Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide

First Published: 2011-11-10

Last Modified: 2015-03-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Cisco ASR 901 Router Overview

Cisco ASR 901 Mobile Wireless Router is a cell-site access platform specifically designed to aggregate and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G radio access network (RAN). The Cisco ASR 901 is availabe in the following models:

- Cisco ASR 901-TDM version (A901-12C-FT-D, A901-4C-FT-D, A901-6CZ-FT-D, A901-6CZ-FT-A)
- Cisco ASR 901-Ethernet version (A901-12C-F-D, A901-4C-F-D, A901-6CZ-F-D, A901-6CZ-F-A)

The Cisco ASR 901 router helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using HSPA or LTE, Base Transceiver Stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Code Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment.

The Cisco ASR 901 router transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1/E1 circuits, including leased line, microwave, and satellite. It also supports alternative backhaul networks, including Carrier Ethernet and Ethernet in the First Mile (EFM).

The Cisco ASR 901 router also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport.

Custom designed for the cell site, the Cisco ASR 901 features a small form factor, extended operating temperature, and cell-site DC input voltages.

The Cisco ASR 901 TDM version provides 12 Gigabit Ethernet ports, 16 T1/E1 ports and one Management port. Whereas, the Cisco ASR 901 Ethernet version does not contain the 16 T1/E1 ports. It has only 12 Gigabit Ethernet ports and one management port.

The Cisco ASR 901 router supports Ethernet Virtual Circuits (EVC) only. Metro-Ethernet Forum (MEF) defines an Ethernet Virtual Connection as an association between two or more user network interfaces identifying a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual *service pipe* within the service provider network.

Introduction

A RAN is typically composed of thousands of BTSs or Node Bs, hundreds of base station controllers or radio network controllers (BSCs or RNCs), and several mobile switching centers (MSCs). The BTS or Node Bs and BSC or RNC are often separated by large geographic distances, with the BTSs or Node Bs located in cell sites uniformly distributed throughout a region, and the BSCs, RNCs, and MSCs located at suitably chosen Central Offices (CO) or mobile telephone switching offices (MTSO).

The traffic generated by a BTS or Node B is transported to the corresponding BSC or RNC across a network, referred to as the backhaul network, which is often a hub-and-spoke topology with hundreds of BTS or Node Bs connected to a BSC or RNC by point-to-point time division multiplexing (TDM) trunks. These TDM trunks may be leased-line T1/E1s or their logical equivalents, such as microwave links or satellite channels.

The Cisco ASR 901 has two different types of interfaces by default: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), EtherChannel Link Aggregation Control Protocol (LACP).

Features

This section contains the following topics:

Performance Features

- Autosensing of port speed and autonegotiation of duplex mode on all ports for optimizing bandwidth.
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 100 and 100/1000 Mbps interfaces and on 100/1000 BASE-T/TX small form-factor pluggable (SFP) module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately.
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gbps (Gigabit EtherChannel) or 800 Mbps (Fast EtherChannel) full duplex of bandwidth between switches, routers, and servers.
- Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links (supported only on NNIs or ENIs).
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate.

Management Options

- CLI—You can access the CLI either by connecting your management station directly to the router console port or by using Telnet from a remote management station. For more information about the CLI, see Using the Command-Line Interface, on page 51
- Cisco Configuration Engine—The Cisco Configuration Engine is a network management device that works with embedded Cisco IOS CNS Agents in the Cisco ASR 901 Series Aggregation Services Router software. You can automate initial configurations and configuration updates by generating router-specific configuration changes, sending them to the router, executing the configuration change, and logging the results.

- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager.

For information about configuring SNMP, see http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html.

For the list of MIBs that Cisco ASR 901 router supports, see the Release Notes for Cisco ASR 901 router.

Manageability Features

- Address Resolution Protocol (ARP) for identifying a router through its IP address and its corresponding MAC address.
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the router and other Cisco devices on the network (supported on NNIs by default, can be enabled on ENIs, not supported on UNIs).
- Network Time Protocol (NTP) for providing a consistent time stamp to all routers from an external source.
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the router uses.
- In-band management access for up to five simultaneous Telnet connections for multiple CLI-based sessions over the network. Effective with Cisco IOS Release 15.3(2)S1, in-band management access for up to 98 simultaneous Telnet connections for multiple CLI-based sessions over the network.
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network.
- In-band management access through SNMP Versions 1 and 2c get and set requests.
- Out-of-band management access through the router console port to a directly attached terminal or to a remote terminal through a serial connection or a modem.
- User-defined command macros for creating custom router configurations for simplified deployment across multiple routers.
- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge devices, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback (requires the metro IP access or metro access image).
- Configuration replacement and rollback to replace the running configuration on a router with any saved Cisco IOS configuration file.
- CPU utilization threshold logs.

Security Features

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes.

- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process.
- Multilevel security for a choice of security level, notification, and resulting actions.
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs or ENIs.
- TACACS+, a proprietary feature for managing network security through a TACACS server.
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services.
- Extended IP access control lists for defining security policies in the inbound direction on physical ports.
- Extended IP access control lists for defining security policies in the inbound and outbound direction on SVIs.

Quality of Service and Class of Service Features

- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue.
- Cisco modular quality of service (QoS) command-line (MQC) implementation
- Classification based on IP precedence, Differentiated Services Code Point (DSCP), and IEEE 802.1p class of service (CoS) packet fields, or assigning a QoS label for output classification
- Policing
    - One-rate policing based on average rate and burst rate for a policer
    - Two-color policing that allows different actions for packets that conform to or exceed the rate
    - Aggregate policing for policers shared by multiple traffic classes
- Table maps for mapping CoS, and IP precedence values
- Queuing and Scheduling
    - Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
    - Port shaping to specify the maximum permitted average rate for a port
    - Class-based weighted queuing (CBWFQ) to control bandwidth to a traffic class
    - Low-latency priority queuing to allow preferential treatment to certain traffic
- Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface.

Layer 3 Features

- IP routing protocols for load balancing and for constructing scalable, routed backbones:
    - OSPF

  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, and BGP routing protocols

- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets

Layer 3 VPN Services

These features are available only when the router is running the Advance Metro IP services.

- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs.
- MPLS VPN is supported.

Monitoring Features

- Router LEDs that provide port- and router-level status
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Enhanced object tracking for HSRP clients (requires metro IP access image)
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring (requires metro IP access or metro access image)
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover (requires metro IP access or metro access image)
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down (requires metro IP access or metro access image)
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy (requires metro IP access or metro access image)

CHAPTER 2

Licensing

This feature module describes the licensing aspects of the Cisco ASR 901 Series Aggregation Services Router.

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 Licensing, on page 21.

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.

Feature Overview

The Cisco ASR 901 router license is similar to any other software license in Cisco. It is tied to the Unique Device Identifier (UDI) —where the license is integrated to the PID (Product Identifier) and SN (Serial Number). A license generated for one router cannot be shared or installed in any other router.

Complete these steps to obtain the license file:

1. Purchase the required Product Authorization Key (PAK).
2. Get the UDI from the device.
3. Enter the UDI and PAK in the Cisco's licensing portal.

You will receive a license file through email.

1. Install the licenses on the device. For more information on how to install the license, see Installing the License , on page 19.

In addition to using the router CLI, you can install the license using the Cisco License Manager (CLM) or the Callhome interface.

Licenses Supported on Cisco ASR 901 Router

The following licenses are supported:

Sl.No.	Chassis PID	License PID	License Description	License Type (Image or Feature)
1	A901-12C-FT-D A901-12C-F-D A901-4C-FT-D A901-4C-F-D A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D A901-6CZ-FS-A A901-6CZ-FS-D	SL-A901-A	AdvancedMetroIPAccess	Image
2	A901-12C-F-D A901-12C-FT-D A901-4C-FT-D A901-4C-F-D A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D A901-6CZ-FS-A A901-6CZ-FS-D	SL-A901-B	IPBase	Image (by default gets enabled)

Sl.No.	Chassis PID	License PID	License Description	License Type (Image or Feature)
3	A901-4C-FT-D A901-4C-F-D	FLS-A901-4S FLS-A901-4S= 1 L-FLS-A901-4S= 1	Gige4SfpUpgrade	Feature
4	A901-4C-FT-D A901-4C-F-D	FLS-A901-4T FLS-A901-4T= 1 L-FLS-A901-4T= 1	Gige4CuUpgrade	Feature
5	A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D A901-6CZ-FS-A A901-6CZ-FS-D	FLS-A901-2Z FLS-A901-2Z= 1 L-FLS-A901-2Z= 1	10gigUpgrade	Feature
6	A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D A901-6CZ-FS-A A901-6CZ-FS-D	FLS-A901-4 FLS-A901-4= 1 L-FLS-A901-4= 1	Gige4portflexi	Feature
7	A901-12C-FT-D A901-12C-F-D A901-4C-FT-D A901-4C-F-D A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D A901-6CZ-FS-A A901-6CZ-FS-D	SL-A901-T	1588BC	Feature
8	A901-6CZ-FS-A A901-6CZ-FS-D	SL-A901-I SL-A901-I= L-SL-A901-I=	IPsec NAT	Feature

1 = variants are spares or represent the e-paper form.

The Cisco ASR 901 software uses the license description to resolve errors related to license availability. You need to map the proper license PID as per the table above and purchase the licenses. The Cisco ASR 901 router supports permanent licenses only.

Note You can configure NAT and IPsec features on the router (A901-6CZ-FS-A and A901-6CZ-FS-D) without a valid license. The router issues a warning message and allows you to configure the feature. A warning message regarding the unlicensed feature is flashed every hour. However, this will not have any impact on the functionality.

You should install only a supported license for the proper chassis PID. You will get a “Not Supported” message while trying to install a wrong license. However, license installation process will go through and a confirmation message is displayed. When you run the **show license** command to display the details of this license, the output shows license state as “NOT IN USE”, and you cannot make it “IN USE”.

The following is a sample confirmation message that is displayed on the router when you try to install a wrong license.

```
Install FLS-A901-4S  license on A901-6CZ-F-A  (10g) boards,
Router# license install flash:CAT1625U0EP_201307231358341640.lic
Installing licenses from "flash:CAT1625U0EP_201307231358341640.lic"
Installing...Feature:Gige4SfpUpgrade...Successful:Not Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

License Types

Cisco ASR 901 router supports the following types of licenses:

- Image Level License
- Feature Based License

Image Level License

An Image level license corresponds to the level of the IOS image that comes up based on the licenses present on the router. This license is enforced while booting and it uses a universal image. It activates all the subsystems corresponding to the license that you purchased. Image based licenses (SL-A901-A and SL-A901-B) need rebooting of the router.

Features Supported

In Cisco ASR 901 , IPBase (SL-A901-B) and AdvancedMetroIPAccess (SL-A901-A) are permanent; once installed they do not expire. Trial or temporary licenses are not supported on the Cisco ASR 901 router.

License	Features
IPBase / SL-A901-B	• L2, EVC, 802.1Q, 802.1ad, QinQ, 802.3ah, H-Qos, IPv4 static routes, routing protocols, host connectivity, ACL, REP, VRF-Lite • E-OAM—CFM (BD, port level), IPSLA (barring LSP) • Clocking—SyncE, 1588-OC Slave, 10M, 1PPS/ToD, G.781 Priority based Clock Selection (no ESMC/SSM) **Note** Time-division multiplexing (TDM) is unavailable.
AdvancedMetroIPAccess / SL-A901-A	• All IPBase license features • MPLS—MPLS, L2VPN (EoMPLS), L3VPN, MPLS OAM, PW redundancy • E-OAM—IPSLA(LSP) • TDM —IPoPPP/HDLC, QoS, CESoPSNoMPLS, PPP/HDLCoMPLS, Clock Recovery from TDM interfaces, Y.1731PM

Feature Based License

Feature based licenses are licenses used to activate individual features once the image level licenses are used. Once the image level license is used and the appropriate subsystems are activated. Individual feature licenses are used to activate individual features. These include:

- Port based licenses

  This license applies to the Ethernet ports of the Cisco ASR 901 series routers. Copper and SFP are applicable only to A901-4C-XX-X PIDs, Flexi and 10G licenses are applicable to A901-6CZ-XX-X PID.

  - Copper license
  - SFP license
  - Flexi license
  - 10G license

- 1588BC license
- IPsec/NAT-PAT license

Note Copper (FLS-A901-4T), SFP (SL-A901-B), and 1588BC (SL-A901-T) licenses are feature-based licenses. Once they are installed, the licenses become active and there is no need to reboot the router.

Port Based/Mode License

The following table lists the port number, type, and the required license for those ports:

Port Number	Port Type	Chassis PID	License PIDs
0-3	Copper	A901-4C-FT-D A901-4C-F-D	FLS-A901-4T

Port Number	Port Type	Chassis PID	License PIDs
4-7	Combo		No license is required. These ports are enabled by default.
8-11	Small Form-Factor Pluggable(SFP)	A901-4C-FT-D A901-4C-F-D	FLS-A901-4S
0-3 and 8-11	Copper and SFP	A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D	FLS-A901-4
TenGig0/1, TenGig0/2	SFP+	A901-6CZ-FT-A A901-6CZ-FT-D A901-6CZ-F-A A901-6CZ-F-D	FLS-A901-2Z

By default, ports 4 to 7 are enabled on the router. When you purchase the copper or SFP port license, the corresponding ports are only enabled. Copper and SFP port licenses can co-exist.

1588BC License

1588BC (SL-A901-T) license is a feature based license. This license does not need rebooting of the router for activation. The following table lists the features supported

License PID	Features
SL-A901-T	Clocking—1588V2 PTP boundary clock

Port or Interface Behavior

The following sections describe the port or interface behavior of the licenses:

Port Based License

When a port based license is not present, ports 4 to 7 are enabled. Ports 0 to 3, and ports 8 to 11 are disabled. This is the expected behavior. Interfaces that are disabled are in the administrative down state.

Example: When Port Based License is not Installed

The following error message appears when the port based license is not installed and you use the **no shutdown** command on the interface:

```
Router# show ip interface brief

Interface               IP-Address      OK? Method Status                Protocol
```

```
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
GigabitEthernet0/3     unassigned      YES unset  administratively down down
GigabitEthernet0/4     unassigned      YES unset  down                  down
GigabitEthernet0/5     unassigned      YES unset  down                  down
GigabitEthernet0/6     unassigned      YES unset  down                  down
GigabitEthernet0/7     unassigned      YES unset  down                  down
GigabitEthernet0/8     unassigned      YES unset  administratively down down
GigabitEthernet0/9     unassigned      YES unset  administratively down down
GigabitEthernet0/10    unassigned      YES unset  administratively down down
GigabitEthernet0/11    unassigned      YES unset  administratively down down
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  down                  down
Router#
Router(config-if)# interface gig 0/0
Router(config-if)# no shutdown

 Router(config-if)#
*Oct  5 14:22:27.743: %LICENSE-1-REQUEST_FAILED: License request for feature fls-a901-4t
1.0 failed. UDI=MWR-3941:FHAK13101A1

Router# show interface gigabitEthernet 0/0

GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
.......
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 RJ45
  output flow-control is unsupported, input flow-control is unsupported
  LICENSE not available! Interface disabled
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
```

Example: When Port Based License is Installed

The following example shows how to install the port based license:

```
Router# license install flash:FHAK13101A1_20110811190230024_fls-a901-4t.lic

Installing licenses from "flash:FHAK13101A1_20110811190230024_fls-a901-4t.lic"
Installing...Feature:Fls-a901-4t...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
Router#*Oct  5 17:23:14.487: %LICENSE-6-INSTALL: Feature Fls-a901-4t 1.0 was installed in
this device. UDI=MWR-3941-TEST:FHAK13101A1; StoreIndex=2:Primary License Storage
Router(config)# interface gig 0/0
Router(config-if)# no shutdown
```

When the port based license is installed for copper or SFP ports, the corresponding ports are enabled. Following is a sample output from the **show ip interface** command:

```
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
```

```
GigabitEthernet0/2     unassigned      YES unset  administratively down down
.....
```

Note Combo ports are either copper or SFP ports depending on the configuration specified in the **media-type** command.

10gigUpgrade License

When you do not have the 10gigUpgrade license, the 10 Gigabit Ethernet ports are enabled in 1 Gigabit Ethernet mode. Install the 10gigUpgrade license to enable new 10 Gigabit Ethernet ports in 10Gigabit Ethernet mode. To enable 1 Gigabit Ethernet mode, 1 Gigabit Ethernet SFPs have to be used on both the ends. There is no speed command to control the speed and this depends on the type of the SFP. The 10 Gigabit Ethernet ports does not support 100M speed. You can connect 10 Gigabit Ethernet SFP+ to 10 Gigabit Ethernet ports only.

Example: When 10gigUpgrade License is not Installed

The following error message appears when the 10gigUpgrade license is not installed and you use the **show interface** command:

```
Router# show interface Ten0/1

TenGigabitEthernet0/1 is down, line protocol is down (notconnect)
  Hardware is TenGigabit Ethernet, address is 2c54.2dd6.c10e (bia 2c54.2dd6.c10e)
  MTU 9216 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown, Unknown, media type is H10GB-CU3M
  output flow-control is unsupported, input flow-control is unsupported
  LICENSE not available or 1G SFP ( Interface in 1G mode )
  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: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 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, 0 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
```

Example: When 10gigUpgrade License is Installed

The following example shows how to install the 10gigUpgrade license:

```
Router# license install flash:10G-ac.lic

Installing licenses from "flash:10G-ac.lic"
Installing...Feature:10gigUpgrade...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

Following is a sample output from the **show license** command:

```
Router# show license

Index 1 Feature: AdvancedMetroIPAccess
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: IPBase
Index 3 Feature: Gige4portflexi
Index 4 Feature: 10gigUpgrade
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
```

Flexi License

When a flexi license is not present, ports 4 to 7 are enabled. Ports 0 to 3, and ports 8 to 11 are disabled. This is the expected behavior. Interfaces that are disabled are in the administrative down state.

FLS-A901-4 flexi license is a combination of copper and SFP ports. This license is not tied to any port types. If you purchase a single FL-A901-4 license and install it, four ports are enabled and if you have two licenses, all the eight ports are enabled. You can purchase and install two flexi licenses in a router.

Flexi license is also called Count-based license, with a maximum count of two. In a normal license, if the license is already installed and when you try to install the same license again, the installation fails and router displays *Duplicate License* error message. With flexi license (as it is count based), you can install the same license twice. Anything above this will throw an error.

Note Flexi license is supported only on the Cisco ASR 901 10G Router.

Example: When Flexi License is not Installed

The following error message appears when the flexi license is not installed and you use the **show ip interface** command on the interface:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
```

```
GigabitEthernet0/3     unassigned      YES unset  administratively down down
GigabitEthernet0/4     unassigned      YES unset  down                  down
GigabitEthernet0/5     unassigned      YES unset  down                  down
GigabitEthernet0/6     unassigned      YES unset  down                  down
GigabitEthernet0/7     unassigned      YES unset  down                  down
GigabitEthernet0/8     unassigned      YES unset  administratively down down
GigabitEthernet0/9     unassigned      YES unset  administratively down down
GigabitEthernet0/10    unassigned      YES unset  administratively down down
GigabitEthernet0/11    unassigned      YES unset  administratively down down
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  down                  down
```

Example: When Flexi License is Installed

Following is a sample output from the **show license** command:

```
Router# show license
Index 1 Feature: AdvancedMetroIPAccess
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: IPBase
Index 3 Feature: Gige4portflexi                    Version: 1.0
        License Type: Permanent
        License State: Active, Not In Use
        License Count: 2/0/0  (Active/In-use/Violation)
        License Priority: Medium
        Store Index: 1
        Store Name: Primary License Storage
```

1588BC License

When the SL-A901-T 1588BC license is not installed, the PTP boundary clock cannot be configured. For more information on configuring the PTP boundary clock, see PTP Boundary Clock, on page 330.

Example: When 1588BC License is not Installed

The following error message appears on configuring the PTP boundary clock, when the 1588BC license is not installed:

Note Though an error message appears on configuring the PTP boundary clock, the running-config file accepts the PTP boundary clock configuration. This configuration can be saved. However, the PTP boundary clock is not configured in the hardware, and is inactive.

```
Router(config)# ptp clock boundary domain 0

%ERROR: Boundary Clock needs a separate license. Please install license and reconfigure
PTP.
Router(config-ptp-clk)#
```

Example: When 1588BC License is Installed

The following example shows how to install the 1588BC license:

```
Router# license install flash:CAT1632U029_20121005013805577.lic

Installing licenses from "flash:CAT1632U029_20121005013805577.lic"
Installing...Feature:1588BC...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

Following is a sample output from the **show license** command:

> **Note** When the 1588BC license is installed and PTP boundary clock is not configured, the license state is displayed as Active, Not in Use . When the 1588BC license is installed and PTP boundary clock is configured, the license state is displayed as Active, In Use .

```
Router# show license

Index 1 Feature: AdvancedMetroIPAccess
Index 2 Feature: IPBase
Index 3 Feature: Gige4portflexi
Index 4 Feature: 10gigUpgrade
Index 5 Feature: 1588BC
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
```

Removing the License

If PTP boundary clock is configured, then the following error message appears when removing the 1588BC license:

> **Note** Removing license is mainly used for development purpose.

```
Router# yes
Feature: 1588BC
        License Type: Permanent
        License State: Active, In Use
        License Addition: Exclusive
        License Count: Non-Counted
        Comment:
        Store Index: 2
        Store Name: Primary License Storage
Are you sure you want to clear? (yes/[no]): &;
Handling Event, Unknown event type: 3
% Error: Could not delete in-use license
```

Complete the following steps to remove the license.

Procedure

Step 1 Use the **yes** command to remove the PTP boundary clock configuration.

Router(config-ptp-clk)# **yes**

Step 2 Use the **license clear** command to remove the 1588BC license.

Router# **yes**

Feature: 1588BC

License Type: Permanent

License State: Active, Not in Use

License Addition: Exclusive

License Count: Non-Counted

Comment:

Store Index: 3

Store Name: Primary License Storage

Are you sure you want to clear? (yes/[no]): &;

Generating the License

Complete the following steps to generate the license:

Procedure

Step 1 Use the **show license udi** command on the router

Step 2 Save the output.

The output contains the UDI with the Product Identifier (PID) and Serial Number (SN).

Step 3 Go to the SWIFT tool at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.

Step 4 Enter the PAK and UDI.

Step 5 Click **Submit**.

You will receive the license file through email.

Installing the License

Complete the following steps to install the license:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**license install ?** **Example:** `Router# license install ?`	(Optional) License can be installed either by placing the license file in the tftp boot directory or by copying the license to the flash: directory.
Step 3	**copy tftp: flash:** **Example:** `Router# copy tftp: flash:`	Copies the license file to the flash: directory.
Step 4	**show flash:** **Example:** `Router# show flash:`	Displays the contents of the flash: directory.
Step 5	**license install** &; **Example:** `Router# license install FHK10LLL021_20110530015634482.lic`	Installs the license from the flash: directory.
Step 6	**reload** **Example:** `Router# reload`	Reboots the system to activate the new license. **Note** The license is activated after installation. Rebooting the router is required only for AdvancedMetroIPAccess.

Changing the License

The **license boot level** command is used only to select the required image-based licensing. For the Cisco ASR 901 Series Routers, only one image based license (AdvancedMetroIPAccess) is available. Installing this license and reloading the router takes care of this license. If the license install does not work properly, use the **license boot level** command for AdvancedMetroIPAccess in the global configuration mode, to change the license and reboot the system to activate the new license.

Note If you do not install a license, the router starts with the lowest level license by default.

Note After installing the AdvancedMetroIPAccess license and reloading the router, the AdvancedMetroIPAccess license will be activated by default.

Verifying the License

To verify the new license, use the **show license** command.

```
Router# show license
Index 1 Feature: AdvancedMetroIPAccess
    Period left: Lifetime
    License Type: Permanent
    License State: Active, In Use
    License Priority: High
    License Count: 1/1/0  (Active/In-use/Violation)

Index 2 Feature:.....
    Period left: 0  minute  0  second
```

Where to Go Next

For additional information on Licensing, see the documentation listed in the Additional References section.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference
Cisco Software Licensing Concepts	Cisco IOS Software Activation Conceptual Overview

Related Topic	Document Title
Cisco ASR 901 Software Configuration Guide	Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	

Technical Assistance

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

Feature Information for Licensing

The following table lists the release history for this feature and provides links to specific configuration information.

