link

To bridge multiple EFPs through the same multilink, you should create two EFPs and add them to the multilink.

To configure an EFP and a multilink, complete the following tasks:

Configuring an EFP

To configure an EFP, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance number ethernet
5. encapsulation dot1q vlan-id
6. rewrite ingress tag pop 1 symmetric
7. bridge-domain bridge-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Specifies an interface type and number, and places the device in interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface GigabitEthernet 0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance number ethernet</td>
<td>Configures an EFP (service instance) and enters service instance configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# service instance 10 ethernet</td>
<td>number—EFP identifier; an integer from 1 to 4000.</td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q vlan-id</td>
<td>Configures encapsulation type for the service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# encapsulation dot1q 50</td>
<td>vlan-id—Virtual LAN identifier. The valid range is from 1 to 4094.</td>
</tr>
<tr>
<td><strong>Step 6</strong> rewrite ingress tag pop 1 symmetric</td>
<td>Specifies that encapsulation modification occurs on packets at ingress.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> bridge-domain bridge-id</td>
<td>Configures the bridge domain ID.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if-srv)# bridge-domain 100</td>
<td>bridge-id—Bridge domain number. The valid range is from 1 to 4094.</td>
</tr>
</tbody>
</table>

Adding an EFP to a Multilink

To add an EFP to a multilink, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance number ethernet
5. encapsulation dot1q vlan-id
6. rewrite ingress tag pop 1 symmetric
7. bridge-domain bridge-id
8. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>interface type number</td>
<td>Specifies an interface type and number, and places the device in interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface Multilink 5</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>service instance number ethernet</td>
<td>Configures an EFP (service instance) and enters service instance configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- number—EFP identifier; an integer from 1 to 4000.</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# service instance 10 ethernet</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q vlan-id</td>
<td>Configures encapsulation type for the service instance.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- vlan-id—Virtual LAN identifier. The valid range is from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# encapsulation dot1q 60</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>rewrite ingress tag pop 1 symmetric</td>
<td>Specifies that encapsulation modification occurs on packets at ingress.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>bridge-domain bridge-id</td>
<td>Configures the bridge domain ID.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- bridge-id—Bridge domain number. The valid range is from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# bridge-domain 100</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Exits service instance configuration mode and enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-if-srv)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Note: Repeat Step 4 to Step 7 to add another EFP to the Multilink.
Configuring Multiple Encapsulated VLANs Bridged Through Different Multilinks

You should create two encapsulated VLANs and add them to two multilinks for this configuration to work.

To configure multiple encapsulated VLANs bridged through different multilinks, complete the following tasks:

Adding an Encapsulated VLAN to Multilinks

To add an encapsulated VLAN to separate multilinks, complete the following steps:

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *number ethernet*
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain** *bridge-id*
8. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <em>type number</em></td>
<td>Specifies an interface type and number, and places the device in</td>
</tr>
<tr>
<td>Example:</td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td>Router(config)# interface Multilink 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance <em>number ethernet</em></td>
<td>Configures an EFP (service instance) and enters service instance</td>
</tr>
<tr>
<td>Example:</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Router(config-if)# service instance 10 ethernet</td>
<td>number—EFP identifier; an integer from 1 to 4000.</td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q <em>vlan-id</em></td>
<td>Configures encapsulation type for the service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td>• vlan-id—Virtual LAN identifier. The valid range is from 1 to 4094.</td>
</tr>
<tr>
<td>Router(config-if-srv)# encapsulation dot1q 60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> rewrite ingress tag pop 1 symmetric</td>
<td>Specifies that encapsulation modification occurs on packets at ingress.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring QoS for BCP Support on MLPPP

The egress policy at the EVC of the multilink interface matches the IP DSCP value and VLAN CoS bits. Based on this classification it re-marks these values and performs egress policing (Priority percent or Bandwidth percent), shaping, priority shaper, BRR/BRP.

To configure QoS for BCP Support on MLPPP, complete the following tasks:

- **Note**: Define a QoS policy, and apply it to the MLPPP interface, and configure a matching policy on the EFP interface.

### Defining a QoS Policy

To define a QoS policy, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. class-map match-any class-map-name
4. match ip dscp dscp-list
5. class-map match-any class-map-name
6. match qos-group qos-group-value
7. policy-map policy-map-name
8. class class-name
9. priority percent percentage
10. set ip dscp ip-dscp-value
11. class class-name
12. bandwidth percent percentage
13. set qos-group group-id
# Defining a QoS Policy

## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>class-map match-any class-map-name</code></td>
<td>Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• <code>class-map-name</code>—Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>match ip dscp dscp-list</code></td>
<td>Matches IP DSCP packeting using Assured Forwarding (AF) by entering the binary representation of the DSCP value.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>class-map match-any class-map-name</code></td>
<td>Creates a class map to be used for matching packets to a specified class.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>match qos-group qos-group-value</code></td>
<td>Identifies a specific quality of service (QoS) group value as a match criterion.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• <code>qos-group-value</code>—The exact value used to identify a QoS group value. The valid range is from 0 to 7.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>policy-map policy-map-name</code></td>
<td>Creates a policy map that can be attached to one or more interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• <code>policy-map-name</code>—Name of the policy map.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>class class-name</code></td>
<td>Specifies the name of the class whose policy you want to create or change. Alternatively, is used to specify the default class (commonly known as the class-default class) before you configure its policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• <code>class-name</code>—Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>priority percent percentage</code></td>
<td>Provides priority to a class of traffic belonging to a policy map.</td>
</tr>
</tbody>
</table>
### Command or Action

**Router(config-pmap-c)# priority percent 20**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>percentage</strong>—Total available bandwidth to be set aside for the priority class. The valid range is from 1 to 100.</td>
</tr>
</tbody>
</table>

**Step 10**

**set ip dscp ip-dscp-value**

**Example:**

```
Router(config-pmap-c)# set ip dscp ef
```

<table>
<thead>
<tr>
<th>Marks a packet by setting the IP DSCP value in the type of service (ToS) byte.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>ip-dscp-value</strong>—IP DSCP value; The valid values are from 0 to 63.</td>
</tr>
</tbody>
</table>

**Step 11**

**class class-name**

**Example:**

```
Router(config-pmap-c)# class qos-group3
```

| Specifies the name of the class whose policy you want to create or change. Alternatively, is used to specify the default class (commonly known as the class-default class) before you configure its policy. |

**Step 12**

**bandwidth percent percentage**

**Example:**

```
Router(config-pmap-c)# bandwidth percent 20
```

<table>
<thead>
<tr>
<th>Specifies the bandwidth allocated for a class belonging to a policy map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>percentage</strong>—Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is from 1 to 100.</td>
</tr>
</tbody>
</table>

**Step 13**

**set qos-group group-id**

**Example:**

```
Router(config-pmap-c)# set qos-group 4
```

<table>
<thead>
<tr>
<th>Sets a QoS group identifier (ID) that can be used later to classify packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>group-id</strong>—Group ID number. The valid range is from 0 to 99.</td>
</tr>
</tbody>
</table>

### Applying a QoS Policy on an MLPPP Interface

To apply a QoS policy on an MLPPP interface, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. service instance number ethernet
5. service-policy output policy-map-name
6. encapsulation dot1q vlan-id
7. rewrite ingress tag pop 1 symmetric
8. bridge-domain bridge-id

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Specifies an interface type and number, and places the device in interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface Multilink 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance number ethernet</td>
<td>Configures an EFP (service instance) and enters service instance configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service instance 20 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> service-policy output policy-map-name</td>
<td>Attaches a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC.</td>
</tr>
<tr>
<td>Example: Router(config-if)# service-policy output bcpmlpppqos</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> encapsulation dot1q vlan-id</td>
<td>Configures encapsulation type for the service instance.</td>
</tr>
<tr>
<td>Example: Router(config-if-srv)# encapsulation dot1q 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> rewrite ingress tag pop 1 symmetric</td>
<td>Specifies that encapsulation modification occurs on packets at ingress.</td>
</tr>
<tr>
<td>Example: Router(config-if-srv)# rewrite ingress tag pop 1 symmetric</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> bridge-domain bridge-id</td>
<td>Configures the bridge domain ID.</td>
</tr>
<tr>
<td>Example: Router(config-if-srv)# bridge-domain 100</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying BCP Support on MLPPP**

To display the Multilink PPP bundle information on various interfaces on a router, use the `show` command, as described in the following example:

```
Router# show ppp multilink interface multilink 1
```

Multilink 1
  Bundle name: ASR1
  Remote Endpoint Discriminator: [1] ASR1
  Local Endpoint Discriminator: [1] ASR2
  Bundle up for 17:06:50, total bandwidth 20480, load 6/255
  2 receive classes, 2 transmit classes
  Receive buffer limit 123040 bytes per class, frag timeout 1000 ms
  Bundle is Distributed
  Receive Class 0:
Configuration Examples for BCP Support on MLPPP

Example: Configuring an EFP

The following are the examples of two ways in which you can configure an EFP.

Method 1

```plaintext
enable
configure terminal
interface GigabitEthernet 0/0
service instance 10 ethernet
encapsulation dot1q 50
rewrite ingress tag pop 1 symmetric
bridge-domain 100
```

Method 2

```plaintext
enable
configure terminal
interface GigabitEthernet 0/0
service instance 10 ethernet
encapsulation dot1q 50
rewrite ingress tag pop 1 symmetric
exit
configure terminal
bridge-domain 100
member Multilink1 service-instance 100
```
Example: Multilink with a Single EFP

The following is a sample configuration of a multilink with a single EFP.