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 following table 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 1: Feature Information for Licensing

Feature Name	Releases	Feature Information
Licensing	15.2(2)SNH1	The following sections provide information about this feature: • Licenses Supported on Cisco ASR 901 Router, on page 8 • License Types, on page 10 • Port or Interface Behavior, on page 12 • Generating the License, on page 18 • Installing the License , on page 19 • Changing the License, on page 19 • Return Materials Authorization License Process
1588BC Licensing	15.2(2)SNI	The following sections provide information about this feature: • Licenses Supported on Cisco ASR 901 Router, on page 8 • License Types, on page 10 • Port or Interface Behavior, on page 12
Licensing	15.4(2)S	New PIDs were added to the document.

CHAPTER 3

First-Time Configuration

This chapter describes the actions to take before turning on your router for the first time.

Setup Mode

The **setup** mode guides you through creating a basic router configuration. If you prefer to configure the router manually or to configure a module or interface that is not included in **setup** mode, go to Using the Command-Line Interface, on page 51 to familiarize yourself with the CLI.

Before Starting Your Router

Complete the following steps before you power on your router and begin using the **setup** mode:

Procedure

Step 1 Set up the hardware and connect the console and network cables as described in the “Connecting Cables” section of the Cisco ASR 901 Series Aggregation Services Router Hardware Installation Guide. .

Step 2 Configure your PC terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.

Using Setup Mode

The **setup** command facility appears in your PC terminal emulation program window. To create a basic configuration for your router, perform the following:

> **Note** If you made a mistake while using the setup command facility, exit the facility and run it again. Press Ctrl-C, and type setup at the enable mode prompt (1900#).

Configuring Global Parameters

Complete the following steps to configure global parameters.

Procedure

Step 1 Power on the router. Messages appear in the terminal emulation program window.

Caution
Do not press any keys on the keyboard until the messages stop . Any keys that you press during this time are interpreted as the first command entered after the messages stop, which might cause the router to power off and start over. Wait a few minutes. The messages stop automatically.

The messages look similar to the following:

Example:

```
System Bootstrap, Version 15.1(2r)SNG, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Compiled Tue 25-Oct-11 12:09 by tinhuang
P2020 platform with 524288 Kbytes of main memory
program load complete, entry point: 0x2000000, size: 0x1d29954
Self decompressing the image :
#########################################################################################
 [OK]
              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, 901 Software (ASR901-UNIVERSALK9-M), Version 15.1(2)SNG, RELEASE SOFTWARE
 (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 25-Oct-11 13:13 by prod_rel_team
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 ASR901-E (P2020) processor (revision 1.0) with 393216K/131072K bytes of memory.
Processor board ID CAT1529U01P
P2020 CPU at 792MHz, E500v2 core, 512KB L2 Cache
1 FastEthernet interface
12 Gigabit Ethernet interfaces
1 terminal line
```

```
256K bytes of non-volatile configuration memory.
98304K bytes of processor board System flash (Read/Write)
65536K bytes of processor board RAM Disk (Read/Write)
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

Note
The messages vary, depending on the Cisco IOS software image and interface modules in your router. This section is for reference only, and output might not match the messages on your console.

Step 2 To begin the initial configuration dialog, enter **yes** when the following message appears:

Example:

```
Would you like to enter the initial configuration dialog? [yes/no]:yes
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 3 Enter a hostname for the router (this example uses 901 -1).

Example:

```
Configuring global parameters:
 Enter host name [Router]: 901-1
```

Step 4 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration.

Example:

```
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: ciscoenable
```

Note
When you enter the enable secret password, the password is visible as you type it. Once you enter the password, it becomes encrypted in the configuration.

Step 5 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration.

Example:

```
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: ciscoenable
```

Step 6 To prevent unauthenticated access to the router through ports other than the console port, enter the virtual terminal password.

Example:

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: ciscoterminal
```

Step 7 Respond to the following prompts as appropriate for your network:

Example:

```
Configure System Management? [yes/no]: no
Configure SNMP Network Management? [yes]:
    Community string [public]: public
```

Step 8 The summary of interfaces appears. This list varies, depending on the network modules installed in your router.

Step 9 Specify the interface to be used to connect to the network management system.

Step 10 Configure the specified interface as prompted.

Completing the Configuration

When you have provided all of the information prompted for by the setup command facility, the configuration appears. Messages similar to the following appear:

```
The following configuration command script was created:
!
hostname 901-1
enable secret 5 $1$5fH0$Z6Pr5EgtR5iNJ2nBg3i6y1 enable password ciscoenable line vty 0 98
password ciscoenablesnmp-server community public !
no ip routing
!
interface GigabitEthernet0/1
shutdown
!
end
```

Complete the following steps to configure the router:

Procedure

Step 1 The setup command facility displays the following prompt.

Example:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!
```

If you answer:

- 0—The configuration information that you entered is *not* saved, and you return to the router enable prompt. To return to the system configuration dialog, enter setup.
- 1—The configuration is not saved, and you return to the EXEC prompt.

The 901-1> prompt appears indicating that you are at the CLI and you completed a basic router configuration.

Note
The basic configuration is not a complete configuration.

Step 2 When the messages stop displaying in your window, press **Return** to view the command line prompt.

Verifying the Cisco IOS Software Version

To verify the version of Cisco IOS software, use the show version command. The show version command displays the configuration of the system hardware, the software version, the names and sources of the configuration files, and the boot images.

Configuring the Hostname and Password

First configure the hostname and set an encrypted password. Configuring a hostname allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

Complete the following steps to configure a hostname and to set an encrypted password:

Procedure

Step 1 Enter enable mode.

Example:

```
Router> enable
```

The Password prompt appears. Enter your password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 2 Enter global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

When the prompt changes to Router(config) , you have entered global configuration mode.

Step 3 Change the name of the router to a meaningful name. Substitute your hostname for Router .

Example:

```
Router(config)# hostname Router
```

Step 4 Enter an enable secret password. This password provides access to privileged EXEC mode. When you type enable at the EXEC prompt (Router>), you must enter the enable secret password to access configuration mode. Enter your secret password.

Example:

```
Router(config)# enable secret secret password
```

Step 5 Exit back to global configuration mode.

Example:

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

Verifying the Hostname and Password

Complete the following steps to verify that you have correctly configured the hostname and password:

Procedure

Step 1 Enter the **show config** command:

Example:

```
Router# show config
Using 1888 out of 126968 bytes
!
version XX.X
.
.
.
!
hostname Router
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
.
.
```

Step 2 Check the hostname and encrypted password, which appear near the top of the command output.

Step 3 Exits the global configuration mode and attempt to re-enter it using the new enable password:

Example:

```
Router# exit
.
.Router con0 is now available
Press RETURN
 to get started.
Router> enable
```

```
Password: password
Router#
```

CHAPTER 4

Managing and Monitoring Network Management Features

This feature module describes how to monitor, manage and deploy a variety of network management features, including Cisco Active Network Abstraction (ANA), Simple Network Management Protocol (SNMP) and Cisco Networking Services (CNS). The CNS software agent on the Cisco ASR 901 can communicate with a Cisco Configuration Engine to allow the Cisco ASR 901 to be deployed in the field without having to pre-stage it for configuration or image upgrade. The Zero-touch deployment capability enables the Cisco ASR 901 router to auto configure itself, download an updated image, connect to the network, and start the operation as soon as it is cabled and powered up.

For more information about the Cisco Configuration Engine, see http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps4617/qa_c67_598467.html.

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 table at the end of this module.

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.

Network Management Features for the Cisco ASR 901

The following sections describe the network management features available on the Cisco ASR 901 .

Cisco Active Network Abstraction (ANA)

Cisco ANA is a powerful, next-generation network resource management solution designed with a fully distributed OSS mediation platform that abstracts the network, its topology and its capabilities from the physical elements. Its virtual nature provides customers with a strong and reliable platform for service activation, service assurance and network management. For more information about ANA, see http://www.cisco.com/en/US/products/ps6776/tsd_products_support_series_home.html .

SNMP MIB Support

To view the current MIBs that the Cisco ASR 901 supports, see http://www.cisco.com/go/mibs .

Cisco Networking Services (CNS)

Cisco Networking Services (CNS) is a collection of services that can provide remote configuration of Cisco IOS networking devices, remote execution of CLI commands, and image downloads by communicating with a Cisco Configuration Engine application running on a server. CNS enables the zero-touch deployment for the Cisco ASR 901 router by automatically downloading its configuration and upgrading its image if needed.

Note The Cisco ASR 901 only supports CNS over motherboard Ethernet interfaces.

For more information about CNS configuration, see Enabling Cisco Networking Services (CNS) and Zero-Touch Deployment, on page 38.

How to Configure Network Management Features on Cisco ASR 901

This section contains the following procedures:

Configuring SNMP Support

Use the following to configure SNMP support for

- Setting up the community access
- Establishing a message queue for each trap host
- Enabling the router to send SNMP trap messages
- Enabling SNMP trap messages for alarms
- Enabling trap messages for a specific environment.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

Complete the following steps to configure SNMP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community string** [**view** *view-name*] [**ro** | **rw**] [**number**] **Example:** `Router(config)# snmp-server community xxxxx RO`	Sets up the community access string to permit access to SNMP. The no form of this command removes the specified community string. • **string**—Community string is the password to access the SNMP protocol. • **view** *view-name*—(Optional) Previously defined view. The view defines the objects available to the community. • **ro**—(Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects. • **rw**—(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. • **number**—(Optional) Specifies an access list of IP addresses allowed to use the community string to gain access to the SNMP agent. Values range from 1 to 99.
Step 4	**snmp-server queue-length** *length* **Example:** `Router(config)# snmp-server queue-length 100`	Establishes the message queue length for each trap host. • *length*—Specifies the number of trap events that can be held before the queue must be emptied.

	Command or Action	Purpose

Step 5	**snmp-server enable traps** [*notification-type*] [*notification-option*]
	Example:
	`Router(config)# snmp-server enable traps`
	`snmp linkdown linkup coldstart warmstart`
		Enables the router to send SNMP traps messages. Use the no form of this command to disable SNMP notifications.
		• *notification-type*—**snmp** [**authentication**] —Enables RFC 1157 SNMP notifications. Note that use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command globally enable (or, if using the no form, disable) the following SNMP traps:
		  • authentication failure
		  • linkup
		  • linkdown
		  • coldstart
		  • warmstart
		• *notification-option*—(Optional) **atm pvc** [**interval** *seconds*] [**fail-interval***seconds*]—The optional interval seconds keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30.
		The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0.

Step 6	**snmp-server enable traps envmon** **Example:** `Router(config)# snmp-server enable traps envmon`	Enables SNMP trap messages for a specific environment. • **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]—When the envmon keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords:

	Command or Action	Purpose
		voltage, shutdown, supply, fan, and temperature.

Step 7	**snmp-server host** *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**notification-type**]
	
	Example:
	
	`Router(config)# snmp-server host 10.20.30.40 version 2c`
		Specifies the recipient of an SNMP trap messages. To remove the specified host, use the no form of this command.
		• *host-address* **traps envmon** host-address—Name or Internet address of the host (the targeted recipient).
		• **traps**—Sends SNMP trap messages to this host. This is the default.
		• **informs**—(Optional) Sends SNMP informs to this host.
		• **version**—(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model because allows packet encryption with the priv keyword. If you use the version keyword, one of the following must be specified:
		  • **1**—SNMP version 1. This option is not available with informs.
		  • **2c**—SNMP version 2C.
		  • **3**—SNMP version 3. The following three optional keywords can follow the version 3 keyword:
		• **auth**–(Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
		• **noauth**–(Default). The no authentication-no privileges security level is the default if the auth | noauth | priv] keyword choice is not specified.
		• **priv**–(Optional). Enables Data Encryption Standard (DES) packet encryption.
		• *community-string*—Password-like community string sent with the notification operation. Though you can set this string using the snmp-server host command by itself, we recommend you define this string using the snmp-server community command before using the snmp-server host command.
		• *port*—UDP port of the host. The default value is 162.
		• **notification-type**—(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent.

	Command or Action	Purpose
		The notification type can be one or more of the following keywords: • **aaa_server**—Enables SNMP AAA Server traps. • **config**—Enables SNMP config traps. • **config-copy**—Enables SNMP config-copy traps. • **cpu**—Allow cpu related traps. • **ds1**—Enables SNMP DS1 traps. • **eigrp**—Enables SNMP EIGRP traps. • **entity**—Enables SNMP entity traps. • **envmon**—Enables SNMP environmental monitor traps. • **flash**—Enables SNMP FLASH notifications. • **frame-relay**—Enables SNMP frame-relay traps. • **hsrp**—Enables SNMP HSRP traps. • **ipmulticast**—Enables SNMP ipmulticast traps. • **ipsla**—Enables SNMP IP SLA traps. • **12tun**—Enables SNMP L2 tunnel protocol traps. • **mpls**—Enables SNMP MPLS traps. • **msdp**—Enables SNMP MSDP traps. • **mvpn**—Enables Multicast Virtual Private Networks traps. • **ospf**—Enables OSPF traps. • **pw**—Enables SNMP PW traps. • **rsvp**—Enables RSVP flow change traps. • **snmp**—Enables SNMP traps. • **syslog**—Enables SNMP syslog traps. • **tty**—Enables TCP connection traps. • **vrrp**—Enables SNMP vrrp traps.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring Remote Network Management

Complete the following steps to configure remote network management on the Cisco ASR 901 router:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip host** *host-name ip-address* **Example:** `Router(config)# ip host om-work 10.0.0.1`	Assigns a host name to each of the network management workstations, where hostname is the name assigned to the Operations and Maintenance (OAM) workstation and ip_address is the address of the network management workstation.
Step 4	**interface loopback** *number* **Example:** `Router(config-if)# interface loopback 5005`	Creates a loopback interface for OAM.
Step 5	**ip-address** *ip-address subnet-mask* **Example:** `Router(config-if)# ip-address 10.10.12.10 23`	Configures the interval at which packets are sent to refresh the MAC cache when HSRP is running.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.
Step 7	**snmp-server host hostname [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port** *port***] [notification-type]** **Example:** `Router(config)# snmp-server host snmp1 version 3 auth`	Specifies the recipient of a Simple Network Management Protocol (SNMP) notification operation. The hostname is the name assigned to the Cisco Info Center workstation with the *ip host* command in Step 3.
Step 8	**snmp-servercommunity public ro** **Example:**	Specifies the public SNMP community name.

	Command or Action	Purpose
	`Router(config)# snmp-server community snmppubliccom RO`	
Step 9	**snmp-servercommunity private rw** **Example:** `Router(config)# snmp-server community snmpprivatecom RW`	Specifies the private SNMP community name.
Step 10	**snmp-serverenable traps** **Example:** `Router(config)# snmp-server enable traps`	Enables the transmission of SNMP traps messages.
Step 11	**snmp-server trap-source loopback** *number* **Example:** `Router(config)# snmp-server trap-source loopback 5005`	Specifies the loopback interface from which SNMP traps messages originate, where number is the number of the loopback interface you configured for the O&M in Step 4.
Step 12	**end** **Example:** `Router(config-if)# end`	Exits global configuration mode.

Enabling Cisco Networking Services (CNS) and Zero-Touch Deployment

To enable CNS and Zero-Touch deployment, you need the following servers:

- A DHCP server (standalone or enabled on the carrier edge router)
- A TFTP server (standalone or enabled on the carrier edge router)
- A server running the Cisco Configuration Engine (formerly known as the CNS-CE server)

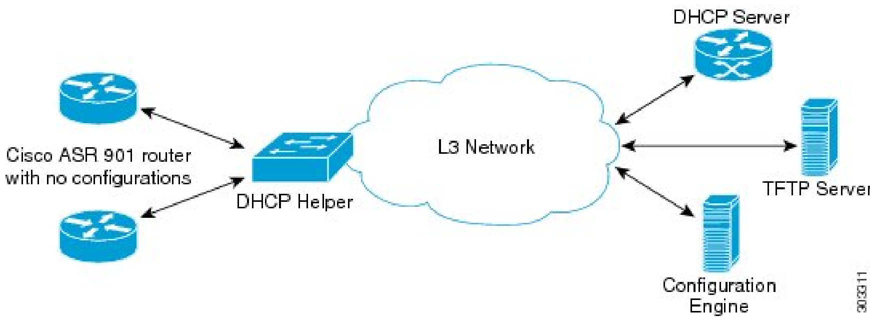
Note The Cisco ASR 901 only supports CNS over motherboard Ethernet interfaces.

This section contains the following procedures:

Zero-Touch Deployment

Zero-touch deployment feature gives the router the ability to retrieve its configuration file from the remote server during initial router deployment with no end-user intervention.

Figure 1: Zero-touch Deployment



The following steps provide an overview of events that take place during Cisco ASR 901 zero-touch deployment.

Procedure

Step 1 Connect the Cisco ASR 901 without any configurations to an upstream router.

Step 2 The Cisco ASR 901 auto-senses the management VLAN of the upstream router for IP connectivity by listening to the traffic it receives on the connected interface.

Step 3 The Cisco ASR 901 sends DHCP discover messages using the discovered VLAN tag. If the upstream router is not using a management VLAN, untagged DHCP discover messages are sent.

Step 4 The DHCP server responds with a DHCP offer.

Step 5 The Cisco ASR 901 sends a DHCP request message to the DHCP server. The DHCP server then sends the DHCP ACK message.

Note
Step 6 and 7 are used only when Option 43 is not configured.

Step 6 The Cisco ASR 901 requests **network-config** file via TFTP.

Step 7 The TFTP server sends the Cisco ASR 901 a **network-config** file.

Step 8 The Cisco ASR 901 sends an HTTP request to the CNS-CE server.

Step 9 The CNS-CE server sends a configuration template to the Cisco ASR 901 .

Step 10 Publish success event.

Image Download

The following events take place when a CNS-enabled Cisco ASR 901 downloads a new image:

Procedure

Step 1 The CNS-CE server requests inventory (disk/flash info) from the ASR 901-DC.

Step 2 The ASR 901-DC. sends an inventory.

Step 3 The CNS-CE server sends an image location.

Step 4 The ASR 901-DC. sends a TFTP image request.

Step 5 The ASR 901-DC. downloads an image from the TFTP server.

Step 6 Refresh the CNS-CE server to check whether the image download is complete.

Step 7 Associate the .inv template in the CNS-CE server. Based on the boot variable, the Cisco ASR 901 reboots with the copied image.

Step 8 The CNS-CE server reboots the ASR 901-DC. router.

Configuring a DHCP Server

The Cisco ASR 901 requires a DHCP server for zero-touch deployment. Complete the following steps to configure a Cisco router as a DHCP server.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp excluded-address** *dhcp-server-ip-address* **Example:** `Router# ip dhcp excluded-address 30.30.1.6`	Specifies to exclude IP address of the DHCP server.
Step 4	**ip dhcp excluded-address** *ip-address subnet-mask* **Example:** `Router# ip dhcp excluded-address 30.30.1.20 30.30.1.255`	Assigns IP addresses with an exception of 30.30.1.6, which is the IP address of the DHCP server.
Step 5	**ip dhcp pool** *pool-name* **Example:** `Router# ip dhcp pabudhcp2`	Specifies the DHCP pool name.
Step 6	**network** *ip-address subnet-mask* **Example:**	Specifies the IP address and subnet mask of the network.

	Command or Action	Purpose
	`Router# network 160.100.100.0 255.255.255.252`	
Step 7	**default-router** *ip-address* **Example:** `Router# default-router 30.30.1.6`	Specifies the IP address of the default router.
Step 8	Do one of the following: • **option 43 ascii string** • **option 150 ip** <*TFTP-server-ip-address*> **Example:** `Router# option 43 ascii 3A1D;A3;B161.100.100.2`	Specifies Option 43 and a string value that has the CNS details, serial number of the hardware, and the code for CE IP address or Option 150 and the IP address of the TFTP server. For more information on Option 43, see Constructing a DHCP Option 43 Message. Cisco ASR 901 Series Routers supports only few letter code options mentioned in this link.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

Configuring a TFTP Server

You need to set up a TFTP server to provide a bootstrap configuration to the Cisco ASR 901 routers when they boot using option 150.

Creating a Bootstrap Configuration

Create or download a file with the initial bootstrap configuration on the TFTP server. An example of the configuration file is shown below:

```
hostname test-router
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
!
end
```

Enabling a TFTP Server on the Edge Router

The Cisco ASR 901 requires a TFTP server for zero-touch deployment while using option 150. The TFTP server is typically implemented on the carrier edge router. You can use the following global configuration commands to enable a TFTP server on the edge router that can send the initial configuration to the Cisco ASR 901 router.

```
tftp-server sup-bootflash:network-confg
```

After the Cisco ASR 901 boots with this configuration, it can connect to the CNS-CE server.

Configuring the Cisco Configuration Engine

The Cisco Configuration Engine (formerly known as the Cisco CNS Configuration Engine) allows you to remotely manage configurations and IOS software images on Cisco devices including the Cisco ASR 901 .

When the Cisco ASR 901 downloads the bootstrap configuration and connects to the Cisco Configuration Engine server, you can use the server to download a full configuration to the router. You can also use the CNS-CE server to complete any of the following tasks:

- Manage configuration templates—The CNS-CE server can store and manage configuration templates.
- Download a new image—You can use the CNS-CE server to load a new IOS image on a Cisco ASR 901 router.
- Loading a new config—You can use the CNS-CE server to load a new configuration file on a Cisco ASR 901 router.
- Enable identification—You can use a unique CNS agent ID to verify the identity of a host device prior to communication with the CNS-CE server.
- Enable authentication—You can configure the CNS-CE server to require a unique password from the Cisco ASR 901 router as part of any communication handshake.
- Enable encryption—You can enable Secure Socket Layer (SSL) encryption for the HTTP sessions between the CNS agent devices (Cisco ASR 901 routers) and the CNS-CE server.

For instructions about how to use the CNS-CE server, see the *Cisco Configuration Engine Installation & Configuration Guide* at http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html .

Configuration Examples

This section provides the following configuration examples:

Example: Configuring SNMP Support

```
!
snmp-server community xxxxx RO
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps envmonsnmp-server host 10.20.30.40 version 2c
!
```

Example: Configuring Remote Network Management

```
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
```

```
cns id hostname image
cns exec 80
logging buffered 20000
!
end
```

Example: Configuring a DHCP Server

```
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool asrdhcp
network 30.30.1.0 255.255.255.0
default-router 30.30.1.6
Option 43 ascii 3A1D;A3;B161.100.100.2
!
end
```

Example: Zero-touch Deployment

The following configuration example sets the Cisco ASR 901 to boot using configurations stored on a CNS–CE server with the IP address 30.30.1.20.

Note This section provides partial configurations intended to demonstrate a specific feature.

```
hostname 901
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
!
end
```

Alarm Port Monitoring

External Alarm Port Monitoring

The Cisco ASR 901 Series Routers supports an external alarm port (RJ45 connector) that serves four external dry-contact alarm inputs. You can connect up to four alarm inputs from external devices, such as a door, a temperature gauge, or a fire alarm, to the alarm input port on the front panel of the router. You can use the IOS command to set the alarm severity to minor, major, or critical. An alarm generates a system message.

The alarm setting is open or closed.

- Open means that the normal condition has current flowing through the contact (referred to as *normally closed* contact). The alarm is generated when the current stops.

- Closed means that no current flows through the contact (referred to as *normally open* contact). The alarm is generated when the current flows.

The alarm status is polled every second to check if there are any changes in the alarm state (based on the user configuration).

Note External alarm port monitoring is disabled by default. CISCO-ENTITY-ALARM-MIB (Oid: 1.3.6.1.4.1.9.9.138: ceAlarmAsserted trap OID -- 1.3.6.1.4.1.9.9.138.2.0.1 and ceAlarmCleared trap OID -- 1.3.6.1.4.1.9.9.138.2.0.2) is used for Alarms.

Enabling Alarms

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**alarm-contact** *contact-number* **description** *description-string* **Example:** `Router(config)# alarm-contact 1 description doorsensor`	Configures a description for the alarm contact number. • The contact-number can be from 1 to 4. • The description string can be up to 48 alphanumeric characters in length and is included in any generated system messages. **Note** To disable this configuration, use the **no** form of the command.
Step 4	**alarm-contact** { *contact-number* | **all** {**severity**{**critical**| **major**| **minor**}} **Example:** `Router(config)# alarm-contact 2 severity major`	Configure 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. **Note**

	Command or Action	Purpose
		To disable this configuration, use the **no** form of the command.
Step 5	**alarm-contact** { *contact-number* | **all** { **trigger** {**closed**| **open**}} **Example:** `Router(config)# alarm-contact 2 trigger closed`	Configure the trigger for an alarm contact number or for all contact numbers. • For trigger, enter open or closed. If you do not configure a trigger, the alarm is triggered when the circuit is closed. **Note** To disable this configuration, use the **no** form of the command.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Enabling Syslogs

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**logging alarm** *severity* **Example:** `Router(config)# logging alarm informational`	Enables the system to send alarm messages to logging devices and to configure the alarm severity threshold.
Step 4	**logging host** *ip-address* **Example:** `Router(config)# logging host syslogServerIp`	Logs system messages and debug output to a remote host.
Step 5	**ip route** *dest-ip-address subnet-mask default-gateway* **Example:**	Configure the static routes.

	Command or Action	Purpose
	`Router(config)# ip route 7.0.0.221 255.255.255.255 7.47.0.1`	
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Enabling SNMP Traps

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server manager** **Example:** `Router(config)# snmp-server manager`	Starts the Simple Network Management Protocol (SNMP) manager process.
Step 4	**snmp-server community** *string* **rw** **Example:** `Router(config)# snmp-server community public rw`	Configures the community access string to permit access to the SNMP.
Step 5	**snmp-server enable traps alarms** *notification-option* **Example:** `Router(config)# snmp-server enable traps alarms informational`	Enables the traps related to alarms. • Severity - 1 is a critical event that affects the service condition. • Severity - 2 is a major event that requires immediate attention. • Severity - 3 is a minor event to indicate warning conditions. • Severity - 4 is meant for informational notifications.
Step 6	**snmp-server host** *host-name ip-address* **version 2c public udp-port** *port notification-type*	Specifies the recipient of a SNMP notification operation.

	Command or Action	Purpose
	Example: `Router(config)# snmp-server host server ip version 2c public udp-port port num`	
Step 7	**ip route** *dest-ip-address subnet-mask default-gateway* **Example:** `Router(config)# ip route 7.0.0.221 255.255.255.255 7.47.0.1`	Configure the static routes.

Verifying Alarm Configuration

To verify the alarm configuration, use the **show** commands as shown in the examples below:

```
Router#  show environment alarm-contact

ALARM CONTACT 1
   Status:      not asserted
   Description: test_1
   Severity:    critical
   Trigger:     open
ALARM CONTACT 2
   Status:      not asserted
   Description: door sensor
   Severity:    major
   Trigger:     closed
ALARM CONTACT 3
   Status:      not asserted
   Description: flood sensor
   Severity:    critical
   Trigger:     closed
ALARM CONTACT 4
   Status:      not asserted
   Description:
   Severity:    critical
   Trigger:     closed
```

```
Router#  show running-config | include alarm

alarm-contact 1 description AC Fail
alarm-contact 1 severity critical
alarm-contact 1 trigger closed
alarm-contact 2 description DC Fail
alarm-contact 2 trigger closed
alarm-contact 3 description Junk 3
alarm-contact 3 severity major
alarm-contact 3 trigger closed
alarm-contact 4 description Test 4
alarm-contact 4 severity critical
alarm-contact 4 trigger closed
```

```
Router#   show facility-alarm status
```

```
Source                  Time                 Severity        Description [Index]
------                 ------               --------        -------------------
AC Fail               Jul 22 2014 18:23:45    CRITICAL       AC Fail [0]
DC Fail               Jul 22 2014 18:23:45    MINOR          DC Fail [1]
Junk 3                Jul 22 2014 18:23:45    MAJOR          Junk 3 [2]
Test 4                Jul 22 2014 18:23:46    CRITICAL       Test 4 [3]


Router#   show environment all | b Alarms

External Alarms:
ALARM CONTACT 1 is not asserted
ALARM CONTACT 2 is not asserted
ALARM CONTACT 3 is not asserted
ALARM CONTACT 4 is not asserted
```

Where to Go Next

For additional information on monitoring and managing the Cisco ASR 901 router, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for Monitoring and Managing the Cisco ASR 901 Router

Table 2: Feature Information for Monitoring and Managing the Cisco ASR 901 Router, on page 50 lists the release history for this feature and provides links to specific configuration information.

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 Table 2: Feature Information for Monitoring and Managing the Cisco ASR 901 Router, on page 50 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 2: Feature Information for Monitoring and Managing the Cisco ASR 901 Router

Feature Name	Releases	Feature Information
Monitoring and Managing the Cisco ASR 901 Router	15.2(2)SNI	The following sections provide information about this feature: • Network Management Features for the Cisco ASR 901 , on page 32 • How to Configure Network Management Features on Cisco ASR 901 , on page 32
Dry Contact Alarm Port	15.5(1)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 5

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure the Cisco ASR 901 router.

Understanding Command Modes

The Cisco IOS user interface is divided into different modes. The commands depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands for each command mode.

When you start a session on the router, you begin in the user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the router reboots.

To gain access to all the commands, enter privileged EXEC mode. You need to enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. When you save the configuration, these commands are stored and used for router reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 3: Command Mode Summary, on page 52 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Router*.

For more detailed information on the command modes, see the command reference guide for this release.

Table 3: Command Mode Summary

Command Mode	Access Method	Router Prompt Displayed	Exit Method	About This Mode
User EXEC	Log in.	Router>	Use the **logout** command.	Use this mode to: • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	From user EXEC mode, use the **enable** command.	Router#	To go to user EXEC mode, use the **disable**, **exit**, or **logout** command.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	From the privileged EXEC mode, use the **configure terminal** command.	Router (config)#	To go to privileged EXEC mode, use the **exit** or **end** command, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire router.
Interface configuration	From the global configuration mode, use the **interface** command (with a specific interface).	Router (config-if)#	To go to global configuration mode, use the **exit** command. To return directly to privileged EXEC mode, press **Ctrl-Z**.	Use this mode to configure parameters for the Ethernet ports.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	Router(config-vlan)#	To go to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or use the **end** command.	Use this mode to configure VLAN parameters.
Line configuration	While in global configuration mode, specify a line by using the **line vty** or **line console** command.	Router(config-line)#	To go to global configuration mode, use the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Understanding the Help System

Enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in Table 4: Help Summary , on page 53.

Table 4: Help Summary

Command	Purpose
help	Obtain a brief description of the help system in any command mode.

*abbreviated-command-entry***?**	Obtain a list of commands that begin with a particular character string.
	For example:
	`Router# di?`
	`dir disable disconnect`

abbreviated-command-entry <**Tab**>	Complete a partial command name.
	For example:
	`Router# sh conf`
	`<tab>`
	`Router# show configuration`

?	List all commands available for a particular command mode. For example: `Router> ?`
command **?**	List the associated keywords for a command. For example: `Router> show ?`

command keyword **?**	List the associated arguments for a keyword.
	For example:
	`Router(config)# cdp holdtime ?`
	`<10-255> Length of time (in sec) that receiver must keep this packet`

Understanding Abbreviated Commands

You need to enter only enough characters for the router to recognize the command as unique.

This example shows how to use the **show configuration** privileged EXEC command in an abbreviated form:

```
Router# show conf
```

Understanding no and default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function, or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Error Messages

The following table lists some error messages that you might encounter while using the CLI to configure your router.

Table 5: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your router to recognize the command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Using Command History

The software provides a history or record of commands that you entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs as described in these sections:

Changing the Command History Buffer Size

By default, the router records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the router records during the current terminal session:

```
Router# terminal history
size
 number-of-lines
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the router records for all sessions on a particular line:

```
Router(config-line)# history

[
size
 number-of-lines
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 6: Recalling Commands , on page 55. These actions are optional.

Table 6: Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

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

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. These procedures are optional.

To disable the feature during the current terminal session, use the **terminal no history** privileged EXEC command.

To disable command history for the line, use the **no history** line configuration command.

Using Editing Features

This section contains the following the editing features that can help you manipulate the command line.

Enabling and Disabling Editing Features

Although the enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Router (config-line)# no editing
```

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Router# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Router(config-line)# editing
```

Editing Commands through Keystrokes

Table 7: Editing Commands through Keystrokes , on page 56 shows the keystrokes that you need to edit command lines. These keystrokes are optional.

Table 7: Editing Commands through Keystrokes

Capability	Keystroke[2]	Purpose
Move around the command line to make changes or corrections.	Press **Ctrl-B**, or press the left arrow key.	Move the cursor back one character.
	Press **Ctrl-F**, or press the right arrow key.	Move the cursor forward one character.
	Press **Ctrl-A**.	Move the cursor to the beginning of the command line.
	Press **Ctrl-E**.	Move the cursor to the end of the command line.
	Press **Esc B**.	Move the cursor back one word.
	Press **Esc F**.	Move the cursor forward one word.
	Press **Ctrl-T**.	Transpose the character to the left of the cursor with the character located at the cursor.

Capability	Keystroke[2]	Purpose
Recall commands from the buffer and paste them in the command line. The router provides a buffer with the last ten items that you deleted.	Press **Ctrl-Y.**	Recall the most recent entry in the buffer.
	Press **Esc Y**.	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Press the **Delete** or **Backspace** key.	Erase the character to the left of the cursor.
	Press **Ctrl-D**.	Delete the character at the cursor.
	Press **Ctrl-K**.	Delete all characters from the cursor to the end of the command line.
	Press **Ctrl-U** or **Ctrl-X**.	Delete all characters from the cursor to the beginning of the command line.
	Press **Ctrl-W**.	Delete the word to the left of the cursor.
	Press **Esc D**.	Delete from the cursor to the end of the word.
Capitalize or lower the case or capitalize a set of letters.	Press **Esc C**.	Capitalize at the cursor.
	Press **Esc L**.	Change the word at the cursor to lowercase.
	Press **Esc U**.	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Press **Ctrl-V** or **Esc Q**.	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.	Press the **Return** key.	Scroll down one line.
	Press the **Space** bar.	Scroll down one screen.

Capability	Keystroke[2]	Purpose
Redisplay the current command line if the router suddenly sends a message to your screen.	Press **Ctrl-L** or **Ctrl-R.**	Redisplay the current command line.

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

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

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

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Router(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Router(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Router(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the Editing Commands through Keystrokes, on page 56.

Searching and Filtering Output of show and more Commands

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

To use this functionality, use **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command| {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you use **exclude output** command, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Router# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Accessing the CLI

You can access the CLI through a console connection, through Telnet, or by using the browser.

Accessing the CLI through a Console Connection or through Telnet

Before accessing the CLI, you must connect a terminal or PC to the router console port and power on the router as described in the hardware installation guide that shipped with your router.

If your router is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your router must first be configured for this type of access..

You can use one of these methods to establish a connection with the router:

- Connect the router console port to a management station or dial-up modem. For information about connecting to the console port, see the router hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The router must have network connectivity with the Telnet or SSH client, and the router must have an enable secret password configured.

The router supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

The router supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

Saving Configuration Changes

To save your configuration changes to NVRAM, so that the changes are not lost during a system reload or power outage, enter the **copy running-config startup-config** command. For example:

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

It might take a few minutes to save the configuration to NVRAM. After the configuration has been saved, the following message appears:

```
[OK]
Router#
```

For additional information about using the Cisco IOS Release 15.1SNG, see the guides listed at:

http://www.cisco.com/en/US/products/ps11280/tsd_products_support_series_home.html

CHAPTER 6

Software Upgrade

This chapter explains how to upgrade the Cisco IOS image installed on the Cisco ASR 901 router.

Selecting a Cisco IOS Image

When you select the Cisco IOS image for upgrade, consider the following:

- Memory requirement—The router should have sufficient disk or flash memory to store the Cisco IOS. The router should also have sufficient memory (DRAM) to run the Cisco IOS. The recommended logging buffer in DRAM ranges from 8 kilobytes to 64 kilobytes. If the router does not have sufficient memory (DRAM), the router will have boot problems when it boots through the new Cisco IOS.
- Interfaces and modules support—You must ensure that the new Cisco IOS supports all the interfaces and modules in the router.
- Software feature support—You must ensure that the new Cisco IOS supports the features used with the old Cisco IOS.
- Security image—ASR 901 does not support loading security images in the non-secure environment or node. Loading the security images affect the functionality.

Upgrading the Cisco IOS image

Complete the following steps to upgrade the Cisco IOS image:

Procedure

Step 1 Download the Cisco IOS software image to the TFTP server.

Download the Cisco IOS software image onto your workstation or PC from the Download Software Area (registered customers only).

Step 2 Identify the file system to copy the image.

The file system type ‘flash’ or ‘disk’ is used to store the Cisco IOS image. The **show file system** command lists the file systems available on the router. The file system should have sufficient space to store the Cisco IOS image. You can use the **show file system** or the **dir file_system** command in order to find the free space.

Example:

```
Router# show file system
File Systems:
Size(b)       Free(b)       Type  Flags  Prefixes
        262144        240157     nvram     rw   nvram:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -    opaque     ro   tar:
             -             -   network     rw   tftp:
             -             -    opaque     wo   syslog:
*    100401148      39104096     flash     rw   flash:
      67108860      67108860     flash     rw   ramdisk:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   cns:
```

Step 3 Prepare for the upgrade.

You should consider these items before you upgrade the Cisco IOS:

- Store both the old Cisco IOS and the new Cisco IOS, if the router has sufficient memory. You can boot the router in the ROMMON mode and boot the old Cisco IOS, in case of boot failure with new Cisco IOS. This method saves time if you want to roll back the Cisco IOS.
- Backup the configuration from the router because some of the Cisco IOS releases add default configurations. This newly added configuration may conflict with your current configuration. Compare the configuration of the router after the Cisco IOS upgrade with the configuration backed up before the upgrade. If there are differences in the configuration, you must ensure they do not affect your requirements.

Step 4 Verify that the TFTP server has IP connectivity to the router.

The TFTP server must have a network connection to the router and must be able to ping the IP address of the router targeted for a TFTP software upgrade. In order to achieve this connection, the router interface and the TFTP server must have an IP address in the same range or a default gateway configured. Check the IP address of the TFTP server in order to verify this configuration.

Step 5 Copy the IOS Image from the TFTP server.

Before you copy the image, ensure that you have started the TFTP server software on your PC, and that you have the file name mentioned in the TFTP server root directory. Cisco recommends that you keep a backup of the router and access server configuration before you upgrade. The upgrade does not affect the configuration, which is stored in nonvolatile RAM [NVRAM]. However, this situation might happen if the right steps are not followed properly.

Example:

```
Router# copy tftp: flash:
```

```
Address or name of remote host []? 10.105.33.135
Source filename []? asr901-universalk9-mz.151-2.SNG
Destination filename [asr901-universalk9-mz.151-2.SNG]?
Accessing tftp://10.105.33.135/asr901-universalk9-mz.151-2.SNG...
Erase flash: before copying? [confirm]n
Loading asr901-universalk9-mz.151-2.SNG from 10.105.33.135 (via FastEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 30551884 bytes]
Verifying checksum...  OK (0xC7E6)
30551884 bytes copied in 199.636 secs (153038 bytes/sec)
Router#
```

Step 6 Verify the Cisco IOS image in the file system.

Example:

```
Router# dir flash:
Directory of flash:/
1  -rw-    30551884                    <no date>  asr901-universalk9-mz.151-2.SNG
100401148 bytes total (69849200 bytes free)
Router#
```

Router# **verify flash:asr901-universalk9-mz.151-2.SNG**

Example:

```
File system hash verification successful.
```

Step 7 Verify the Configuration Register.

Use the **show version** command to check the config-register value. The value is displayed in the last line of the show version output. It should be set to 0x2102.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# config-register 0x2102
Router(config)#^Z
```

Step 8 Verify the Boot Variable

The router tries to boot with the first file in the Flash. If the first file is not the Cisco IOS Software image, you need to configure a boot system statement in order to boot the specified image. If there is only one file in Flash and it is the Cisco IOS Software image, this step is not necessary.

Example:

```
Router#show run | inc boot
boot-start-marker
boot system flash asr901-universalk9-mz.151-2.SNG.fc1
boot-end-marker
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no boot system
Router(config)#boot system flash asr901-universalk9-mz.151-2.SNG
Router(config)#end
Router#
Router#show run | inc boot
boot-start-marker
boot system flash asr901-universalk9-mz.151-2.SNG
```

```
boot-end-marker
Router#
```

Step 9 Save the configuration and reload the router.

Example:

```
Router# write memory
Router# reload
Proceed with reload? [confirm]
Jul 24 20:17:07.787: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Step 10 Verify the Cisco IOS upgrade.

After the reload is complete, the router should run the desired Cisco IOS Software image. Use the **show version** command in order to verify the Cisco IOS software.

Example:

```
Router# show version
Cisco IOS Software, 901 Software (ASR901-UNIVERSALK9-M), Version 15.1(2)SNG, RELEASE SOFTWARE
 (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 27-Oct-11 15:52 by prod_rel_team
ROM: System Bootstrap, Version 15.1(2r)SNG, RELEASE SOFTWARE (fc1)
ASR901 uptime is 4 minutes
System returned to ROM by reload at 13:11:07 UTC Wed Apr 19 2000
System image file is "tftp://10.105.33.135/rajuvenk/asr901-universalk9-mz.151-2.SNG.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
License Level: AdvancedMetroIPAccess
License Type: Permanent
Next reload license Level: AdvancedMetroIPAccess
Cisco ASR901-E (P2020) processor (revision 1.0) with 393216K/131072K bytes of memory.
Processor board ID CAT1529U01P
P2020 CPU at 792MHz, E500v2 core, 512KB L2 Cache
1 FastEthernet interface
12 Gigabit Ethernet interfaces
1 terminal line
256K bytes of non-volatile configuration memory.
98304K bytes of processor board System flash (Read/Write)
65536K bytes of processor board RAM Disk (Read/Write)
Configuration register is 0x2102
```

Auto Upgrading the MCU

Upgradable MCU is bundled with the IOS image. You can upgrade the MCU using one of the following

ways:

- MCU Auto upgrade can be enabled or disabled by setting the ROMMON variable AUTO_UPGRADE_ROMMON to TRUE or FALSE:
  - From the ROMMON:

rommon> **AUTO_UPGRADE_MCU=TRUE | FALSE**

-
  - From theIOS:

Router# **upgrade mcu preference [enable | disable]**

Once the MCU is upgraded, the router is not reloaded. Subsequent reload versions are compared; if the versions are same, then the MCU is not upgraded.

- If the AUTO_UPGRADE_ROMMON variable is set to FALSE, then the MCU can be upgraded as follows:

Router# **upgrade mcu file flash:image.hex**

Manually Upgrading the ROMMON

Complete the following steps to manually upgrade the router ROMMON:

Procedure

Step 1 Load the IOS image.

Step 2 Copy the upgradable ROMMON file **ASR901_RM2.srec**, to the flash memory.

Step 3 Upgrade the ROMMON using the following command:

Router# **upgrade rom-monitor file flash:ASR901_RM2.srec**

The router reloads and comes up with upgradable ROMMON.

Step 4 Check the status of the currently running ROMMON using any one of the following commands:

- From the ROMMON:
- rommon>**rommon-pref readonly**
- From the IOS:
- router>**show rom-monitor**

Note
While upgrade is in progress, if something goes wrong like power-off or power cycler removed, or if the erase program is not done properly, you can reset the board. It falls back to the read-only rommon.

What to do next

After the ROMMON upgrade, if you need to fall back to either the read-only ROMMON, or the upgrade ROMMON, use any one of the following commands:

- From the IOS:

Router# **upgrade rom-monitor preference readonly | upgrade**

- From the ROMMON:

rommon> **rommon-pref readonly**

Auto Upgrade of ROMMON

Upgradable rommon is bundled with the IOS image. You can do an auto upgrade of the ROMMON using one of the following ways:

- Rommon Auto upgrade can be enabled or disabled with by setting the rommon variable AUTO_UPGRADE_ROMMON to TRUE or FALSE using the following commands:
    - From the ROMMON:

rommon> **AUTO_UPGRADE_ROMMON=TRUE | FALSE**

- From the IOS:

Router# **upgrade rom-monitor preference autoupgrade enable | disable**

By default, the upgrade variable is set to be TRUE.

Once the ROMMON is upgraded, the IOS falls back to the ROMMON. Subsequent reload versions are compared; if the version is the same, then the ROMMON will not be upgraded.

- If the AUTO_UPGRADE_ROMMON variable is set to FALSE, use the following command in IOS, to upgrade:

Router# **upgrade rom-monitor internal**

CHAPTER 7

Configuring Gigabit Ethernet Interfaces

This chapter explains how to configure the Gigabit Ethernet (GE) interface on the Cisco ASR 901 router.

Configuring the Interface

To configure the GE interface, complete the following steps:

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters enable mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.

	Command or Action	Purpose
Step 3	**interface gigabit ethernet** *slot/port* **Example:** `Router(config)# interface gigabit ethernet 0/1`	Specifies the port adapter type and the location of the interface to be configured. The slot is always 0 and the port is the number of the port.
Step 4	**cdp enable** **Example:** `Router(config-if)# cdp enable`	Enables Cisco Discovery Protocol on the router, use the **cdp enable** command.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

Setting the Speed and Duplex Mode

The Gigabit Ethernet ports of the Cisco ASR 901 Router can run in full or half- duplex mode—10 Mbps, 100 Mbps or 1000 Mbps (1 Gbps). The Cisco ASR 901 router has an auto-negotiation feature that allows the router to negotiate the speed and duplex mode with the corresponding interface at the other end of the connection.

Auto-negotiation is the default setting for the speed and transmission mode.

When you configure an interface speed and duplex mode, follow these guidelines:

- If both ends of the line support auto-negotiation, use the default auto-negotiation settings.
- When auto-negotiation is turned on, it auto-negotiates both speed and the duplex mode.
- If one interface supports auto-negotiation, and the interface at the other end does not, configure the duplex mode and speed on both interfaces. If you use the auto-negotiation setting on the supported side, the duplex mode setting is set at half-duplex.
- Auto-negotiation must be enabled for 1000M full duplex Gigabit Ethernet devices; otherwise behavior is unpredictable.
- To configure different speeds (10M / 100M), auto-negotiation should be disabled.

Speed and duplex can be configured only on the following interfaces:

- Copper gigabitethernet interfaces (0/0-3)
- Combo gigabitethernet interface (0/4-7), when the media type is configured as RJ-45

Note In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

Note From the Cisco IOS Release 15.5(3)S onwards, to make 10 G port work with 10 Gbps speed, you must use 10G SFP+ pluggable and for it to work in 1 Gbps speed, you must use the 1G SFP. This is specific to 10G port only.

To configure speed and duplex operation, complete these steps in the interface configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**duplex** [**half** | **full**] **Example:** `Router(config-if)# duplex half`	Specify the duplex operation.
Step 2	**speed** [**1000** | **100** | **10**] **Example:** `Router(config-if)# speed 1000`	Specify the speed.

Enabling the Interface

To enable the interface, complete these steps:

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

Procedure

	Command or Action	Purpose
Step 1	**no shutdownno shutdown** **Example:** `Router(config)# interface` **`gigabitethernet 0/1`**	Specify the port adapter type and the location of the interface to be configured. The *type number* is always 0 and the *type number* is the number of the port.
Step 2	**no shutdown**	Enable the gigabit Ethernet interface using the **no shutdown** command.

Modifying MTU Size on the Interface

Complete the following steps to modify the MTU size on Gigabit Ethernet interface:

Note To configure mtu under SVI interface, use mtu bytes command since ip mtu bytes command is not supported under SVI interface.

Note Maximum frame size allowed is calculated as the sum of configured MTU value and size of Layer 2 header.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Selects a Gigabit Ethernet interface and enters interface configuration mode. • *slot/port*—Specifies the slot and port number.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 6000`	Configures the MTU size for Gigabit Ethernet interface. • *bytes*—The range is from 1500 to 9216. The default is 9216. **Note** To set the MTU size to its default value, use the **no mtu** or **default mtu** command. **Note** Maximum frame size allowed is calculated as the sum of configured MTU value and size of Layer 2 header.