Figure 6: Multilink with a Single EFP

Example: Multilink with Multiple EFPs

The following is a sample configuration of a multilink with multiple EFPs.
Example: Multilink with QoS

The following is a sample configuration of Multilink with QoS:
Example: Multilink Between Cisco ASR 903 Series Routers and Cisco C7600 Series Routers

The following is a sample configuration of multilink between a Cisco ASR 903 Series Routers and Cisco C7600 Series Routers:
Example: Multilink with Maximum 10 Links

The following is a sample configuration of multilink with maximum 10 links.

```
class-map match-any qos-group1
  match qos-group 1
class-map match-any qos-group2
  match qos-group 2
class-map match-any qos-group3
```

The following sample configurations show how to configure multilink with maximum 10 links.

Policy Map 1
match qos-group 3  
class-map match-any qos-group4  
match qos-group 4  
class-map match-any qos-group5  
match qos-group 5  
class-map match-any qos-group6  
match qos-group 6  
class-map match-any qos-group7  
match qos-group 7  

policy-map bcpmlpppqos  
class qos-group1  
priority percent 20  
set qos-group 2  
class qos-group2  
bandwidth percent 20  
set qos-group 3  
class qos-group3  
bandwidth percent 10  
set qos-group 4  
class qos-group4  
bandwidth percent 5  
set qos-group 5  
class qos-group5  
bandwidth percent 30  
set qos-group 6  
class qos-group6  
bandwidth percent 15  
set qos-group 1  

Policy Map 2  

class-map match-any dscpaf11  
match ip dscp af11  
class-map match-any dscpaf12  
match ip dscp af12  
class-map match-any dscpaf21  
match ip dscp af21  
class-map match-any dscpaf31  
match ip dscp af31  
class-map match-any dscpcs1  
match ip dscp cs1  
class-map match-any dscpef  
match ip dscp ef  
class-map match-any dscpdefault  
match ip dscp default  

policy-map bcpmlpppdscp  
class dscpaf11  
priority percent 20  
set ip dscp af12  
class dscpaf12  
bandwidth percent 20  
set ip dscp af13  
class dscpaf21  
bandwidth percent 10  
set ip dscp af22  
class dscpaf31  
bandwidth percent 5  
set ip dscp af32  
class dscpcs1  
bandwidth percent 30
set ip dscp cs2
class dscpEF
bandwidth percent 10
set ip dscp cs7
class dscpdefault
bandwidth percent 5
set ip dscp cs5

MLPPP-GIG - 1

interface Multilink1
service instance 1 ethernet
service-policy output bcpmlpppqos
   encapsulation untagged
   bridge-domain 3000

interface Multilink2
service instance 1 ethernet
service-policy output bcpmlpppqos
   encapsulation dot1q 50
   bridge-domain 2000
service instance 2 ethernet
   encapsulation dot1q 60
   bridge-domain 2001

interface gigabitethernet 0/5
service instance 1 ethernet
   encapsulation dot1q 50
   bridge-domain 2000
service instance 2 ethernet
   encapsulation dot1q 60
   bridge-domain 2001
service instance 3 ethernet
   encapsulation untagged
   bridge-domain 3000

ADD-MLPPP-GIG - 1

interface Multilink1
service instance 2 ethernet
service-policy output bcpmlpppqos
   encapsulation dot1q 70
   bridge-domain 3001

interface gigabitethernet 0/5
service instance 4 ethernet
   encapsulation dot1q 70
   bridge-domain 3001

MLPPP-GIG-2

interface Multilink1
service instance 1 ethernet
service-policy output bcpmlpppsdscp
   encapsulation untagged
   bridge-domain 3000
interface Multilink2
  service instance 2 ethernet
  service-policy output bcpmlpppdscp
    encapsulation dot1q any
    bridge-domain 3001
interface gigabitethernet 0/5
  service instance 1 ethernet
  encapsulation untagged
  bridge-domain 3000
  service instance 2 ethernet
  encapsulation dot1q any
  bridge-domain 3001

MLPPP-GIG-3

interface Multilink1
  service instance 1 ethernet
  service-policy output bcpmlpppdscp
    encapsulation default
    bridge-domain 3000
interface gigabitethernet 0/5
  service instance 1 ethernet
  encapsulation default
  bridge-domain 3000

Sample Configuration of MLPPP Bundled 10 Member Links

interface Multilink1
  no ip address
  load-interval 30
  ppp pfc local request
  ppp pfc remote apply
  ppp acfc local request
  ppp acfc remote apply
  ppp multilink
  ppp multilink interleave
  ppp multilink group 1
  ppp multilink fragment size 256
  ppp multilink multiclass
  service instance 102 ethernet
  service-policy output bcpmlpppqos
    encapsulation dot1q 102
    rewrite ingress tag pop 1 symmetric
    bridge-domain 102

interface Serial0/0:0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
interface Serial0/1:0
  no ip address
  encapsulation ppp
  ppp multilink
Additional References

The following sections provide references related to BCP Support on MLPPP feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3518</td>
<td>Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)</td>
</tr>
</tbody>
</table>

Technical Assistance

Table 14: Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for BCP Support on MLPPP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP Support on MLPPP</td>
<td>Cisco IOS XE Everest 16.5.1</td>
<td>This feature was introduced on the Cisco ASR 903 Series Routers.</td>
</tr>
</tbody>
</table>