Verifying the MTU Size

To verify the MTU size, use the **show interface gigabitethernet** and **show interface mtu** commands.

```
Router# show interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 4055.398d.bd05 (bia 4055.398d.bd05)
  MTU 6000 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 unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 21:01:41
  Input queue: 0/200/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 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
Router# show interface mtu
Port    Name               MTU
Gi0/0                      9216
Gi0/1                      6000
Gi0/2                      3000
Gi0/3                      9216
Gi0/4                      9216
Gi0/5                      9216
Gi0/6                      9216
Gi0/7                      9216
Gi0/8                      9216
Gi0/9                      9216
Gi0/10                     9216
Gi0/11                     9216
```

MAC Flap Control

A MAC flap occurs when a switch receives packets from two different interfaces, with the same source MAC address. This happens when wrong configurations such as loops are introduced in networks. MAC flapping can cause CPU hogs and software induced crashes, if preventive action is not taken.

The two main aspects of MAC flap control feature are:

- Identification of MAC Flapping—Identified when MAC movement counter threshold is hit at specified time intervals.
- Preventive Action—Err-Disabling is done in one of the ports that has MAC flapping.

This feature is disabled by default and can be enabled or disabled through the CLI. You can configure the maximum number of MAC movements that are allowed in a specified time interval, beyond which the MAC movement is termed as flapping.

Once the port is err-disabled, it can be administratively brought up using the **shut** and **no shut** commands.

Restrictions and Limitations

- If MAC learning is done in tens of thousands, the CPU may slow down. This feature does not address the slow down or CPU hog due to MAC learning.
- When the router is learning tens of thousands of MACs, and there are a couple of genuine MAC movements (not due to a loop), they are not tagged as MAC flapping since these are valid MAC movements.
- Average MAC Movement issue

For example, let us assume that MAC movement counter is configured for a maximum of 5 MAC movements in 10 seconds.

If 2000 MACs have contributed for 4 MAC movements each in 10 seconds, the total number of AC movements will be 8000. Since the individual MAC threshold is not hit in this case, the router does not take any preventive action. However, this condition may not really occur in practice.

Configuring MAC FLap Control

Complete the following steps to configure MAC Flap control:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 2	**mac-flap-ctrl on per-mac** *mac-movement time-interval* **Example:** `Router(config)# mac-flap-ctrl on per-mac 20 10`	Enables MAC flap control. • mac-movement—Maximum number of MAC movements that are allowed in the specified time. • time-interval—Time interval that can elapse before the MAC movements are tagged as flapping. If values are not specified for the above parameters, the default values are taken by the router. The default values for the counters are five and ten; that is five movements in ten seconds. The **no** form of the command disables this feature.

Configuring a Combo Port

A combo port is considered as a single interface with dual front ends (an RJ-45 connector and an SFP module connector). The dual front ends of a combo port are non-redundant interfaces; the Cisco ASR 901 Router activates only one connector of the pair. Combo ports can be configured as copper ports or small form-factor pluggable (SFP) module ports.

By default, the Cisco ASR 901 Router selects the RJ-45 connector. However, you can use the **media-type** command to manually select the media type. When the media type is auto-select, the router gives preference to SFP module if both copper and fiber-optic signals are simultaneously detected.

Note

- When DOM is enabled on a port (with active SFP link status) and the SFP encounters violations of any kind, an error message is displayed, irrespective of the port being combo or non-combo.
- When the media type is auto-select, the Cisco ASR 901 Router configures both types with auto negotiation of speed and duplex.
- When the media type is auto-select, you cannot use 100M SFPs.
- When the media type is auto-select, you cannot use the **speed** and **duplex** commands.
- When the media type is auto-select, the Cisco ASR 901 Router uses the following criteria to select the type:
  - If only one connector is installed, that interface is active and remains active until the media is removed or the router is reloaded.
  - If both media are installed in the combo port, the router gives preference to the SFP module interface.
  - If both media are installed in the combo port, when the SFP module interface is inactive, the RJ-45 connector is selected. When the SFP module interface recovers and becomes active, the RJ-45 connector is disabled and the router gives preference to the SFP module interface.
  - If both media are installed in the combo port, and the router is reloaded or the port is disabled and then re-enabled through the **shutdown** and the **no shutdown** interface configuration commands, the router gives preference to the SFP module interface.
  - Copper SFPs are not supported on combo ports in Cisco ASR 901 Router

  Note Copper SFPs auto-negotiation is not mandatory for 1000Base-T devices.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Selects a Gigabit Ethernet interface and enters interface configuration mode. • *slot/port*—Specifies the slot and port number.
Step 4	**media-type** {**auto-select** | **rj45** | **sfp**} **Example:** `Router(config-if)# media-type rj45`	Configures the media type. • **auto-select**—Specifies dynamic selection of the physical connection. • **rj45**—Specifies an RJ-45 physical connection. • **sfp**—Specifies an SFP physical connection for fiber media.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Verifying the Media Type

To verify the media type, use the **show interface gigabitethernet** command.

Following is a sample output when the media type is RJ-45:

```
Router# show interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 4055.398d.bd05 (bia 4055.398d.bd05)
  MTU 9216 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 unsupported, input flow-control is unsupported
```

Following is a sample output when fiber-optic is selected as the physical connection:

```
Router# show interface gigabitethernet 0/7
GigabitEthernet0/7 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 4055.398d.bd0b (bia 4055.398d.bd0b)
  MTU 9216 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 SX
  output flow-control is unsupported, input flow-control is unsupported
```

Following is a sample output when the media type is auto-select and the interface is down:

```
Router# show interface gigabitethernet 0/7
GigabitEthernet0/7 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 9216 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 unknown
  output flow-control is unsupported, input flow-control is unsupported
```

CHAPTER 8

Configuring EtherChannels

This chapter describes how to configure EtherChannels on the Cisco ASR 901 router Layer 2 or Layer 3 LAN ports.

Understanding How EtherChannels Work

This section contains the following topics:

EtherChannel Feature Overview

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

The Cisco ASR 901 router supports a maximum of eight EtherChannels with a maximum eight member links in each EtherChannel.

You can form an EtherChannel with up to eight compatibly configured LAN ports in a Cisco ASR 901 . All LAN ports in each EtherChannel must be of the same speed and must all be configured as Layer 2 LAN ports.

Note The network device to which a Cisco ASR 901 is connected may impose its own limits on the number of ports in an EtherChannel.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel. When a failure occurs, the EtherChannel feature sends a trap that identifies the router, the EtherChannel, and the failed link. Inbound broadcast packets on one segment in an EtherChannel are blocked from returning on any other segment of the EtherChannel.

Understanding How EtherChannels Are Configured

This section contains the following topics:

EtherChannel Configuration Overview

You can configure EtherChannels manually or use the Link Aggregation Control Protocol (LACP) to form EtherChannels. The EtherChannel protocols allow ports with similar characteristics to form an EtherChannel through dynamic negotiation with connected network devices. LACP is defined in IEEE 802.3ad.

Table 8: EtherChannel Modes , on page 78 lists the user-configurable EtherChannel modes.

Table 8: EtherChannel Modes

Mode	Description
on	This is the mode that forces the LAN port to channel unconditionally. In the **on** mode, a usable EtherChannel exists only when a LAN port group in the **on** mode is connected to another LAN port group in the **on** mode. Because ports configured in the **on** mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the **on** mode with an EtherChannel protocol.
passive	(Default for LACP) LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

Understanding Manual EtherChannel Configuration

Manually configured EtherChannel ports do not exchange EtherChannel protocol packets. A manually configured EtherChannel forms only when you enter configure all ports in the EtherChannel compatibly.

Understanding IEEE 802.3ad LACP EtherChannel Configuration

LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in **passive** and **active** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **passive** and **active** modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A LAN port in **active** mode can form an EtherChannel successfully with another LAN port that is in **active** mode.
- A LAN port in **active** mode can form an EtherChannel with another LAN port in **passive** mode.
- A LAN port in **passive** mode cannot form an EtherChannel with another LAN port that is also in **passive** mode, because neither port will initiate negotiation.

Table 9: LACP EtherChannel Modes, on page 79 provides a summary of these combinations.

Table 9: LACP EtherChannel Modes

Router A	Router B	Result
passive mode	**passive** mode	No EtherChannel group is created.
passive mode	**active** mode	EtherChannel group is created.
active mode	**passive** mode	EtherChannel group is created.
active mode	**active** mode	EtherChannel group is created.

LACP uses the following parameters:

Note The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

Note Port priority is only effective when it is configured on a device with an LACP system priority higher than the peer.

- LACP administrative key—LACP automatically configures an administrative key value equal to the channel group identification number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:
  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration restrictions that you establish

On ports configured to use LACP, LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails. You can configure an additional 8 standby ports (total of 16 ports associated with the EtherChannel).

Understanding Port-Channel Interfaces

Each EtherChannel has a numbered port-channel interface. The configuration that you apply to the port-channel interface affects all LAN ports assigned to the port-channel interface.

After you configure an EtherChannel, the configuration that you apply to the port-channel interface affects the EtherChannel; the configuration that you apply to the LAN ports affects only the LAN port to which you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port-channel interface, for example, Spanning Tree Protocol (STP) commands or commands to configure a Layer 2 EtherChannel as a trunk.

Understanding Load Balancing

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses. EtherChannel load balancing can use either source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the router. EtherChannel load balancing can use MPLS Layer 2 information.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

EtherChannel Configuration Guidelines and Restrictions

Note When EtherChannel interfaces are configured improperly, they are disabled automatically to avoid network loops and other problems.

- The commands in this chapter can be used on all LAN ports in the Cisco ASR 901 .
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.
- Enable all LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is moved to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- For Layer 2 EtherChannels:
  - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
  - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
  - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.
  - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are still compatible for the formation of an EtherChannel.
  - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.
- You can configure a maximum of eight port-channel interfaces, numbered from 1 to 8.

- After you configure an EtherChannel, the configuration that you apply to the port-channel interface affects the EtherChannel. The configuration that you apply to the LAN ports affects only those LAN ports to which you apply the configuration.
- Enable Bidirectional Forwarding Detection (BFD) for a port channel on Switch Virtual Interface (SVI) to achieve better convergence during failover.

Configuring Etherchannels

This section contains the following topics:

Note Ensure that the LAN ports are configured correctly (see the EtherChannel Configuration Guidelines and Restrictions, on page 80).

Configuring Channel Groups

Note When configuring Layer 2 EtherChannels, configure the LAN ports with the **channel-group** command as described in this section, which automatically creates the port-channel logical interface. You cannot add Layer 2 LAN ports into a manually created port-channel interface.

- To create port-channel interfaces for Layer 2 EtherChannels, the Layer 2 LAN ports must be connected and functioning.

To configure channel groups, complete the following steps for each LAN port in interface configuration mode:

Procedure

	Command or Action	Purpose
Step 1	Router(config)# **interface** *type slot/port*	Selects a LAN port to configure.
Step 2	Router(config-if)# **no ip address**	Ensures that there is no IP address assigned to the LAN port.
Step 3	Router(config-if)# **channel-protocol lacp**	(Optional) On the selected LAN port, restricts the **channel-group** command to the EtherChannel protocol configured with the **channel-protocol** command.
Step 4	Router(config-if)# **channel-group** *number* **mode** {**active** | **on** | **passive**}	Configures the LAN port in a port-channel and specifies the mode (see table in the EtherChannel Configuration Overview, on page 78 section). LACP supports the active and passive modes.

	Command or Action	Purpose
Step 5	Router(config-if)# **lacp port-priority** *priority_value*	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
Step 6	Router(config-if)# **end**	Exits configuration mode.
Step 7	Router# **show running-config interface** *type slot/port* **Example:** `Router# show interfaces type slot/port etherchannel`	Verifies the configuration. *type*—**gigabitethernet**.

Configuring the LACP System Priority and System ID

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router. To configure the LACP system priority and system ID, complete the following tasks:

Procedure

	Command or Action	Purpose
Step 1	**lacp system-priority** *priority_value* **Example:** `Router(config)# lacp system-priority 23456`	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
Step 2	**end** **Example:** `Router(config)# end`	Exits configuration mode.
Step 3	**show lacp sys-id** **Example:** `Router# show lacp sys-id`	Verifies the configuration.

What to do next

Configuration examples for LACP system priority

This example shows how to configure the LACP system priority:

```
Router# configure terminal

Router(config)# lacp system-priority 23456
Router(config)# end
```

This example shows how to verify the configuration:

```
Router# show lacp sys-id
```

```
23456,0050.3e8d.6400
```

The system priority is displayed first, followed by the MAC address of the router.

Configuring the LACP Transmit Rate

To configure the rate at which Link Aggregation Control Protocol (LACP) control packets are transmitted to an LACP-supported interface, complete the following tasks:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**lacp rate {fast | normal}** **Example:** `Router(config-if)# lacp rate fast`	Configures the transmission rate of LACP control packets to an LACP-supported interface. • **fast**—Specifies that LACP control packets are transmitted at the fast rate, once every second. • **normal**—Specifies that LACP control packets are transmitted at the normal rate, every 30 seconds after the link is bundled.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits the interface configuration mode and enters the privileged EXEC mode.

Verifying the LACP Transmit Rate

To verify the LACP control packet transmission rate, use the following show command:

```
Router# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi0/1     FA      bndl      32768         0xA       0xA     0x102       0x7D
```

Configuring EtherChannel Load Balancing

To configure EtherChannel load balancing, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	Router(config)# **port-channel load-balance** {**src-mac** | **dst-mac** | **src-dst-mac** | **src-ip** | **dst-ip** | **src-dst-ip**}	Configures EtherChannel load balancing. The load-balancing keywords indicate the following information: • **dst-ip**—Destination IP addresses • **dst-mac**—Destination MAC addresses • **src-dst-ip**—Source and destination IP addresses • **src-dst-mac**—Source and destination MAC addresses • **src-ip**—Source IP addresses • **src-mac**—Source MAC addresses
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show etherchannel load-balance**	Verifies the configuration.

Configuration Examples

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Router# configure terminal

Router(config)# port-channel load-balance src-dst-ip

Router(config)# end

Router(config)#
```

This example shows how to verify the configuration:

```
Router# show etherchannel load-balance
```

```
Source XOR Destination IP address
Router#
```

Modifying MTU Size on Port-Channel

Complete the following steps to modify MTU size on the port-channel interface:

Note If the MTU size of a port-channel member link is different from the MTU size of the port-channel interface, the member link is not bundled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface port-channel** *number* **Example:** `Router(config)# interface port-channel 1`	Selects a port-channel interface and enters interface configuration mode. • *number*—Specifies the port-channel interface number. The range is from 1 to 8.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 4000`	Configures the MTU size for port-channel interface. • *bytes*—The range is from 1500 to 9216. The default is 9216. **Note** To set the MTU size to its default value, use the **no mtu** or **default mtu** command.

Verifying the MTU Size on Port-Channel

To verify the MTU size on port-channel interface, use the **show interface port-channel** command.

```
Router# show interface port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 4055.3989.4a15 (bia 4055.3989.4a15)
  MTU 4000 bytes
, BW 2000000 Kbit/sec, DLY 1000 usec,
```

```
     reliability 255/255, txload 1/255, rxload 0/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  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: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP 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
```

EVC On Port-Channel

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.The EVC EtherChannel feature provides support for EtherChannels on Ethernet Virtual Connection Services (EVCS) service instances.

The EVC EtherChannel feature supports MPBE, local connect, and xconnect service types.

Load balancing is accomplished on a Ethernet flow point (EFP) basis where a number of EFPs exclusively pass traffic through member links. In a default load balancing, you have no control over how the EFPs are grouped together, and sometimes the EFP grouping may not be ideal. To avoid this, use manual load balancing to control the EFP grouping.

Restrictions for EVC EtherChannel

The following restrictions apply to EVC EtherChannel:

- Bridge-domains, EVCs, and IP subinterfaces are allowed over the port-channel interface and the main interface.
- If you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.
- If port-channel is configured on an MPLS core, the encapsulation ID should be the same as the bridge domain.
- A physical port that is part of an EVC port-channel cannot have EVC configuration.
- Statically configuring port-channel membership with LACP is not supported.
- You can apply QoS policies under EVCs on a port-channel.
- You cannot use the police percent commands on EVC port-channels in flat policy-maps or in parent of HQoS policy-maps.

Configuring EVC on Port-Channel

To configure the EVC on port-channel, complete these steps in the interface configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**interface port-channel** *number* **Example:** `Router(config)# interface port-channel 11`	Creates the port-channel interface.
Step 2	**[no] service instance** *id* **ethernet** *service-name* **Example:** `Router(config-if)# service instance 101 ethernet`	Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.
Step 3	**encapsulation {untagged | dot1q** *vlan-id* **[second-dot1q** *vlan-id***]}** **Example:** `Router(config-if-srv)# encapsulation dot1q 13`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 4	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.
Step 5	**[no] bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 12`	The bridge-domain command binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.

Verifying the Configuration

Use the following commands to verify the configuration:

Command	Purpose
Router# show ethernet service evc [id evc-id | interface interface-id] [detail]	Displays information pertaining to a specific EVC if an EVC ID is specified, or pertaining to all EVCs on an interface if an interface is specified. The detailed option provides additional information on the EVC.
Router# show ethernet service instance interface port-channel number [summary]	Displays the summary of all the configured EVCs within the interface.

Command	Purpose
Router# show ethernet service instance [id instance-id interface interface-id | interface interface-id] [detail]	Displays information about one or more service instances. If a service instance ID and interface are specified, only data pertaining to that particular service instance is displayed. If only an interface ID is specified, displays data for all service instances s on the given interface.
Router# show mpls l2 transport vc detail	Displays detailed information related to the virtual connection (VC).
Router# show mpls forwarding	Displays the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB). **Note** Output should have the label entry l2ckt.
Router# show etherchannel summary	Displays view all EtherChannel groups states and ports.
Router# show policy-map interface service instance	Displays the policy-map information for a given service instance.

Troubleshooting Scenarios for EVC on a Port-Channel

Problem	Solution
Port data block issues in port-channel	Use the show ethernet service interface [interface-id] [detail] command to view information on the port data. Share the output with TAC for further investigation.
Issues with platform events or errors	Use the debug platform npc custom-ether client [event, error] command to debug and trace platform issues. Share the output with TAC for further investigation.

CHAPTER 9

Configuring Ethernet OAM

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks, to increase management capability within the context of the overall Ethernet infrastructure.

The Cisco ASR 901 router supports:

- IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback.
- IEEE 802.1ag Connectivity Fault Management (CFM)
- Ethernet Local Management Interface (E-LMI)
- IP Service Level Agreements (SLAs) for CFM
- ITU-T Y.1731 fault management

This chapter provides information about configuring the Ethernet OAM, CFM and E-LMI and also enabling Ethernet Loopback.

For complete command and configuration information for Ethernet OAM see the *Cisco IOS Carrier Ethernet Configuration Guide* at this URL:
http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/12-2sr/ce-12-2sr-book.html

Note The Cisco ASR 901 router does not necessarily support all of the commands listed in the Cisco IOS Carrier Ethernet documentation.

Note Cisco ASR 901 does not support CFM pre-draft version.

Understanding Ethernet CFM

Ethernet CFM is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end can be provider-edge-to-provider-edge (PE-to-PE) device. Ethernet CFM, as specified by IEEE 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network.

For more information about ethernet CFM, see Ethernet Connectivity Fault Management .

IP SLA Support for CFM

The router supports CFM with IP Service Level Agreements (SLA), which provides the ability to gather Ethernet layer network performance metrics. Available statistical measurements for the IP SLA CFM operation include round-trip time, jitter (interpacket delay variance), and packet loss. You can schedule multiple IP SLA operations and use Simple Network Management Protocol (SNMP) trap notifications and syslog messages for proactive threshold violation monitoring.

IP SLA integration with CFM gathers Ethernet layer statistical measurements by sending and receiving Ethernet data frames between CFM MEPs. Performance is measured between the source MEP and the destination MEP. Unlike other IP SLA operations that provide performance metrics for only the IP layer, IP SLA with CFM provides performance metrics for Layer 2.

You can manually configure individual Ethernet ping or jitter operations. You can also configure an IP SLA automatic Ethernet operation that queries the CFM database for all MEPs in a given maintenance domain and VLAN. The operation then automatically creates individual Ethernet ping or jitter operations based on the discovered MEPs.

Because IP SLA is a Cisco proprietary feature, interoperability between CFM draft 1 and CFM 802.1ag is handled automatically by the router.

For more information about IP SLA operation with CFM, see the *IP SLAs for Metro-Ethernet* feature module at this URL:

http://www.cisco.com/en/US/docs/ios/12_2sr/12_2srb/feature/guide/sr_meth.html

Configuring Ethernet CFM

Configuring Ethernet CFM requires configuring the CFM domain. You can optionally configure and enable other CFM features such as crosschecking, remote MEP, port MEPs, SNMP traps, and fault alarms. Note that some of the configuration commands and procedures differ from those used in CFM draft 1.

This section contains the following topics:

Default Ethernet CFM Configuration

- CFM is globally disabled.
- CFM is enabled on all interfaces when CFM is globally enabled.
- A port can be configured as a flow point (MIP/MEP), a transparent port, or disabled (CFM disabled). By default, ports are transparent ports until configured as MEP, MIP, or disabled.

- There are no MEPs or MIPs configured.
- When configuring a MEP, if you do not configure direction, the default is up (inward facing) which is not supported for CFM hardware offload sessions.
- For Multi-UNI CFM MEPs (with up direction), port-based model for MAC address assignment is used instead of bridge brain model.

Ethernet CFM Configuration Restrictions and Guidelines

- You cannot configure CFM on VLAN interfaces.
- CFM is configurable only under EVC and physical or port channel interfaces.
- CFM is supported on ports running MSTP.
- You must configure a port MEP at a lower level than any service (VLAN) MEPs on an interface.

Configuring the CFM Domain

Complete the following steps to configure the Ethernet CFM domain, configure a service to connect the domain to a VLAN, or configure a port to act as a MEP. You can also enter the optional commands to configure other parameters, such as continuity checks.

Note You do not need to enter the **ethernet cfm ieee** global configuration command to configure the CFM version as IEEE 802.1ag; the CFM version is always 802.1ag and the command is automatically generated when you enable CFM.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm global**	Globally enable Ethernet CFM on the router.
Step 3	**ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	(Optional) Configure the CFM traceroute cache. You can set a maximum cache size or hold time. • (Optional) For **size**, enter the cache size in number of entry lines. The range is from 1 to 4095; the default is 100 lines. • (Optional) For **hold-time**, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.
Step 4	**ethernet cfm mip auto-create level** *level-id* **vlan** *vlan-id*	(Optional) Configure the router to automatically create MIPs for VLAN IDS that are not associated with specific maintenance associations at the specified level. The level range is 0 to 7.

	Command or Action	Purpose
		Note Configure MIP auto-creation only for VLANs that MIPs should monitor. Configuring for all VLANs can be CPU and memory-intensive.
Step 5	**ethernet cfm mip filter**	(Optional) Enable MIP filtering, which means that all CFM frames at a lower level are dropped. The default is disabled.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 7	**id** {*mac-address domain_number* | **dns** *name* | **null**}	(Optional) Assign a maintenance domain identifier. • *mac-address domain_number* — Enter the MAC address and a domain number. The number can be from 0 to 65535. • **dns** *name* —Enter a DNS name string. The name can be a maximum of 43 characters. • **null**—Assign no domain name.
Step 8	**service** {*ma-name* | *ma-number* | *vpn-id vpn* } {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number* —a value from 0 to 65535. • *vpn-id vpn* —enter a VPN ID as the *ma-name* . • **vlan** *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 9	**continuity-check**	Enable sending and receiving of continuity check messages.
Step 10	**continuity-check interval** *value*	(Optional) Set the interval at which continuity check messages are sent. The available values

	Command or Action	Purpose
		are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 11	**continuity-check loss-threshold** *threshold-value*	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 12	**maximum meps** *value*	(Optional) Configure the maximum number of MEPs allowed across the network. The range is from 1 to 65535. The default is 100.
Step 13	**sender-id chassis none**	(Optional) Include the sender ID TLVs, attributes containing type, length, and values for neighbor devices. • **chassis**—Send the chassis ID (host name). • **none**—Do not include information in the sender ID.
Step 14	**mip auto-create** [**lower-mep-only** | **none**]	(Optional) Configure auto creation of MIPs for the service. • **lower-mep-only** —Create a MIP only if there is a MEP for the service in another domain at the next lower active level. • **none** —No MIP auto-create.
Step 15	**exit**	Return to ethernet-cfm configuration mode.
Step 16	**mip auto-create** [**lower-mep-only**]	(Optional) Configure auto creation of MIPs for the domain. • **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.
Step 17	**mep archive-hold-time** *minutes*	(Optional) Set the number of minutes that data from a missing maintenance end point is kept before it is purged. The range is 1 to 65535; the default is 100 minutes.
Step 18	**exit**	Return to global configuration mode.
Step 19	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.

	Command or Action	Purpose
Step 20	**service instance** *number* **ethernet** *name*	Specify the service instance number and the name of the EVC.
Step 21	**cfm mip level** *level-id*	(Optional) Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7. **Note** This step is not required if you have entered the **ethernet cfm mip auto-create** global configuration command or the **mip auto-create** ethernet-cfm or ethernet-cfm-srv configuration mode.
Step 22	**cfm mep domain** *domain-name* **mpid** *identifier*	Configure maintenance end points for the domain, and enter Ethernet cfm mep mode. • **domain** *domain-name* —Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
Step 23	**cos** *value*	(Optional) Specify the class of service (CoS) value to be sent with the messages. The range is 0 to 7.
Step 24	**end**	Return to privileged EXEC mode.
Step 25	**show ethernet cfm maintenance-points** {**local** | **remote**}	Verify the configuration.
Step 26	**show ethernet cfm errors [configuration]**	(Optional) Display the configuration error list.
Step 27	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Note Use the **no** form of each command to remove the configuration or return to the default configurations.

Example for Basic CFM configuration

```
Router(config)# ethernet cfm ieee
Router(config)# ethernet cfm global
Router(config)# ethernet cfm domain abc level 3
Router(config-ecfm)# service test evc EVC1 vlan 5
Router(config-ecfm-srv)# continuity-check
```

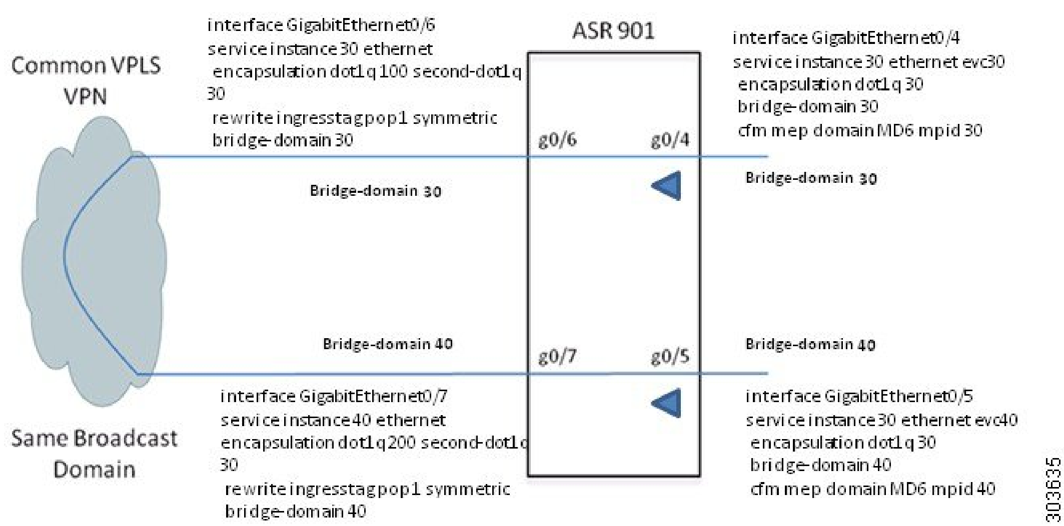
```
Router(config-ecfm-srv)# exit
Router(config-ecfm)# exit
Router(config)# ethernet evc EVC1
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service instance 1 ethernet EVC1

Router(config-if-srv)# encapsulation dot1q 5
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 5
Router(config-if-srv)# cfm mep domain abc mpid 100
Router(config-if-ecfm-mep)# exit
```

Configuring Multi-UNI CFM MEPs in the Same VPN

Effective with Cisco IOS Release 15.3(2)S, services are configured such that two or more bridge domains (BDs) are used to achieve UNI isolation and backhauling towards provider edge (PE) device. Local MEPs (with up direction) need to be configured on the UNIs (with the associated BDs) to monitor the service backhaul connection. To achieve this, use the alias command to configure a CFM MA, MA2, as an alias to another MA, MA1. As a result, MA1 behaves as though it is configured as MA2 on a different Bridge Domain (BD) associated with it. MA1 and MA2 function as if they are part of the same service, thus associating the same CFM MA to two different BDs and UNI isolation.

The following figure shows the configuring Mutli-NNI CFM in the same VPN.

Figure 2: Configuring Multi-NNI CFM in the Same VPN



Restrictions:

- Two MAs can be configured such that MA2 connected with different BD will act as a proxy (alias) for MA1 only for the MEPs which have the service direction as Up.
- Y1731-PM is not supported with Multi-NNI CFM.

Complete these steps to configure Multi-UNI CFM MEPs in the same VPN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode. Enter your password if prompted.
Step 2	**ethernet cfm global** **Example:** `Router(config)# ethernet cfm global`	Globally enable Ethernet CFM on the router.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Router(config)# ethernet cfm domain MD6 level 6`	Define a CFM domain, set the domain level, and enter ethernet-CFM configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 4	**service** {*ma-name* | *ma-number* | *vpn-id vpn* } {**vlan** *vlan-id* [**direction down**] | **port**} **Example:** `Router(config-ecfm)# service MA6 evc evc30 vlan 30`	Define a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number* —a value from 0 to 65535. • *vpn-id vpn* —enter a VPN ID as the *ma-name* . • **vlan** *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. **Note** Two MAs can be configured such that MA2 connected with different BD will act as a proxy (alias) for MA1 only for the MEPs which have the service direction as Up. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 5	**continuity-check** **Example:** `Router(config-ecfm-srv)# continuity-check`	Enable sending and receiving of continuity check messages.

	Command or Action	Purpose
Step 6	**continuity-check interval** *value* **Example:** `Router(config-ecfm-srv)# continuity-check interval 1s`	(Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute, and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 7	**continuity-check loss-threshold** *threshold-value* **Example:** `Router(config-ecfm-srv)# continuity-check loss-threshold 4`	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 8	**alias**{ **alias-short-ma-name** | **icc** *icc-code meg-id* | **number** *ma-number* | **vlan** *vlan-id* | **vpn** *vpn-id*} **Example:** `Router(config-ecfm-srv)# alias MA6`	Define a customer alias maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode. • **alias-short-ma-name**—a string of no more than 48 characters that identifies the MAID. **Note** If the **alias-short-ma-name** option is not configured, then the MAID is automatically generated as a combination of service ID and CFM domain name. When creating an MEP for an EFP, if the length of the MAID exceeds 48 characters, then CC messages are not sent out. We recommend that you use the **alias-short-ma-name** option if a long service ID or domain name is configured. • **icc icc-code meg-id**—specify the ITU Carrier Code (ICC) (maximum: 6 characters) and Unique Maintenance Entity Group (MEG) ID Code (UMC). The maximum characters allowed is 12. • **number** *ma-number* —a value from 0 to 65535. • *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.

	Command or Action	Purpose
		• *vpn-id* —enter a VPN ID as the *ma-name* .
Step 9	**exit**	Return to ethernet-CFM configuration mode.
Step 10	**exit**	Return to global configuration mode.
Step 11	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/4`	Specify an interface to configure, and enter interface configuration mode.
Step 12	**service instance** *number* **ethernet** *name* **Example:** `Router(config-if)# service instance 30 ethernet EVC30`	Specify the service instance number and the name of the EVC.
Step 13	**cfm mep domain** *domain-name* **mpid** *identifier* **Example:** `Router(config-if-srv)# cfm mep domain MD6 mpid 30`	Configure maintenance end points for the domain, and enter Ethernet cfm mep mode. • **domain** *domain-name* —Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
Step 14	**end**	Return to privileged EXEC mode.
Step 15	**show ethernet cfm maintenance-points** {**local** | **remote**}	Verify the configuration.
Step 16	**show ethernet cfm errors [configuration]**	(Optional) Display the configuration error list.
Step 17	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuration Examples for Multi-UNI CFM MEPs

Example Configuration for Multi-UNI CFM MEPs in the same VPN

```
Router(config)# ethernet cfm ieee
Router(config)# ethernet cfm global
Router(config)# ethernet cfm domain MD6 level 6
Router(config-ecfm)# service MA6 evc evc30 vlan 30
Router(config-ecfm-srv)# continuity-check
Router(config-ecfm-srv)# continuity-check interval ls
Router(config-ecfm-srv)# service MA6_alias evc evc40 vlan 40
Router(config-ecfm-srv)# continuity-check
Router(config-ecfm-srv)# continuity-check interval ls
Router(config-ecfm-srv)# alias MA6
Router(config-ecfm-srv)# exit
```

```
Router(config-ecfm)# exit
Router(config)# ethernet evc EVC30
Router(config)# interface gigabitethernet 0/4
Router(config-if)# service instance 30 ethernet EVC30
Router(config-if-srv)# encapsulation dot1q 30
Router(config-if-srv)# bridge domain 30
Router(config-if-srv)# cfm mep domain MD6 mpid 30
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# ethernet evc EVC40
Router(config)# interface gigabitethernet 0/5
Router(config-if)# service instance 30 ethernet EVC40
Router(config-if-srv)# encapsulation dot1q 30
Router(config-if-srv)# bridge domain 40
Router(config-if-srv)# cfm mep domain MD6 mpid 40
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/6
Router(config-if)# service instance 30 ethernet
Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 30
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 30
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/7
Router(config-if)# service instance 40 ethernet
Router(config-if-srv)# encapsulation dot1q 200 second-dot1q 30
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 40
Router(config-if-srv)# exit
Router(config-if)# exit
```

Verification

Use the following commands to verify a configuration:

- Use the show ethernet cfm maintenance-point local command to verify the Multi-UNI CFMs over EVC configuration. This command shows the basic configuration information for Multi-UNI CFM.

```
Router# show ethernet cfm maintenance-points local
Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                    Lvl   MacAddress     Type  CC
Ofld Domain Id                                      Dir   Port           Id
     MA Name                                              SrvcInst       Source
     EVC name
--------------------------------------------------------------------------------
30   MD6                                            6     4055.3989.7868 BD-V  Y
No   MD6                                            Up    Gi0/4          30
     MA6                                                  30             Static
     evc30
40   MD6                                            6     4055.3989.7869 BD-V  Y
No   MD6                                            Up    Gi0/5          40
     MA6_alias (MA6)                                      40             Static
     evc40
Total Local MEPs: 2
Local MIPs: None
```

- Use the show ethernet cfm maintenance-point remote to verify the MEP configuration:

```
Router# show ethernet cfm maintenance-points remote
```

```
--------------------------------------------------------------------------------
MPID  Domain Name                               MacAddress          IfSt  PtSt
Lvl  Domain ID                                 Ingress
 RDI  MA Name                                   Type Id             SrvcInst
      EVC Name                                                      Age
      Local MEP Info
--------------------------------------------------------------------------------
40    MD6                                       4055.3989.7869      Up    Up
 6    MD6                                       Gi0/6
 -    MA6                                       BD-V 30             30
      evc30                                                         0s
      MPID: 30 Domain: MD6 MA: MA6
30    MD6                                       4055.3989.7868      Up    Up
 6    MD6                                       Gi0/7
 -    MA6_alias (MA6)                           BD-V 40             40
      evc40                                                         1s
      MPID: 40 Domain: MD6 MA: MA6_alias (MA6)
Total Remote MEPs: 2
```

Configuring Ethernet CFM Crosscheck

Complete the following steps to configure Ethernet CFM crosscheck:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm mep crosscheck start-delay** *delay*	Configure the number of seconds that the device waits for remote MEPs to come up before the crosscheck is started. The range is 1 to 65535; the default is 30 seconds.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 4	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id*}	Define a customer service maintenance association name or number or VPN ID to be associated with the domain, and a VLAN ID, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number* —a value from 0 to 65535. • *vpn-id vpn* —enter a VPN ID as the *ma-name* . • **vlan** *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.

	Command or Action	Purpose
Step 5	**mep mpid** *identifier*	Define the MEP maintenance end point identifier in the domain and service. The range is 1 to 8191
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**ethernet cfm mep crosscheck** {**enable** | **disable**} **domain** *domain-name* {**vlan** {*vlan-id* | **any**} | **port**}	Enable or disable CFM crosscheck for one or more VLANs or a port MEP in the domain. • **domain** *domain-name*—Specify the name of the created domain. • **vlan** {*vlan-id* | **any**}—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs s}eparated by comma. Enter **any** for any VLAN. • **port**—Identify a port MEP.
Step 8	**show ethernet cfm maintenance-points remote crosscheck**	Verify the configuration.
Step 9	**show ethernet cfm errors** [**configuration**]	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note Use the **no** form of each command to remove a configuration or to return to the default settings.

Configuring Static Remote MEP

Complete the following steps to configure Ethernet CFM static remote MEP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.

	Command or Action	Purpose
Step 3	**service** { *short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id* } {**vlan** *vlan-id* | **port** | **evc** *evc-name* }	Configure the maintenance association and set a universally unique ID for a customer service instance (CSI) or the maintenance association number value, primary VLAN ID and VPN ID within a maintenance domain in Ethernet connectivity fault management (CFM) configuration mode.
Step 4	**continuity-check**	Enable sending and receiving of continuity check messages.
Step 5	**mep mpid** *identifier*	Define the static remote maintenance end point identifier. The range is 1 to 8191
Step 6	**continuity-check static rmep**	Enable checking of the incoming continuity check message from a remote MEP that is configured in the MEP list.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show ethernet cfm maintenance-points remote static**	Verify the configuration.
Step 9	**show ethernet cfm errors** [**configuration**]	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

> **Note** Use the **no** form of each command to remove a configuration or to return to the default settings.

Configuring a Port MEP

A port MEP is a down MEP that is not associated with a VLAN and that uses untagged frames to carry CFM messages. You configure port MEPs on two connected interfaces. Port MEPs are always configured at a lower domain level than native VLAN MEPs.

Complete the following steps to configure Ethernet CFM port MEPs:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 3	**service** {*ma-name* | *ma-number* | *vpn-id*} **port**	Define a customer service maintenance association name or number or VPN ID to be associated with the domain, define a port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id vpn*—enter a VPN ID as the *ma-name* .
Step 4	**mep mpid** *identifier*	Define the static remote maintenance end point identifier in the domain and service. The range is 1 to 8191
Step 5	**continuity-check**	Enable sending and receiving of continuity check messages.
Step 6	**continuity-check interval** *value*	(Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 7	**continuity-check loss-threshold** *threshold-value*	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 8	**continuity-check static rmep**	Enable checking of the incoming continuity check message from a remote MEP that is configured in the MEP list.
Step 9	**exit**	Return to ethernet-cfm configuration mode.
Step 10	**exit**	Return to global configuration mode.
Step 11	**interface** *interface-id*	Identify the port MEP interface and enter interface configuration mode.

	Command or Action	Purpose
Step 12	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* **port**	Configure the interface as a port MEP for the domain. • **domain** *domain-name* —Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show ethernet cfm maintenance-points remote static**	Verify the configuration.
Step 15	**show ethernet cfm errors** [**configuration**]	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 16	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Note Use the **no** form of each command to remove a configuration or to return to the default settings.

This is a sample configuration for a port MEP:

```
Router(config)# ethernet cfm domain abc level 3
Router(config-ecfm)# service PORTMEP port
Router(config-ecfm-srv)# mep mpid 222
Router(config-ecfm-srv)# continuity-check
Router(config-ecfm-srv)# continuity-check static rmep
Router(config-ecfm-srv)# exit
Router(config-ecfm)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet cfm mep domain abc mpid 111 port
Router(config-if)# end
```

CFM with Hardware Offloading for G.8032

To support ITU-T G.8032 Ethernet Ring Protection Switching, the remote CFM fault detection needs to be faster using CFM continuity check messages (CCM). Earlier to Cisco IOS Release 15.4(3)S , the CFM sessions flap with CCM interval less than 1s. All the CFM operations such as CCM packet forward, drop, and processing are taking place at CPU, and this leads to heavy CPU usage with lower CCM intervals. Effective from Cisco IOS Release 15.4(3)S, the Cisco ASR 901 Router supports CFM hardware offloading. Configuring Ethernet CFM for offload CFM session requires configuring the CFM domain with the supported offload CCM intervals

3.3 ms,10 ms, and 100 ms. You can optionally configure the sampling rate for the offload cfm sessions and the default sampling rate is 20000.

Note The **efd notify g8032** command is optional for offload cfm sessions. This command must be used under CFM configuration to notify G.8032 of failures, if any.

Restrictions

- CFM offload is not supported on up MEPs.
- CFM offload is not supported on xconnect EVC.
- Loopback reply (LBR) and loopback trace (LTR) packets are generated at CPU for offloaded sessions.
- CFM offload is supported on port-channel EVC and port MEP from Cisco IOS XE Release 3.14 onwards.
- CFM offload is not supported on following EVC encapsulation types :
    - Dot1Q without rewrite
    - QinQ with Pop1
    - Default EFP
    - Dot1ad-dot1Q with Pop1
    - Untagged EVC
- Delay Measurement Message (DMM) is supported for CFM offload sessions from Cisco IOS XE Release 3.15 onwards.
- MIP is not supported for CFM offload sessions.
- MIP configured for offloaded MEP does not identify remote MEPs. This affects the traceroute and loopback CFM protocols because the CPU does not receive CCM for the offloaded MEP.

Configuring CFM with Hardware Offloading for G.8032

Complete the following steps to configure the CFM with hardware offloading for G.8032.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ethernet cfm global**	Globally enables Ethernet CFM on the router.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id*	Defines a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 4	**service** {*ma-name* | *ma-number* | *vpn-id vpn* } {**vlan** *vlan-id* [**direction down**] | **port**}	Defines a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID

	Command or Action	Purpose
		or port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number* —a value from 0 to 65535. • *vpn-id vpn* —enter a VPN ID as the *ma-name* . • **vlan** *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—Specifies the service direction as down. • **port**—Configures port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 5	**continuity-check**	Enables sending and receiving of continuity check messages.
Step 6	**continuity-check interval** *value*	(Optional) Sets the interval at which continuity check messages are sent. The available values are 100 ms, 10 ms, 3.3 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 7	**continuity-check loss-threshold** *threshold-value*	(Optional) Sets the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 8	**offload sampling** *value*	Defines the sampling rate for the offloaded CFM session. The default is 20,000. The range is 5000 to 65535.
Step 9	**efd notify g8032**	Monitors and notifies G.8032 for failures.
Step 10	**exit**	Returns to global configuration mode.

Verifying the CFM Configuration with Hardware Offloading for G.8032

To verify the maintenance points configured on a device, use the **show ethernet cfm maintenance-points local detail** command, as shown in this example:

```
Router# show ethernet cfm maintenance-points local detail

Local MEPs:
----------
MPID: 2051
DomainName: d7
MA Name: s7
Level: 7
Direction: Down
EVC: e7
Bridge Domain: 200
Service Instance: 100
Interface: Gi0/6
CC Offload: Yes
CC Offload Status: Succeeded
CC Offload Sampling: 20000 (default)
CC-Status: Enabled
CC Loss Threshold: 3
MAC: c067.afdf.321a
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No
Source: Static

MIP Settings:
-------------
Local MIPs: None
```

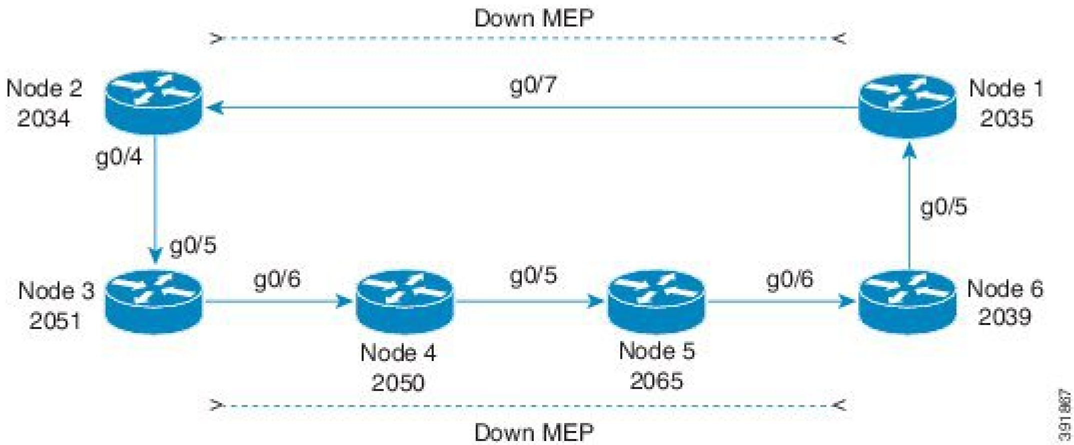
To verify the information about a remote maintenance point domains or levels or details in the CFM database, use the **show ethernet cfm maintenance-points remote** command, as shown in this example:

```
Router# show ethernet cfm maintenance-points remote

--------------------------------------------------------------------------------
MPID  Domain Name                                 MacAddress          IfSt  PtSt
Lvl  Domain ID                                   Ingress
 RDI  MA Name                                     Type Id             SrvcInst
      EVC Name                                                        Age
      Local MEP Info
--------------------------------------------------------------------------------
2039  d7                                          7cad.749d.9276      Up    Up
 7    d7                                          Gi0/6
 -    s7                                          BD-V 200            100
      e7                                                              7s
      MPID: 2051 Domain: d7 MA: s7

Total Remote MEPs: 1
```

Configuration Examples for CFM with Hardware Offloading for G.8032

The following is a sample configuration of CFM with hardware offloading for G.8032.

Figure 3: Sample G.8032 Topology with CFM Hardware Offload



The following sample configuration shows how to configure CFM with hardware offloading for G.8032.

Down MEP between Node 3 and Node 6

```
!
interface GigabitEthernet0/6
no ip address
media-type auto-select
negotiation auto
service instance 2 ethernet
  encapsulation dot1q 50
  rewrite ingress tag pop 1 symmetric
  bridge-domain 50
!
service instance 100 ethernet e7
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
  cfm mep domain d7 mpid 2051
!
end
```

Configuring SNMP Traps

To configure traps for Ethernet CFM, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]	(Optional) Enable Ethernet CFM continuity check traps.

	Command or Action	Purpose
Step 3	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**]	(Optional) Enable Ethernet CFM crosscheck traps.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Note Use the **no** form of each command to remove a configuration or to return to the default settings.

Configuring IP SLA CFM Operation

You can manually configure an individual IP SLA ethernet ping, or jitter echo operation, or you can configure IP SLA ethernet operation with endpoint discovery. You can also configure multiple operation scheduling. For accurate one-way delay statistics, the clocks on the endpoint switches must be synchronized. You can configure the endpoint switches with Network Time Protocol (NTP) so that the switches are synchronized to the same clock source.

For more information about configuring IP SLA ethernet operations, see the IP SLAs Configuration Guide, Cisco IOS Release 15.0S. For detailed information about commands for IP SLAs, see the Cisco IOS IP SLAs Command Reference .

Note The Cisco ASR 901 does not necessarily support all of the commands listed in the Cisco IOS IP SLA documentation.

This section includes these procedures:

Manually Configuring an IP SLA CFM Probe or Jitter Operation

To manually configure an IP SLA ethernet echo (ping) or jitter operation, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**ip sla** *operation-number*	Create an IP SLA operation, and enter IP SLA configuration mode.

	Command or Action	Purpose
Step 3	Do one of the following: • **ethernet echo mpid** *type number***domain***type number***vlan** *type number* • • **ethernet jitter***type number* **mpid** *type number***domainvlan** *type number* [**interval***type number*] [**num-frames***type number*]	Configure the IP SLA operation as an echo (ping) or jitter operation, and enter IP SLA ethernet echo configuration mode. • Enter **echo** for a ping operation or **jitter** for a jitter operation. • For **mpid** *identifier*, enter a maintenance endpoint identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • For **domain***type number*, enter the CFM domain name. • For **vlan** *vlan-id*, the VLAN range is from 1 to 4095. • (Optional—for jitter only) Enter the **interval** between sending of jitter packets. • (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.
Step 4	**cos** *operation-number*	(Optional) Set a class of service value for the operation.
Step 5	**frequency***operation-number*	(Optional) Set the rate at which the IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	**history***operation-number*	(Optional) Specify parameters for gathering statistical history information for the IP SLA operation.
Step 7	**owner***operation-number*	(Optional) Configure the SNMP owner of the IP SLA operation.
Step 8	**request-data-size***operation-number*	(Optional) Specify the protocol data size for an IP SLA request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.
Step 9	**tag***operation-number*	(Optional) Create a user-specified identifier for an IP SLA operation.
Step 10	**threshold***operation-number*	(Optional) Specify the upper threshold value in milliseconds (ms0 for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 11	**timeout***operation-number*	(Optional) Specify the amount of time in ms that the IP SLA operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.

	Command or Action	Purpose
Step 12	**exit**	Return to the global configuration mode.

Step 13	**ip sla schedule***operation-number*[**ageout** *operation-number*] [**life** {**forever** | *operation-number* }] [**recurring**] [**start-time** {*operation-number*} [*operation-number* | *operation-number*] | **pending** | **now** | **after***operation-number*}]	Schedule the time parameters for the IP SLA operation.
		• *operation-number* —Enter the IP SLA operation number.
		• (Optional) **ageout***operation-number*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds.
		• (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds* . The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
		• (Optional) **recurring**—Set the probe to be automatically scheduled every day.
		• (Optional) **start-time**—Enter the time for the operation to begin collecting information:
		  • To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month.
		  • Enter **pending** to select no information collection until a start time is selected.
		  • Enter **now** to start the operation immediately.
		  • Enter **after***operation-number*to show that the operation should start after the entered time has elapsed.

Step 14	**end**	Return to the privileged EXEC mode.
Step 15	**show ip sla configuration** [*operation-number*]	Show the configured IP SLA operation.
Step 16	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To remove an IP SLA operation, enter the no **ip sla** *operation-number* global configuration command.

Configuring an IP SLA Operation with Endpoint Discovery

To automatically discover the CFM endpoints for a domain and VLAN ID, using IP SLAs, complete the steps given below. You can configure ping or jitter operations to the discovered endpoints.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla ethernet-monitor** *operation-number*	Begin configuration of an IP SLA automatic ethernet operation, and enter IP SLA ethernet monitor configuration mode.
Step 3	**type echo domain** *domain-name* **vlan** *vlan-id* [**exclude-mpids** *mp-ids*] **Example:** `type jitter domain domain-name vlan vlan-id [exclude-mpids mp-ids] [interval interpacket-interval] [num-frames number-of frames transmitted]`	Configure the automatic Ethernet operation to create echo (ping) or jitter operation and enter IP SLA ethernet echo configuration mode. • Enter **type echo** for a ping operation or **type jitter** for a jitter operation. • For **mpid** *identifier*, enter a maintenance endpoint identifier. The range is 1 to 8191. • For **domain** *domain-name*, enter the CFM domain name. • For **vlan** *vlan-id*, the VLAN range is from 1 to 4095. • (Optional) Enter **exclude-mpids** *mp-ids* to exclude the specified maintenance endpoint identifiers. • (Optional—for jitter only) Enter the **interval** between sending of jitter packets. • (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.
Step 4	**cos** *cos-value*	(Optional) Set a class of service value for the operation. Before configuring the **cos** parameter, you must globally enable QoS by entering the **mls qos** global configuration command.
Step 5	**owner** *owner-id*	(Optional) Configure the SNMP owner of the IP SLA operation.
Step 6	**request-data-size** *bytes*	(Optional) Specify the protocol data size for an IP SLA request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.

	Command or Action	Purpose
Step 7	**tag** *text*	(Optional) Create a user-specified identifier for an IP SLA operation.
Step 8	**threshold** *milliseconds*	(Optional) Specify the upper threshold value in milliseconds for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 9	**timeout** *milliseconds*	(Optional) Specify the amount of time in milliseconds that the IP SLA operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.
Step 10	**exit**	Return to global configuration mode.

Step 11	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds* }] [**recurring**] [**start-time**{*hh:mm* {*:ss*} [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	Schedule the time parameters for the IP SLA operation.
		• *operation-number*—Enter the IP SLA operation number.
		• (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds.
		• (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds* . The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
		• (Optional) **recurring**—Set the probe to be automatically scheduled every day.
		• (Optional) **start-time**—Enter the time for the operation to begin collecting information:
		  • To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month.
		  • Enter **pending** to select no information collection until a start time is selected.
		  • Enter **now** to start the operation immediately.
		  • Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.

	Command or Action	Purpose
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ip sla configuration** [*operation-number*]	Show the configured IP SLA operation.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To remove an IP SLA operation, enter the **no ip sla** *operation-number* global configuration command.

Configuring CFM over EFP with Cross Connect

The CFM over EFP Interface with cross connect feature allows you to:

- Forward continuity check messages (CCM) towards the core over cross connect pseudowires.

To know more about pseudowires, see

- Receive CFM messages from the core.
- Forward CFM messages to the access side (after Continuity Check Database [CCDB] based on maintenance point [MP] filtering rules).

This section contains the following topics:

Configuring CFM over EFP Interface with Cross Connect

To configure CFM over EFP Interface with cross connect, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** [*pw-class-name*] **Example:** `Router(config)# pseudowire-class vlan-xconnect`	Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.

	Command or Action	Purpose
Step 4	**encapsulation mpls** **Example:** `Router(config-if)# encapsulation mpls`	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.
Step 5	**exit** **Example:** `Router(config-if-srv)# exit`	Exits the pseudowire class configuration mode.
Step 6	**interface** {**gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port*} **Example:** `Router(config-if-srv)# interface Gi2/0/2`	Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet interface to configure.
Step 7	**service instance id ethernet** [**service-name**] **Example:** `Router(config-if-srv)# service instance 101 ethernet`	Creates a service instance (an instantiation of an EVC) on an interface and sets the device into the config-if-srv submode.
Step 8	**encapsulation** {**untagged** | **dot1q vlan-id** | **default**} **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Configures the encapsulation. Defines the matching criteria that maps the ingress dot1q or untagged frames on an interface for the appropriate service instance. Effective with Cisco IOS Release 15.3(2)S, default encapsulation is supported. **Note** **dot1q range** and **second-dot1q** are not supported for EFP Interface with Cross Connect.
Step 9	**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**}] **Example:** `Router(config-if-srv)# xconnect 10.0.3.201 123 pw-class vlan-xconnect`	Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire.
Step 10	**cfm mep domain** *domain-name* [**up** | **down**] **mpid** *mpid-value* [**cos** *cos-value*] **Example:**	Configures a maintenance endpoint (MEP) for a domain.

	Command or Action	Purpose
	`Router(config-if-srv)# cfm mep down mpid 100 domain Core`	
Step 11	**exit** **Example:** `Router(config-if-srv)# exit`	Exits the interface configuration mode.

Examples

This example shows how to configure CFM over EVC using cross connect.

```
ASR901(config)#ethernet cfm ieee
ASR901(config)#ethernet cfm global
ASR901(config)#ethernet cfm domain L5 level 5
ASR901(config-ecfm)# service s1 evc e711
ASR901(config-ecfm-srv)#  continuity-check
ASR901(config-ecfm-srv)#exit
ASR901(config-ecfm)#exit
```

Example for untagged Encapsulation

```
ASR901(config)#int g0/1
ASR901(config-if)#service instance 711 ethernet e711
ASR901(config-if-srv)#encapsulation untagged
ASR901(config-if-srv)# xconnect 3.3.3.3 3 encapsulation mpls
ASR901(cfg-if-ether-vc-xconn)#   mtu 1500
ASR901(cfg-if-ether-vc-xconn)#  cfm mep domain L5 mpid 511
```

Example for single tag Encapsulation

```
ASR901(config)#int g0/1
ASR901(config-if)#service instance 711 ethernet e711
ASR901(config-if-srv)#  encapsulation dot1q 711
ASR901(config-if-srv)#  xconnect 3.3.3.3 3 encapsulation mpls
ASR901(cfg-if-ether-vc-xconn)#   mtu 1500
ASR901(cfg-if-ether-vc-xconn)#  cfm mep domain L5 mpid 511
```

Configuring CFM over EFP Interface with Cross Connect—Port Channel-Based Cross Connect Tunnel

This section describes how to configure CFM over EFP Interface with Port Channel-Based cross connect Tunnel.

Examples

This example shows how to configure CFM over EFP Interface with Port Channel-Based cross connect Tunnel:

```
ASR901(config)#ethernet cfm ieee
ASR901(config)#ethernet cfm global
```

```
ASR901(config)#ethernet cfm domain L5 level 5
ASR901(config-ecfm)# service s1 evc e711
ASR901(config-ecfm-srv)#  continuity-check
ASR901(config-ecfm-srv)#exit
ASR901(config-ecfm)#exit
ASR901(config)#interface GigabitEthernet0/1
ASR901(config-if)# negotiation auto
ASR901(config-if)# no keepalive
ASR901(config-if)# channel-group 1 mode on
ASR901(config-if)#exit
ASR901(config)#interface GigabitEthernet0/7
ASR901(config-if)# negotiation auto
ASR901(config-if)# channel-group 1 mode on
ASR901(config-if)#exit
ASR901(config)#int port-channel 1
ASR901(config-if)#service instance 711 ethernet e711
ASR901(config-if-srv)#  encapsulation dot1q 711
ASR901(config-if-srv)#  xconnect 3.3.3.3 3 encapsulation mpls
ASR901(cfg-if-ether-vc-xconn)#   mtu 1500
ASR901(cfg-if-ether-vc-xconn)#  cfm mep domain L5 mpid 511
```

Verification

Use the following commands to verify a configuration:

- Use the show ethernet cfm maintenance-point local commands to verify the CFM over EVC configuration. This command shows the basic configuration information for CFM.

```
Router-30-PE1#show ethernet cfm maintenance-point local
Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                 Lvl   MacAddress     Type  CC
     Domain Id                                   Dir   Port           Id
     MA Name                                           SrvcInst
     EVC name
--------------------------------------------------------------------------------
1    L6                                          6     000a.f393.56d0 XCON  Y
     L6                                          Down  Gi0/2 N/A
     bbb                                               1
     bbb
3    L5                                          5     0007.8478.4410 XCON  Y
     L5                                          Up    Gi0/2 N/A
     bbb                                               1
     bbb
Total Local MEPs: 2
Local MIPs:
* = MIP Manually Configured
--------------------------------------------------------------------------------
 Level Port          MacAddress     SrvcInst   Type    Id
--------------------------------------------------------------------------------
 7     Gi0/2 0007.8478.4410 1          XCON    N/A
Total Local MIPs: 1
```

- Use the show ethernet cfm maintenance-point remote to verify the MEP configuration:

```
Router-30-PE1#show ethernet cfm maintenance-point remote
--------------------------------------------------------------------------------
MPID  Domain Name                                 MacAddress          IfSt  PtSt
 Lvl  Domain ID                                   Ingress
 RDI  MA Name                                     Type Id             SrvcInst
      EVC Name                                                        Age
--------------------------------------------------------------------------------
```

```
4     L5                                        000a.f393.56d0      Up    Up
 5    L5                                        Te2/0/0:(2.2.2.2, 1)
 -    bbb                                       XCON N/A            1
      bbb                                                           9s
2     L6                                        000a.f393.56d0      Up    Up
 6    L6                                        Te2/0/0:(2.2.2.2, 1)
 -    bbb                                       XCON N/A            1
      bbb                                                           1s
Total Remote MEPs: 2
```

- Use the show ethernet cfm mpdb command to verify the catalouge of CC with MIP in intermediate routers.

```
PE2#show ethernet cfm mpdb
* = Can Ping/Traceroute to MEP
-------------------------------------------------------------------------------------
MPID  Domain Name                               MacAddress          Version
Lvl   Domain ID                                 Ingress
Expd  MA Name                                   Type Id             SrvcInst
      EVC Name                                                      Age
-------------------------------------------------------------------------------------
600 * L6                                        0021.d8ca.d7d0      IEEE-CFM
6     L6                                        Te2/1:(2.2.2.2, 1)
-     s1                                        XCON N/A            1
      1                                                             2s
700   L7                                        001f.cab7.fd01      IEEE-CFM
7     L7                                        Te2/1:(2.2.2.2, 1)
-     s1                                        XCON N/A            1
      1                                                             3s
Total Remote MEPs: 2
```

- Use show ethernet cfm error command to view the error report:

```
PE2#show ethernet cfm error
-------------------------------------------------------------------------------------
MPID Domain Id                                 Mac Address     Type   Id  Lvl
     MAName                                    Reason                 Age
-------------------------------------------------------------------------------------
  -  L3                                        001d.45fe.ca81  BD-V   200  3
     s2                                        Receive AIS            8s
PE2#
```

Configuring CFM with EVC Default Encapsulation

Complete the following steps to configure CFM with EVC default encapsulation:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/9`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**service instance** *instance-id* **ethernet** *evc-name* **Example:** `Router(config-if)# service instance 1 ethernet evc100`	Creates a service instance on an interface and defines the matching criteria. • *instance-id*—Integer that uniquely identifies a service instance on an interface. • *evc-name*—String that associates an EVC to the service instance. Maximum byte size is 100.
Step 5	**encapsulation default** **Example:** `Router(config-if-srv)# encapsulation default`	Configures the default service instance.
Step 6	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 99`	Binds the service instance to a bridge domain instance using an identifier.
Step 7	**cfm encapsulation** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**dot1q** *vlan-id* | **second-dot1q** *vlan-id*] **Example:** `Router(config-if-srv)# cfm encapsulation dot1q 75`	Configures connectivity fault management (CFM) Ethernet frame encapsulation. • **dot1ad**—Indicates the 802.1ad provider bridges encapsulation type. • **dot1q**—Supports the IEEE 802.1q standard for encapsulation of traffic and specifies the outer dot1q encapsulation tag. • **second-dot1q**—Specifies the inner dot1q encapsulation tag. Valid option only when you first select the outer **dot1q** encapsulation tag. When the dot1ad encapsulation type is selected first, **dot1q** is a valid option. • *vlan-id*—Integer from 1 to 4094 that specifies the VLAN on which to send CFM frames.

	Command or Action	Purpose
Step 8	**cfm mep domain** *domain-id* **mpid** *mpid-value* **Example:** `Router(config-if-srv)# cfm mep domain md2 mpid 111`	Configures a maintenance endpoint (MEP) for a domain. • *domain-name*—String from 1 to 154 characters that identifies the domain name. • **mpid**—Indicates the maintenance point ID (MPID). • *mpid-value*—Integer from 1 to 8191 that identifies the MPID.

Verifying CFM with EVC Default Encapsulation

To verify the configuration of CFM with EVC default encapsulation, use the show command shown below.

```
Router# show running-config interface gigabitEthernet 0/9
Building configuration...
Current configuration : 210 bytes
!
interface GigabitEthernet0/9
no ip address
negotiation auto
service instance 1 ethernet evc100
  encapsulation default
  bridge-domain 99
  cfm mep domain md2 mpid 111
  cfm encapsulation dot1q 75
!
end
```

Example: Configuring CFM with EVC Default Encapsulation

```
!
interface GigabitEthernet0/9
service instance 1 ethernet evc100
  encapsulation default
  bridge-domain 99
  cfm encapsulation dot1q 75
  cfm mep domain md2 mpid 111
!
```

Configuring Y.1731 Fault Management

The ITU-T Y.1731 feature provides new CFM functionality for fault and performance management for service providers in large network. The router supports Ethernet Alarm Indication Signal (ETH-AIS) and Ethernet Remote Defect Indication (ETH-RDI) functionality for fault detection, verification, and isolation.

For more information on Y.1731 Fault Management, see
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_y1731.html

To configure Y.1731 fault management, you must enable CFM and configure MIPs on the participating interfaces. AIS messages are generated only on interfaces with a configured MIP.

This section contains the following topics:

Default Y.1731 Configuration

- ETH-AIS is enabled by default when CFM is enabled.
- When you configure ETH-AIS, you must configure CFM before ETH-AIS is operational.
- ETH-RDI is set automatically when continuity check messages are enabled.

Configuring ETH-AIS

Complete the following steps to configure ETH- AIS on the router:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm ais link-status global**	Configure AIS-specific SMEP commands by entering config-ais-link-cfm mode.
Step 3	**level** *level-id* or **disable**	Configure the maintenance level for sending AIS frames transmitted by the SMEP. The range is 0 to 7. or Disable generation of ETH-AIS frames.
Step 4	**period** *value*	Configure the SMEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 7	**service** {*short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id*} {**vlan** *vlan-id* | **port** | **evc** *evc-name*}	Configure the maintenance association and set a universally unique ID for a customer service instance (CSI) or the maintenance association number value, primary VLAN ID and VPN ID within a maintenance domain in Ethernet connectivity fault management (CFM) configuration mode.

	Command or Action	Purpose
Step 8	**ais level** *level-id*	(Optional) Configure the maintenance level for sending AIS frames transmitted by the MEP. The range is 0 to 7.
Step 9	**ais period** *value*	(Optional) Configure the MEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 10	**ais expiry-threshold** *value*	(Optional) Set the expiring threshold for the MA as an integer. The range is 2 to 255. The default is 3.5.
Step 11	**no ais suppress-alarms**	(Optional) Override the suppression of redundant alarms when the MEP goes into an AIS defect condition after receiving an AIS message.
Step 12	**exit**	Return to ethernet-cfm configuration mode.
Step 13	**exit**	Return to global configuration mode.
Step 14	**interface** *interface-id*	Specify an interface ID, and enter interface configuration mode.
Step 15	[**no**] **ethernet cfm ais link-status**	Enable or disable sending AIS frames from the SMEP on the interface.
Step 16	**ethernet cfm ais link-status period** *value*	Configure the ETH-AIS transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds.
Step 17	**ethernet cfm ais link-status level** *level-id*	Configure the maintenance level for sending AIS frames transmitted by the SMEP on the interface. The range is 0 to 7.
Step 18	**end**	Return to privileged EXEC mode.
Step 19	**show ethernet cfm smep** [**interface** *interface-id*]	Verify the configuration.
Step 20	**show ethernet cfm error**	Display received ETH-AIS frames and other errors.
Step 21	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Use the **no** form of this commands to return to the default configuration or to remove a configuration. To disable the generation of ETH-AIS frames, enter the **disable** config-ais-link-cfm mode command.

This is an example of the output from the **show ethernet cfm smep** command when Ethernet AIS has been enabled:

```
Router# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet1/0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

Configuring ETH-LCK

Complete the following steps to configure ethernet locked signal on a switch:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm lck link-status global**	Execute SMEP LCK commands by entering config-lck-link-cfm mode.
Step 3	**level** *level-id* or **disable**	Configure the maintenance level for sending ETH-LCK frames transmitted by the SMEP. The range is 0 to 7. or Disable the generation of ETH-LCK frames.
Step 4	**period** *value*	Configure the SMEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association name or number to be associated with the domain, or a VLAN ID or VPN-ID, and enter ethernet-cfm-service configuration mode. • *ma-name* —a string of no more than 100 characters that identifies the MAID. • *ma-number* —a value from 0 to 65535.

	Command or Action	Purpose
		• *vpn-id* —enter a VPN ID as the *ma-name* . • **vlan** *vlan-id* —VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 8	**lck level** *level-id*	(Optional) Configure the maintenance level for sending ETH-LCK frames sent by the MEP. The range is 0 to 7.
Step 9	**lck period** *value*	(Optional) Configure the MEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds.
Step 10	**lck expiry-threshold** *value*	(Optional) Set the expiring threshold for the MA. The range is 2 to 255. The default is 3.5.
Step 11	**exit**	Return to ethernet-cfm configuration mode.
Step 12	**exit**	Return to global configuration mode.
Step 13	**interface** *interface-id*	Specify an interface ID, and enter interface configuration mode.
Step 14	[**no**] **ethernet cfm lck link-status**	Enable or disable sending ETH-LCK frames from the SMEP on the interface.
Step 15	**ethernet cfm lck link-status period** *value*	Configure the ETH-LCK transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds.
Step 16	**ethernet cfm lck link-status level** *level-id*	Configure the maintenance level for sending ETH-LCK frames sent by the SMEP on the interface. The range is 0 to 7.
Step 17	**end**	Return to privileged EXEC mode.
Step 18	**ethernet cfm lck start interface** *interface-id* **direction** {**up** | **down**} { **drop l2-bpdu**]	(Optional) Apply the LCK condition to an interface. • **interface** *interface-id* —Specify the interface to be put in LCK condition. • **directioninward**—The LCK is in the direction toward the relay; that is, within the switch.

	Command or Action	Purpose
		• **directionoutward**—The LCK is in the direction of the wire. • (Optional) **drop l2-bpdu** specifies that all Layer 2 BPDUs except CFM frames, all data frames, and all Layer 3 control traffic are dropped for that MEP. If not entered, only data frames and Layer 3 control frames are dropped.
Step 19	**show ethernet cfm smep** [**interface** *interface-id*]	Verify the configuration.
Step 20	**show ethernet cfm error**	Display received ETH-LCK frames.
Step 21	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the LCK condition from MEP, enter the **ethernet cfm lck stop mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* privileged EXEC command. To put an interface out of LCK condition, enter the **ethernet cfm lck start interface** *interface-id* **direction** {**inward** | **outward**} privileged EXEC command.

This is an example of the output from the **show ethernet cfm smep** command when ethernet LCK has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

Managing and Displaying Ethernet CFM Information

Use the following commands in the privileged EXEC mode to clear Ethernet CFM information.

Table 10: Clearing CFM Information

Command	Purpose
clear ethernet cfm ais domain *domain-name* **mpid** *id* {**vlan** *vlan-id* | **port**}	Clear MEPs with matching domain and VLAN ID out of AIS defect condition.
clear ethernet cfm ais link-status interface *interface-id*	Clear a SMEP out of AIS defect condition.
clear ethernet cfm error	Clear all CFM error conditions, including AIS.

Use the commands in Table 11: Displaying CFM Information , on page 126 in the privileged EXEC mode to display Ethernet CFM information.

Table 11: Displaying CFM Information

Command	Purpose
show ethernet cfm domain [brief]	Displays CFM domain information or brief domain information.
show ethernet cfm errors [configuration | domain-id]	Displays CFM continuity check error conditions logged on a device since it was last reset or the log was last cleared. When CFM crosscheck is enabled, displays the results of the CFM crosscheck operation.
show ethernet cfm maintenance-points local [detail | domain | interface | level | mep | mip]	Displays maintenance points configured on a device.
show ethernet cfm maintenance-points remote [crosscheck | detail | domain | static]	Displays information about a remote maintenance point domains or levels or details in the CFM database.
show ethernet cfm mpdb	Displays information about entries in the MIP continuity-check database.
show ethernet cfm smep interface *interface-id*	Displays Ethernet CFM SMEP information.
show ethernet cfm traceroute-cache	Displays the contents of the traceroute cache.
show platform cfm	Displays platform-independent CFM information.

This is an example of output from the **show ethernet cfm domain brief** command:

```
Router# show ethernet cfm domain brief
Domain Name                                 Index Level Services Archive(min)
level5                                          1     5        1      100
level3                                          2     3        1      100
test                                            3     3        3      100
name                                            4     3        1      100
test1                                           5     2        1      100
lck                                             6     1        1      100Total Services : 1
```

This is an example of output from the **show ethernet cfm errors** command:

```
Router# show ethernet cfm errors
--------------------------------------------------------------------------------
MPID Domain Id                                       Mac Address     Type    Id  Lvl
     MAName                                          Reason                  Age
--------------------------------------------------------------------------------
6307 level3                                          0021.d7ee.fe80  Vlan    7    3
     vlan7                                           Receive RDI             5s
```

This is an example of output from the **show ethernet cfm maintenance-points local detail** command:

```
Router# show ethernet cfm maintenance-points local detail
Local MEPs:
----------
MPID: 7307
DomainName: level3
Level: 3
Direction: Up
```

```
Vlan: 7
Interface: Gi0/3
CC-Status: Enabled
CC Loss Threshold: 3
MAC: 0021.d7ef.0700
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No
MIP Settings:
-------------
Local MIPs:
* = MIP Manually Configured
------------------------------------------------------------------------------
 Level Port           MacAddress     SrvcInst   Type    Id
------------------------------------------------------------------------------
*5     Gi0/3          0021.d7ef.0700 N/A        Vlan    2,7
```

This is an example of output from the **show ethernet cfm traceroute** command:

```
Router# show ethernet cfm traceroute
Current Cache-size: 0 Hops
Max Cache-size: 100 Hops
Hold-time: 100 Minutes
```

Use the commands in Table 12: Displaying IP SLA CFM Information, on page 127 in the privileged EXEC mode to display IP SLA ethernet CFM information.

Table 12: Displaying IP SLA CFM Information

Command	Purpose
show ip sla configuration *entry-number*]	Displays configuration values including all defaults for all IP SLA operations or a specific operation.
show ip sla ethernet-monitor configuration *entry-number*]	Displays the configuration of the IP SLA automatic ethernet operation.
show ip sla statistics *entry-number* | **aggregated** | **details**]	Display current or aggregated operational status and statistics.

Understanding the Ethernet OAM Protocol

The Ethernet OAM protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sublayer in the data link layer of the OSI model. Normal link operation does not require Ethernet OAM. You can implement Ethernet OAM on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network (specified interfaces).

OAM frames, called OAM protocol data units (OAM PDUs) use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network. Ethernet OAM is a relatively slow protocol, with a maximum transmission rate of 10 frames per second, resulting in minor impact to normal operations. However, when you enable link monitoring, because the CPU must poll error counters frequently, the number of required CPU cycles is proportional to the number of interfaces that must be polled.

Ethernet OAM has two major components:

- The OAM client establishes and manages Ethernet OAM on a link and enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality. After the discovery phase, it manages the rules of response to OAM PDUs and the OAM remote loopback mode.
- The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces facing the superior and inferior MAC sublayers. It provides a dedicated interface for the OAM client to pass OAM control information and PDUs to and from the client. It includes these components:
  - The control block provides the interface between the OAM client and other OAM sublayer internal blocks.
  - The multiplexer manages frames from the MAC client, the control block, and the parser and passes OAM PDUs from the control block and loopback frames from the parser to the subordinate layer.
  - The parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and sends them to the appropriate entity: OAM PDUs to the control block, MAC client frames to the superior sublayer, and loopback frames to the multiplexer.

Benefits of Ethernet OAM

Ethernet OAM provides the following benefits:

- Competitive advantage for service providers
- Standardized mechanism to monitor the health of a link and perform diagnostics

OAM Features

The following OAM features are defined by IEEE 802.3ah:

Discovery

Discovery is the first phase of Ethernet OAM and it identifies the devices in the network and their OAM capabilities. Discovery uses information OAM PDUs. During the discovery phase, the following information is advertised within periodic information OAM PDUs:

- OAM mode—Conveyed to the remote OAM entity. The mode can be either active or passive and can be used to determine device functionality.
- OAM configuration (capabilities)—Advertises the capabilities of the local OAM entity. With this information a peer can determine what functions are supported and accessible; for example, loopback capability.
- OAM PDU configuration—Includes the maximum OAM PDU size for receipt and delivery. This information along with the rate limiting of 10 frames per second can be used to limit the bandwidth allocated to OAM traffic.
- Platform identity—A combination of an organization unique identifier (OUI) and 32-bits of vendor-specific information. OUI allocation, controlled by the IEEE, is typically the first three bytes of a MAC address.

Discovery includes an optional phase in which the local station can accept or reject the configuration of the peer OAM entity. For example, a node may require that its partner support loopback capability to be accepted into the management network. These policy decisions may be implemented as vendor-specific extensions.

Link Monitoring

Link monitoring in Ethernet OAM detects and indicates link faults under a variety of conditions. Link monitoring uses the event notification OAM PDU and sends events to the remote OAM entity when there are problems detected on the link. The error events include the following:

- Error Symbol Period (error symbols per second)—The number of symbol errors that occurred during a specified period exceeded a threshold. These errors are coding symbol errors.
- Error Frame (error frames per second)—The number of frame errors detected during a specified period exceeded a threshold.
- Error Frame Period (error frames per n frames)—The number of frame errors within the last n frames has exceeded a threshold.
- Error Frame Seconds Summary (error seconds per m seconds)—The number of error seconds (1-second intervals with at least one frame error) within the last m seconds has exceeded a threshold.

Since IEEE 802.3ah OAM does not provide a guaranteed delivery of any OAM PDU, the event notification OAM PDU may be sent multiple times to reduce the probability of a lost notification. A sequence number is used to recognize duplicate events.

Remote Failure Indication

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. The following failure conditions can be communicated:

- Link Fault—Loss of signal is detected by the receiver; for instance, the peer's laser is malfunctioning. A link fault is sent once per second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.
- Dying Gasp—This notification is sent for power failure, link down, router reload and link administratively down conditions. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.
- Critical Event—An unspecified critical event occurs. This type of event is vendor specific. A critical event may be sent immediately and continuously.

Remote Loopback

An OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

The loopback command is acknowledged by responding with an information OAM PDU with the loopback state indicated in the state field. This acknowledgement allows an administrator, for example, to estimate if a network segment can satisfy a service-level agreement. Acknowledgement makes it possible to test delay, jitter, and throughput.

When an interface is set to the remote loopback mode the interface no longer participates in any other Layer 2 or Layer 3 protocols; for example Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). The reason is that when two connected ports are in a loopback session, no frames other than the OAM PDUs are sent to the CPU for software processing. The non-OAM PDU frames are either looped back at the MAC level or discarded at the MAC level.

From a user's perspective, an interface in loopback mode is in a link-up state.

Cisco Vendor-Specific Extensions

Ethernet OAM allows vendors to extend the protocol by allowing them to create their own type-length-value (TLV) fields.

OAM Messages

Ethernet OAM messages or OAM PDUs are standard length, untagged Ethernet frames within the normal frame length bounds of 64 to 1518 bytes. The maximum OAM PDU frame size exchanged between two peers is negotiated during the discovery phase.

OAM PDUs always have the destination address of slow protocols (0180.c200.0002) and an Ethertype of 8809. OAM PDUs do not go beyond a single hop and have a hard-set maximum transmission rate of 10 OAM PDUs per second. Some OAM PDU types may be transmitted multiple times to increase the likelihood that they will be successfully received on a deteriorating link.

Four types of OAM messages are supported:

- Information OAM PDU—A variable-length OAM PDU that is used for discovery. This OAM PDU includes local, remote, and organization-specific information.
- Event notification OAM PDU—A variable-length OAM PDU that is used for link monitoring. This type of OAM PDU may be transmitted multiple times to increase the chance of a successful receipt; for example, in the case of high-bit errors. Event notification OAM PDUs also may include a time stamp when generated.
- Loopback control OAM PDU—An OAM PDU fixed at 64 bytes in length that is used to enable or disable the remote loopback command.
- Vendor-specific OAM PDU—A variable-length OAM PDU that allows the addition of vendor-specific extensions to OAM.

For instructions on how to configure Ethernet Link OAM, see Setting Up and Configuring Ethernet OAM, on page 130.

Setting Up and Configuring Ethernet OAM

This section includes the following topics:

Default Ethernet OAM Configuration

- Ethernet OAM is disabled on all interfaces.
- When Ethernet OAM is enabled on an interface, link monitoring is automatically turned on.
- Remote loopback is disabled.
- No Ethernet OAM templates are configured.

Restrictions and Guidelines

Follow these guidelines when configuring Ethernet OAM:

- The router does not support monitoring of egress frames sent with cyclic redundancy code (CDC) errors. The **ethernet oam link-monitor transmit crc** interface-configuration or template-configuration commands are visible but are not supported on the router. The commands are accepted, but are not applied to an interface.
- For a remote failure indication, the router does not generate link fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The router supports generating and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, the router is reloading, or during power failure.
- Effective with Cisco IOS Release 15.3(2)S, the Cisco ASR 901 router supports sub-second OAM timers.
- The Cisco ASR 901 router supports up to two Ethernet OAM sessions with sub-second OAM timers.
- Ethernet OAM sessions with sub-second OAM timers reduce the scalability for Ethernet CFM sessions.

Enabling Ethernet OAM on an Interface

Complete the following steps to enable Ethernet OAM on an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**interface** *interface-id*	Defines an interface to configure as an Ethernet OAM interface, and enters interface configuration mode.
Step 3	**ethernet oam**	Enables Ethernet OAM on the interface.

Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* **ms** **mode** {**active** **passive**} **timeout** *seconds* [**ms**]]	Configures the OAM parameters:
		• **max-rate**—(Optional) Configures the maximum number of OAM PDUs sent per second.
		• *oampdus* —The range is from 1 to 10.
		• **min-rate**— (Optional) Configures the minimum transmission rate when one OAM PDU is sent per second.
		• *seconds* —The range is as follows:
		  • 1 to 10 seconds
		  • 100 to 900 milliseconds (multiples of 100)
		• **ms**—Specifies the minimum transmission rate value in milliseconds.
		• **mode active**—(Optional) Sets OAM client mode to active.
		• **mode passive**—(Optional) Sets OAM client mode to passive.
		Note

	Command or Action	Purpose

		When Ethernet OAM mode is enabled on two interfaces passing traffic, at least one must be in the active mode.
		• **timeout**—(Optional) Sets a time for OAM client timeout.
		• *seconds* —The range is as follows:
		  • 2 to 30 seconds
		  • 500 to 1900 milliseconds (multiples of 100)
		• **ms**—Specifies the timeout value in milliseconds.

Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show ethernet oam status** [**interface** *interface-id*	Verifies the configuration.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

What to do next

Use the **no ethernet oam** interface configuration command to disable Ethernet OAM on the interface.

Configuration Example

The following example shows how to configure an Ethernet OAM session with sub-second OAM timers on an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ethernet oam
Router(config-if)# ethernet oam min-rate 100 ms
Router(config-if)# ethernet oam timeout 500 ms
Router(config-if)# end
```

Enabling Ethernet OAM Remote Loopback

Enable Ethernet OAM remote loopback on an interface for the local OAM client to initiate OAM remote loopback operations. Changing this setting causes the local OAM client to exchange configuration information with its remote peer. Remote loopback is disabled by default.

Restrictions

- Internet Group Management Protocol (IGMP) packets are not looped back.
- If dynamic ARP inspection is enabled, ARP or reverse ARP packets are not looped or dropped.

Complete the following steps to enable Ethernet OAM remote loopback on an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface** *type number*	Define an interface to configure as an EOM interface, and enter interface configuration mode.
Step 3	**ethernet oam remote-loopback** {**supported** | **timeout** *type number*}	Enable Ethernet remote loopback on the interface or set a loopback timeout period. • Enter **supported** to enable remote loopback. • Enter **timeout** *type number* to set a remote loopback timeout period. The range is from 1 to 10 seconds.
Step 4	**end**	Return to the privileged EXEC mode.
Step 5	**ethernet oam remote-loopback** {**start** | **stop**} {**interface** *type number*}	Turn on or turn off Ethernet OAM remote loopback on an interface.
Step 6	**show ethernet oam status** [**interface***type number*	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Use the **no ethernet oam remote-loopback** {**supported** | **timeout**} interface configuration command to disable remote loopback support or remove the timeout setting.

Configuring Ethernet OAM Link Monitoring

You can configure high and low thresholds for link-monitoring features. If no high threshold is configured, the default is **none** —no high threshold is set. If you do not set a low threshold, it defaults to a value lower than the high threshold.

Complete the following steps to configure Ethernet OAM link monitoring on an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.

	Command or Action	Purpose
Step 3	**ethernet oam link-monitor supported**	Enable the interface to support link monitoring. This is the default. You need to enter this command only if it has been disabled by previously entering the **no ethernet oam link-monitor supported** command.
Step 4	**ethernet oam link-monitor high-threshold action** {**error-disable-interface** | **failover**}	Use the **ethernet oam link-monitor high-threshold** command to configure an error-disable function on the Ethernet OAM interface when a high threshold for an error is exceeded. **Note** Release 15.0(1)MR does not support the **failover** keyword.
Step 5	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*}	**Note** Repeat this step to configure both high and low thresholds. (Optional) Configure high and low thresholds for an error-symbol period that trigger an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.
Step 6	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames* }} | **window** *milliseconds*}	**Note** Repeat this step to configure both high and low thresholds. (Optional) Configure high and low thresholds for error frames that trigger an error-frame link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. The default is **none**.

	Command or Action	Purpose
		• Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 7	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	**Note** Repeat this step to configure both high and low thresholds. (Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.
Step 8	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	**Note** Repeat this step to configure both high and low thresholds. (Optional) Configure high and low thresholds for the frame-seconds error that triggers an error-frame-seconds link event. • Enter **threshold high** *high-frames* to set a high error frame-seconds threshold in number of seconds. The range is 1 to 900. The default is none. • Enter **threshold high none** to disable the high threshold if it was set. This is the default.

	Command or Action	Purpose
		• Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter **window** *frames* to set the a polling window size in number of milliseconds. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.
Step 9	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* **none**} | **low** { *low-frames* }} | **window** *milliseconds*}	**Note** Repeat this step to configure both high and low thresholds. (Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 10	**ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*highframes* | **none**} | **low** *low-frames*} | **window** *milliseconds*}}	Use the **ethernet oam link-monitor transmit-crc** command to configure an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time.
Step 11	**[no] ethernet link-monitor on**	(Optional) Start or stop (when the **no** keyword is entered) link-monitoring operations on the interface. Link monitoring operations start automatically when support is enabled.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The **ethernet oam link-monitor transmit-crc threshold high** *high-frames* **none**} | **low** *low-frames*}} | **window** *milliseconds*} command is visible on the router and you are allowed to enter it, but it is not supported. Use the **no** form of this commands to disable the configuration. Use the **no** form of each command to disable the threshold setting.

Configuring Ethernet OAM Remote Failure Indications

You can configure an error-disable action to occur on an interface if one of the high thresholds is exceeded, if the remote link goes down, if the remote device is rebooted, if the remote device disables Ethernet OAM on the interface, or if the power failure occurs on the remote device .

Complete the following steps to enable Ethernet OAM remote-failure indication actions on an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.
Step 3	**ethernet oam remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action error-disable-interface**	Configure the Ethernet OAM remote-failure action on the interface. You can configure disabling the interface for one of these conditions: • Select **critical-event** to shut down the interface when an unspecified critical event has occurred. • Select **dying-gasp** to shut down the interface when Ethernet OAM is disabled or the interface enters the error-disabled state. • Select **link-fault** to shut down the interface when the receiver detects a loss of signal.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The router does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The router supports sending and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the router is reloading. It can respond to and generate Dying Gasp PDUs based on loss of power. Use the **no ethernet remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** command to disable the remote failure indication action.

Configuring Ethernet OAM Templates

You can create a template for configuring a common set of options on multiple Ethernet OAM interfaces. The template can be configured to monitor frame errors, frame-period errors, frame-second errors, received CRS errors, and symbol-period errors and thresholds. You can also set the template to put the interface in error-disabled state if any high thresholds are exceeded. These steps are optional and can be performed in any sequence or repeated to configure different options.

Complete the following steps to configure an Ethernet OAM template and to associate it with an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**template** *template-name*	Create a template, and enter template configuration mode.
Step 3	**ethernet oam link-monitor receive-crc** {**threshold** {**high** *high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter the **threshold high** *high-frames* command to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter the **threshold high none** command to disable the high threshold. • Enter the **threshold low** *low-frames* command to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter the **window** *milliseconds* command to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*}	(Optional) Configure high and low thresholds for an error-symbol period that triggers an error-symbol period link event. • Enter the **threshold high** *high-symbols* command to set a high threshold in number of symbols. The range is 1 to 65535. • Enter the **threshold high none** command to disable the high threshold. • Enter the **threshold low** *low-symbols* command to set a low threshold in

	Command or Action	Purpose
		number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter the **window** *symbols* command to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.
Step 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event. • Enter the **threshold high** *high-frames* command to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter the **threshold high none** command to disable the high threshold. • Enter the **threshold low** *low-frames* command to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter the **window** *milliseconds* command to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in a multiple of 100. The default is 100.
Step 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter the **threshold high** *high-frames* command to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter the **threshold high none** command to disable the high threshold. • Enter the **threshold low** *low-frames* command to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter the **window** *frames* command to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.

	Command or Action	Purpose
Step 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-seconds* | **none**} | **low**{ *low-seconds* }} | **window** *milliseconds*}	(Optional) Configure frame-seconds high and low thresholds for triggering an error-frame-seconds link event. • Enter the **threshold high** *high-seconds* command to set a high threshold in number of seconds. The range is 1 to 900. You must enter a high threshold. • Enter the **threshold high none** command to disable the high threshold. • Enter the **threshold low** *low-frames* command to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter the **window** *frames* command to set the a polling window size in number of frames. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.
Step 8	**ethernet oam link-monitor high threshold action error-disable-interface**	(Optional) Configure the router to move an interface to the error disabled state when a high threshold for an error is exceeded.
Step 9	**exit**	Return to global configuration mode.
Step 10	**interface** *interface-id*	Define an Ethernet OAM interface, and enter interface configuration mode.
Step 11	**source-template** *template-name*	Associate the template to apply the configured options to the interface.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The router does not support monitoring egress frames with CRC errors. The **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*}} | **window** *milliseconds*} command is visible on the router and you can enter it, but it is not supported. Use the **no** form of each command to remove the option from the template. Use the **no source-template** *template-name* to remove the source template association.

Configuration Example

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)# interface gigabitEthernet 0/8
Router(config-if)# ethernet oam

Router(config-if)# ethernet oam link-monitor symbol-period threshold high 299
Router(config-if)# ethernet oam link-monitor frame window 399
Router(config-if)# ethernet oam link-monitor frame-period threshold high 599
Router(config-if)# ethernet oam link-monitor frame-seconds window 699
Router(config-if)# ethernet oam link-monitor receive-crc window 99
Router(config-if)# ethernet oam link-monitor transmit-crc threshold low 199
Router(config-if)# ethernet oam link-monitor high-threshold action error-disable-interface
Router(config-if)# end
Router# show running-config
interface gigabitEthernet 0/8
Building configuration...
Current configuration : 478 bytes
!
interface GigabitEthernet0/8
no ip address
negotiation auto
ethernet oam link-monitor symbol-period threshold high 299
ethernet oam link-monitor frame window 399
ethernet oam link-monitor frame-period threshold high 599
ethernet oam link-monitor frame-seconds window 699
ethernet oam link-monitor receive-crc window 99
ethernet oam link-monitor transmit-crc threshold low 199
ethernet oam link-monitor high-threshold action error-disable-interface
ethernet oam
end
```

Displaying Ethernet OAM Protocol Information

Use these commands in the privileged EXEC to display the Ethernet OAM protocol information.

Table 13: Displaying Ethernet OAM Protocol Information

Command	Purpose
show ethernet oam discovery [**interface** *interface-id*	Displays discovery information for all Ethernet OAM interfaces or the specified interface.
show ethernet oam statistics [**interface** *interface-id*	Displays detailed information about Ethernet OAM packets.
show ethernet oam status [**interface** *interface-id*	Displays Ethernet OAM configuration for all interfaces or the specified interface.
show ethernet oam summary	Displays active Ethernet OAM sessions on the router.

Verifying Ethernet OAM Configuration

Verifying an OAM Session

To verify an OAM session, use the **show ethernet oam summary** command.

In the following example, the local client interface is in session with a remote client with MAC address 442b.0348.bc60 and organizationally unique identifier (OUI) 00000C, which is the OUI for Cisco Systems.

The remote client is in active mode, and has established capabilities for link monitoring and remote loopback for the OAM session.

```
Router# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
                  & - Error Block State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval
  Local                        Remote
Interface       MAC Address    OUI    Mode    Capability
  Gi0/8         442b.0348.bc60 00000C active    L R
```

Verifying OAM Discovery Status

To verify OAM Discovery status on the local client and remote peer, use the **show ethernet oam discovery** command as shown in the following example:

```
Router# show ethernet oam discovery interface gigabitethernet 0/8
GigabitEthernet0/8
Local client
------------
  Administrative configurations:
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported (on)
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
  Operational status:
    Port status:       operational
    Loopback status:   no loopback
    PDU revision:      0
Remote client
-------------
  MAC address: 442b.0348.bc60
  Vendor(oui): 00000C(cisco)
  Administrative configurations:
    PDU revision:      0
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
```

Verifying Information OAMPDU and Fault Statistics

To verify statistics for information OAMPDUs and local and remote faults, use the **show ethernet oam statistics** command as shown in the following example:

```
Router# show ethernet oam statistics interface gigabitethernet  0/8
GigabitEthernet0/8
Counters:
---------
  Information OAMPDU Tx                    : 5549
  Information OAMPDU Rx                    : 5914
  Unique Event Notification OAMPDU Tx     : 0
  Unique Event Notification OAMPDU Rx     : 0
  Duplicate Event Notification OAMPDU TX  : 0
  Duplicate Event Notification OAMPDU RX  : 0
```

```
  Loopback Control OAMPDU Tx              : 0
  Loopback Control OAMPDU Rx              : 0
  Variable Request OAMPDU Tx              : 0
  Variable Request OAMPDU Rx              : 0
  Variable Response OAMPDU Tx             : 0
  Variable Response OAMPDU Rx             : 0
  Cisco OAMPDU Tx                         : 1
  Cisco OAMPDU Rx                         : 0
  Unsupported OAMPDU Tx                   : 0
  Unsupported OAMPDU Rx                   : 0
  Frames Lost due to OAM                  : 0
Local Faults:
-------------
  0 Link Fault records
  1 Dying Gasp records
    Total dying gasps       : 1
    Time stamp              : 23:27:13
  0 Critical Event records
Remote Faults:
--------------
  0 Link Fault records
  0 Dying Gasp records
  0 Critical Event records
Local event logs:
-----------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records
Remote event logs:
------------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records
```

Verifying Link Monitoring Configuration and Status

To verify link monitoring configuration and status on the local client, use the **show ethernet oam status** command. The Status field in the following example shows that link monitoring status is supported and enabled (on).

```
Router# show ethernet oam status interface gigabitethernet  0/8
GigabitEthernet0/8
General
-------
  Admin state:           enabled
  Mode:                  active
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1000 ms
  Link timeout:          5000 ms
  High threshold action: error disable interface
  Link fault action:     no action
  Dying gasp action:     no action
  Critical event action: no action
Link Monitoring
---------------
  Status: supported (on)
  Symbol Period Error
    Window:              100 x 1048576 symbols
    Low threshold:       1 error symbol(s)
    High threshold:      299 error symbol(s)
```

```
  Frame Error
    Window:              400 x 100 milliseconds
    Low threshold:       1 error frame(s)
    High threshold:      none
  Frame Period Error
    Window:              1000 x 10000 frames
    Low threshold:       1 error frame(s)
    High threshold:      599 error frame(s)
  Frame Seconds Error
    Window:              700 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none
```

Verifying Status of the Remote OAM Client

To verify the status of a remote OAM client, use the **show ethernet oam summary** and **show ethernet oam status** commands.

To verify the remote client mode and capabilities for the OAM session, use the **show ethernet oam summary** command and observe the values in the Mode and Capability fields. The following example shows that the local client (local interface Gi0/8) is connected to the remote client

```
Router# show ethernet oam summary
Symbols:           * - Master Loopback State,  # - Slave Loopback State
                   & - Error Block State
Capability codes: L - Link Monitor,  R - Remote Loopback
                   U - Unidirection,  V - Variable Retrieval
  Local                        Remote
Interface       MAC Address    OUI    Mode    Capability
  Gi0/8         442b.0348.bc60 00000C active   L R
```

Understanding E-LMI

Ethernet Local Management Interface (E-LMI) is a protocol between the customer-edge (CE) device and the provider-edge (PE) device. It runs only on the PE-to-CE UNI link and notifies the CE device of connectivity status and configuration parameters of Ethernet services available on the CE port. E-LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level (UPE to UPE with inward-facing MEPs at the UNI).

OAM manager, which streamlines interaction between any two OAM protocols, handles the interaction between CFM and E-LMI. This interaction is unidirectional, running only from OAM manager to E-LMI on the UPE side of the router. Information is exchanged either as a result of a request from E-LMI or triggered by OAM when it received notification of a change from the OAM protocol. This type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

You can configure Ethernet virtual connections (EVCs), service VLANs, UNI ids (for each CE-to-PE link), and UNI count and attributes. You need to configure CFM to notify the OAM manager of any change to the number of active UNIs and or the remote UNI ID for a given S-VLAN domain.

You can configure the router as a provider-edge device.

Restrictions

E-LMI is not supported for the service instances in which the pseudowire cross-connects are configured.

Configuring E-LMI

For E-LMI to work with CFM, you configure EVCs, EFPs, and E-LMI customer VLAN mapping. Most of the configuration occurs on the PE device on the interfaces connected to the CE device. On the CE device, you only need to enable E-LMI on the connecting interface. Note that you must configure some OAM parameters, for example, EVC definitions, on PE devices on both sides of a metro network.

This section contains the following topics:

Default E-LMI Configuration

Ethernet LMI is globally disabled by default. When enabled, the router is in provider-edge (PE) mode by default.

When you globally enable E-LMI by entering the **ethernet lmi global** global configuration command, it is automatically enabled on all interfaces. You can also enable or disable E-LMI per interface to override the global configuration. The E-LMI command that is given last is the command that has precedence.

There are no EVCs, EFP service instances, or UNIs defined.

UNI bundling service is bundling with multiplexing.

Enabling E-LMI

You can enable E-LMI globally or on an interface and you can configure the router as a PE device. Beginning in privileged EXEC mode, follow these steps to enable for E-LMI on the router or on an interface. Note that the order of the global and interface commands determines the configuration. The command that is entered last has precedence.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**ethernet lmi global**	Globally enable E-LMI on all interfaces. By default, the router is a PE device.
Step 3	**interface** *type number*	Define an interface to configure as an E-LMI interface, and enter interface configuration mode.
Step 4	**ethernet lmi interface**	Configure Ethernet LMI on the interface. If E-LMI is enabled globally, it is enabled on all interfaces unless you disable it on specific interfaces. If E-LMI is disabled globally, you can use this command to enable it on specified interfaces.

	Command or Action	Purpose
Step 5	**ethernet lmi** {**n391***type number* | **n393***type number*| **t391** *value* | **t392***type number*}	Configure E-LMI parameters for the UNI. The keywords have these meanings: • **n391** *type number*—Set the event counter on the customer equipment. The counter polls the status of the UNI and all Ethernet virtual connections (EVCs). The range is from 1 to 65000; the default is 360. • **n393** *type number*—Set the event counter for the metro Ethernet network. The range is from 1 to 10; the default is 4. • **t391** *type number*—Set the polling timer on the customer equipment. A polling timer sends status enquiries and when status messages are not received, records errors. The range is from 5 to 30 seconds; the default is 10 seconds. • **t392** *type number*—Set the polling verification timer for the metro Ethernet network or the timer to verify received status inquiries. The range is from 5 to 30 seconds, or enter 0 to disable the timer. The default is 15 seconds. **Note** The **t392** keyword is not supported when the router is in CE mode.
Step 6	**end**	Return to the privileged EXEC mode.
Step 7	**show ethernet lmi evc**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Use the **no ethernet lmi** global configuration command to globally disable E-LMI. Use the **no** form of the **ethernet lmi** interface configuration command with keywords to disable E-LMI on the interface or to return the timers to the default settings.

Use the **show ethernet lmi** commands to display information that was sent to the CE from the status request poll. Use the **show ethernet service** commands to show current status on the device.

Displaying E-LMI Information

Use the following commands in privileged EXEC mode to display E-LMI information.

Table 14: Displaying E-LMI Information

Command	Purpose
show ethernet lmi evc [**detail** *evc-id* [**interface** *interface-id*] | **map interface** *type number*]	Displays details sent to the CE from the status request poll about the E-LMI EVC.
show ethernet lmi parameters interface *interface-id*	Displays Ethernet LMI interface parameters sent to the CE from the status request poll.
show ethernet lmi statistics interface *interface-id*	Displays Ethernet LMI interface statistics sent to the CE from the status request poll.
show ethernet lmi uni map interface [*interface-id*]	Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.
show ethernet service instance detail | id *efp-identifier* **interface** *interface-id* | **interface** *interface-id*	Displays information relevant to the specified Ethernet service instances (EFPs).

Understanding Ethernet Loopback

The local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, and Gigabit Ethernet interfaces connect to a remote system. The Loopback command is used to place the interface in loopback mode. You can use per-port and per EFP Ethernet loopback to test connectivity at initial startup, to test throughput, and to test quality of service in both directions. The RFC2544 for latency testing specifies that the throughput must be measured by sending frames at increasing rate, representing the percentage of frames received as graphs, and reporting the frames dropping rate. This rate is dependent on the frame size. This throughput measurement at traffic generator requires the ethernet loopback support on the responder.

Ethernet loopback can be achieved with External or Internal loopback. External loopback is the process of looping frames coming from the port on the wire side. Internal loopback is the process of looping frames coming from the port on the relay side.

Configuring Ethernet Loopback

This section contains the following topics:

Restrictions

- Ethernet loopback is not supported on a routed port.
- A single terminal session is initiated at a time over a cross connect or bridge domain.
- The maximum total traffic that can be looped back across all sessions combined, is 1GB.
- For an internal loopback over bridge domain, the traffic for loopback must have encapsulation that matches the egress encapsulation. If there is a rewrite operation on the egress EFP, the traffic post the operation must match the EFP encapsulation.
- Dot1q tag-based filtering is not available on the Cisco ASR 901 router.
- Internal Loopback over bridge domain cannot be initiated if SPAN is already active.
- Internal Loopback over bridge domain cannot be initiated if Traffic generator is already active.
- Loopback is not supported on Fast Ethernet interface.

- External loopback is not supported on EFP with VLAN range.
- Source and destination address specified in the EXEC command are the MAC fields. These addresses are used for MAC swap. The source and destination MAC addresses cannot be identical or multicast MAC addresses.
- Source MAC address is mandatory.
- External loopback is only supported over bridge domain.
- Internal loopback is not supported over a port-channel interface
- When Ethernet Loopback is enabled, the L2CP forward and L2CP tunnel protocols are not functional on any ports.
- Internal loopback over cross connect cannot be initiated if the Traffic Generator is already active.

Enabling Ethernet Loopback

Complete the following steps to configure Ethernet Loopback on the Cisco ASR 901 router:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitEthernet0/1`	Specifies an interface type and number to enter the interface configuration mode.
Step 4	**service instance instance-number ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Creates a service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dotlq-number** **Example:** `Router(config-if-srv)# encapsulation dot1q 10`	Defines the matching criteria to be used in order to map the ingress dot1q frames on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance. Go to Step 7 if you want to configure Ethernet loopback for a bridge-domain. Go to Step 8 if you want to configure Ethernet loopback for cross connect.
Step 7	**bridge domain-number** **Example:** `Router(config-if-srv)# bridge domain 10`	Binds the service instance to a bridge domain. Perform this step if you want to configure Ethernet loopback for a bridge-domain.
Step 8	**xconnect peer-ip-address vc-id encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 1.1.1.1 100 encapsulation mpls`	Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire. Perform this step if you want to configure Ethernet loopback for cross connect. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers. • *encapsulation*—Specifies the tunneling method to encapsulate the data in the pseudowire. • *mpls*—Specifies MPLS as the tunneling method.
Step 9	ethernet loopback permit external **Example:** `Router(config-if-srv)# ethernet loopback permit external`	Configures Ethernet permit external loopback on an interface. External loopback allows loopback of traffic from the wire side. This command is supported under a service instance and interface.
Step 10	ethernet loopback permit internal **Example:** `Router(config-if-srv)# ethernet loopback permit internal`	Configures Ethernet permit internal loopback on an interface. Internal loopback allows loopback of traffic from the relay side. This command is supported under a service instance and interface.
Step 11	**end** **Example:** `Router(config-if-srv)# end`	Returns to the privileged EXEC mode.

	Command or Action	Purpose
Step 12	**ethernet loopback start local interface type number service instance instance-number { external | internal } source mac-address source mac-address [destination mac-address destination-mac-address] [timeout {time-in-seconds | none}]** **Example:** `Router#` **`ethernet loopback start local interface gigabitEthernet 0/1 service instance 10 external source mac-address 0123.4567.89ab destination mac-address 255.255.255 timeout 9000`**	Starts Ethernet external or internal loopback process on the service instance. Destination MAC address is an optional field. If destination mac address is not provided, the loopback interface MAC address is assigned to the source MAC address after swapping. • *(Optional)* Use the **timeout** *time-in-seconds* command to set a loopback timeout period. The range is from 1 to 90000 seconds (25 hours). The default value is 300 seconds. • *(Optional)* Use the timeout none command to set the loopback to no time out.
Step 13	**ethernet loopback stop local interface type number id session id** **Example:** `Router#` **`ethernet loopback stop local interface gigabitEthernet 0/1 id 3`**	Stops Ethernet loopback.

Configuration Example

This example shows how to configure Ethernet External Loopback for a bridge-domain:

```
!
interface GigabitEthernet0/0
service instance 201 ethernet evc201
encapsulation dot1q 201
rewrite ingress tag pop 1 symmetric
bridge-domain 201
ethernet loopback permit external
ethernet loopback permit internal
!
ethernet loopback  start  local  interface GigabitEthernet0/0 service instance 201  external
  source mac-address 5000.10a1.6ab8  destination mac-address 0000.0000.0202 timeout 9000
!
!
ethernet loopback stop local interface gigabitEthernet 0/0 id 1
!
```

This example shows how to configure Ethernet Internal Loopback for cross connect:

```
!
interface GigabitEthernet0/0
service instance 201 ethernet evc201
encapsulation dot1q 201
rewrite ingress tag pop 1 symmetric
xconnect 2.2.2.2 10 encapsulation mpls
```

```
ethernet loopback permit external
ethernet loopback permit internal
!
ethernet loopback  start  local  interface GigabitEthernet0/0 service instance 201  internal
  source mac-address 5000.10a1.6ab8  destination mac-address 0000.0000.0202 timeout 9000
!
!
ethernet loopback stop local interface gigabitEthernet 0/0 id 1
!
```

This following is the example of the output from the **show ethernet loopback** command:

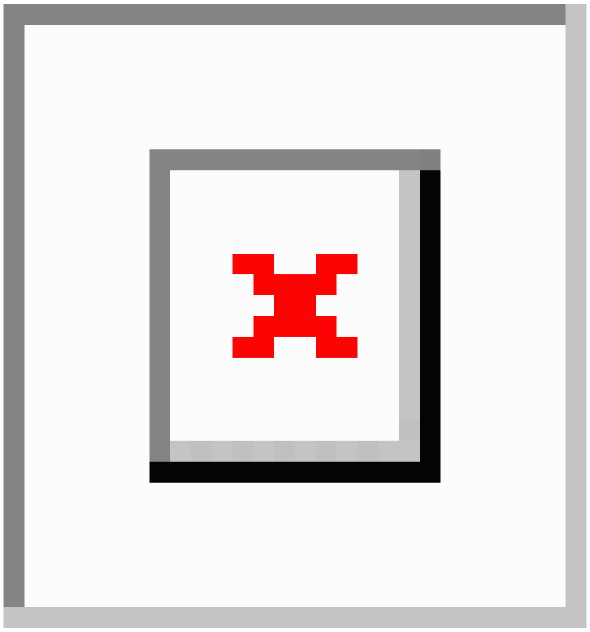
```
Router# show ethernet loopback active interface GigabitEthernet0/0 service instance 201
Loopback Session ID     : 1
Interface               : GigabitEthernet0/0
Service Instance        : 201
Direction               : Internal
Time out(sec)           : 300
Status                  : on
Start time              : 12:06:35.300 IST Mon Sep 23 2013
Time left               : 00:03:28
Dot1q/Dot1ad(s)         : 201
Second-dot1q(s)         :
Source Mac Address      : 5000.10a1.6ab8
Destination Mac Address : 0000.0000.0202
Ether Type              : Any
Class of service        : Any
Llc-oui                 : Any
Total Active Session(s): 1
Total Internal Session(s): 1
Total External Session(s): 0
```

Configuring Y.1564 to Generate Ethernet Traffic

Y.1564 is an Ethernet service activation or performance test methodology for turning up, installing, and troubleshooting Ethernet-based services. This test methodology allows for complete validation of Ethernet service-level agreements (SLAs) in a single test. Using traffic generator performance profile, you can create the traffic based on your requirements. The network performance like throughput, loss, and availability are analyzed using Layer 2 traffic with various bandwidth profiles. Availability is inversely proportional to frame loss ratio.

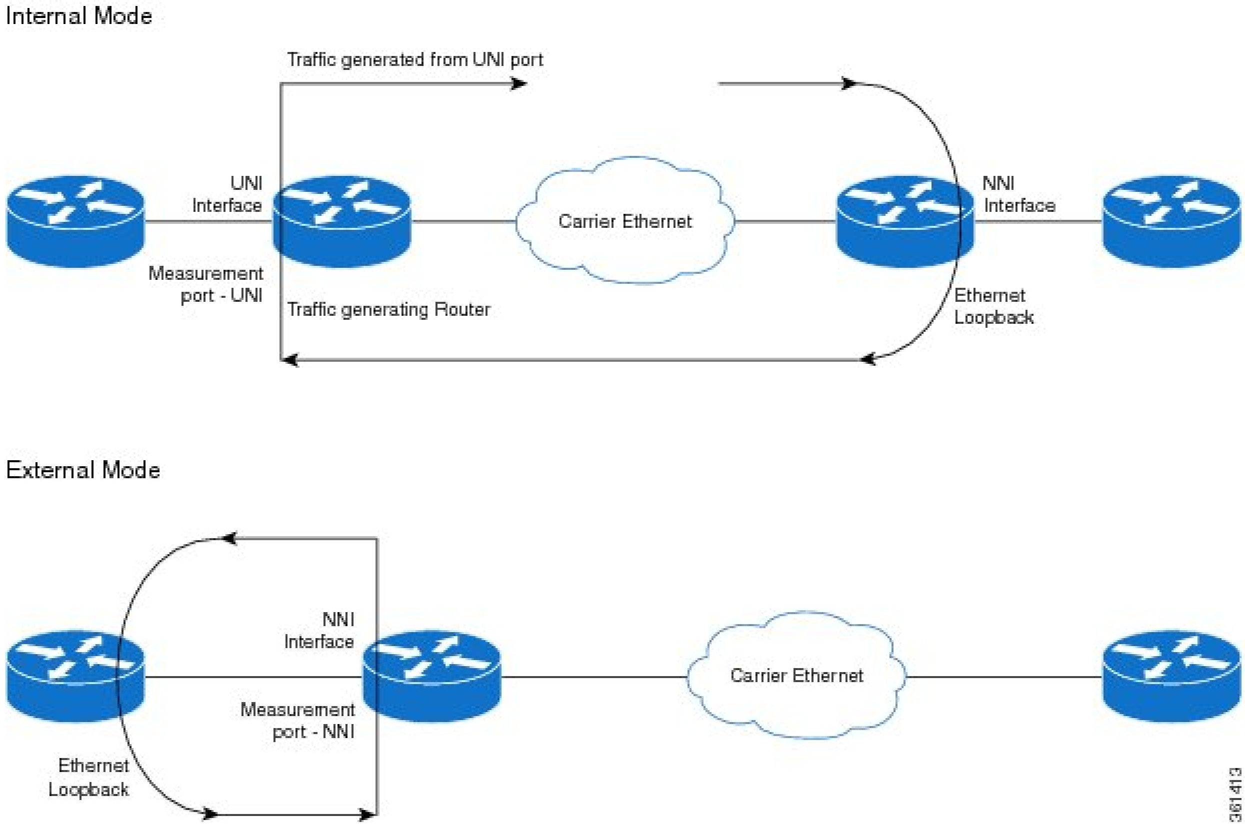
The following figure shows the Traffic Generator topology over bridge domain describing the traffic flow in the external and internal modes. The traffic is generated at the wire-side of network to network interface (NNI) and is transmitted to the responder through the same interface for the external mode. The traffic is generated at the user to network interface (UNI) and transmitted to the responder through NNI respectively for the internal mode. External mode is used to measure the throughput and loss at the NNI port where as internal mode is used to measure the throughput and loss at the UNI port. During traffic generation, traffic at other ports is not impacted by the generated traffic and can continue to switch network traffic.

Figure 4: Traffic Generator Topology over Bridge Domain



Effective with Cisco IOS release 15.4.(01)S, traffic can be generated over cross connect interface. The following figure shows the Traffic Generator topology over cross connect describing the traffic flow in the external and internal modes.

Figure 5: Traffic Generator Topology over cross connect



To generate traffic using Y.1564, complete the following tasks:

- Configure EVC on the interface path such that the Layer 2/L2VPN path should be complete between transmitter and receiver.
- Configure Traffic Generator on the transmitter.
- Configure ethernet loopback on the receiver. For information on Ethernet loopback, see Understanding Ethernet Loopback, on page 147.
- Start the IP SLA session.

Note Using traffic generator, a maximum traffic of 1GB is generated.

Restrictions

- A single traffic session is generated.
- Traffic generation will not be supported on VLAN interface.
- One-way traffic generation and passive measurement features are not supported.
- Payload signature verification is not supported.

- The QoS functions like classification and policing are supported on the ingress EVC.
- Internal mode traffic generation cannot be configured on port channel interfaces.
- Maximum throughput rate is 1GB.
- SPAN and Traffic generator cannot be used simultaneously since both uses the mirror mechanism.
- For Traffic generation over cross connect port-channel will not be supported for both internal and external modes.
- Ethernet loopback and Traffic generator cannot be used simultaneously.
- After reload, the Traffic generator over cross connect should be rescheduled (stop and start).
- After cross connect flaps, the Traffic generator over cross connect should be rescheduled (stop and start).

Configuring IP SLA for Traffic Generation

Complete these steps to configure IP SLA for traffic generation.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip sla** *sla_id* **Example:** `Router(config)# ip sla 100p sla 100`	Specify the SLA ID to start the IP SLA session.
Step 3	**service-performance type ethernet dest-mac-addr** *destination mac-address* **interface** *type number* **service-instance** *number* **Example:** `Router(config-ip-sla)# service-performance type ethernet dest-mac-addr 0001.0001.0001 interface gigabitEthernet0/10 service-instance 10`	Specifies the service performance type as ethernet and the destination MAC address in H.H.H format. Specifies an interface type and number which traffic generator uses to send the packets. Also, specifies the service instance number that is required to create a service instance on an interface. The range is 1 to 4096.
Step 4	**aggregation | default | description | duration | exit | frequency | measurement-type direction | no | profile | signature** **Example:**	Specify the type of service performance. The following are the options: • **aggregation**—Represents the statistics aggregation. • **default**—Set a command to its defaults.

	Command or Action	Purpose
	`Router(config-ip-sla-service-performance)# profile traffic direction external`	• **description**—Description of the operation. • **duration**—Sets the service performance duration configuration. • **frequency**—Represents the scheduled frequency. The options available are iteration and time. The range is 20 to 65535 seconds. • **measurement-type** *direction*—Specifies the statistics to measure traffic. The options available are external or internal; the default option is Internal. If you use this option, go to Step 5. • **profile**—Specifies the service performance profile. If you use the packet or traffic option, go to Step 7 or Step 9 respectively. • **signature**—Specifies the payload contents.
Step 5	**default | exit | loss | no | throughput** **Example:** `Router(config-ip-sla-service-performance-measurement)# throughput`	Specifies the measurement type based on which the service performance is calculated. The following are the options: • **default**—Set a command to its defaults • **loss**—Specifies the measurement such as frame loss. • **throughput**—Specifies the measurement such as average rate of successful frame delivery.
Step 6	**exit**	Exits the measurement mode.
Step 7	**default | exit | inner-cos | inner-vlan | no | outer-cos | outer-vlan | packet-size | src-mac-addr** **Example:** `Router(config-ip-sla-service-performance-packet)# src-mac-addr 4055.3989.7b56`	Specifies the packet type. The following are the options: • **default**—Set a command to its defaults • **inner-cos**—Specify the class of service (CoS) value for the inner VLAN tag of the interface from which the message will be sent. • **inner-vlan**—Specify the VLAN ID for the inner vlan tag of the interface from which the message will be sent. • **outer-cos**—Specify the CoS value which will be filled in the outer VLAN tag of the packet. • **outer-vlan**—Specify the VLAN ID which will be filled in the outer VLAN tag of the packet.

	Command or Action	Purpose
		• **packet-size**—Specify the packet size; the default size is 64 bytes. The supported packet size are 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1280 bytes, and 1518 bytes. • **src-mac-addr**—Specifies the source MAC address in H.H.H format.
Step 8	**exit**	Exits the packet mode.
Step 9	**direction {external | internal}** **Example:** `Router(config-ip-sla-service-performance)# profile traffic direction external`	Specifies the direction of the profile traffic. The options are external and internal.
Step 10	Do one of the following: • **default** • **exit** • **no** • **rate-step** **Example:** `Router(config-ip-sla-service-performance-traffic)# rate-step kbps 1000`	Specifies the traffic type. The following are the options: • **default**—Set a command to its defaults • **rate-step**—Specifies the transmission rate in kbps. The rate-step range is from 1-1000000 (1 Kbps to 1Gbps).
Step 11	**exit**	Exits the traffic mode.

Configuration Examples

This section shows sample configuration examples for traffic generation on Cisco ASR 901 router:

```
ip sla 10
 service-performance type ethernet dest-mac-addr 0001.0001.0001 interface
TenGigabitEthernet0/0 service instance 30
  measurement-type direction external
   loss
   throughput
  profile packet
   outer-vlan 30
   packet-size 512
   src-mac-addr d48c.b544.93dd
  profile traffic direction external
   rate-step kbps 1000
  frequency time 35
```

Example: Two-Way Measurement

The following is a sample configuration for two-way measurement to measure throughput, loss, tx, rx, txbytes, and rxbytes.

```
INTERNAL: (to test UNI scenario)
ip sla 2
service-performance type ethernet dest-mac-addr aaaa.bbbb.cccc interface GigabitEthernet0/0
 service instance 2
measurement-type direction internal
loss
throughput
profile packet
outer-vlan 10
packet-size 512
src-mac-addr d48c.b544.9600
profile traffic direction internal
rate-step kbps 1000 2000 3000
frequency time 95
EXTERNAL: (to test NNI scenario)
ip sla 2
service-performance type ethernet dest-mac-addr aaaa.bbbb.cccc interface gigabitEthernet0/7
 service instance 2
measurement-type direction external
loss
throughput
profile packet
outer-vlan 10
packet-size 512
src-mac-addr d48c.b544.9600
profile traffic direction external
rate-step kbps 1000 2000 3000
frequency time 95
```

Example: Traffic Generation Mode

The following is a sample configuration for traffic generation mode to measure tx and txbytes.

```
INTERNAL: (to test UNI scenario)
ip sla 2
service-performance type ethernet dest-mac-addr aaaa.bbbb.cccc interface GigabitEthernet0/0
 service instance 2
measurement-type direction internal
profile packet
outer-vlan 10
packet-size 512
src-mac-addr d48c.b544.9600
profile traffic direction internal
rate-step kbps 1000 2000 3000
frequency time 95

EXTERNAL: (to test NNI scenario)
ip sla 2
service-performance type ethernet dest-mac-addr aaaa.bbbb.cccc interface GigabitEthernet0/7
 service instance 2
measurement-type direction external
profile packet
outer-vlan 10
packet-size 512
src-mac-addr d48c.b544.9600
profile traffic direction external
rate-step kbps 1000 2000 3000
frequency time 95
```

The following is an example of the output from the **show ip sla statistics** command.

```
show ip sla statistics 10
```

```
IPSLAs Latest Operation Statistics
IPSLA operation id: 10
Type of operation: Ethernet Service Performance
Test mode: Traffic Generator
Steps Tested (kbps): 1000
Test duration: 30 seconds
Latest measurement:  01:34:08.636 IST Wed Sep 25 2013
Latest return code:  OK
Step 1 (1000 kbps):
Stats:
Tx Packets: 1425  Tx Bytes: 729600
Step Duration: 6 seconds
```

Note Statistics are cumulative over a period of time and not specific to any particular time instance.

CHAPTER 10

ITU-T Y.1731 Performance Monitoring

This chapter provides information on the ITU-T Y.1731 Performance Monitoring for the Cisco ASR 901 Series Aggregation Services Router.

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 ITU-T Y.1731 Performance Monitoring, on page 184.

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 ITU-T Y.1731 Performance Monitoring

- Configure and enable IEEE-compliant connectivity fault management (CFM) for Y.1731 performance monitoring to function.

Restrictions for ITU-T Y.1731 Performance Monitoring

- One-way delay measurement (1DM) is not supported.

- Loss Measurement Message (LMM) is not supported.
- Delay Measurement Message (DMM) is supported only from Cisco IOS Release 15.5(2)S.
- Synthetic Loss Measurement (SLM) is not supported on the port level cross connect.
- You can configure only a maximum of 100 DMM responders.
- Multi-NNI Connectivity Fault Management (CFM) and SLM are not supported over the cross-connect Ethernet flow point (EFP) simultaneously. However, you can enable Multi-NNI CFM or SLM over the cross-connect EFP function in a node.
- Two-way Ethernet frame Delay Measurement (ETH-DM) on Port maintenance endpoint (MEP) is not supported.
- For Two-way ETH-DM on DOWN MEP CFM, one index is reserved to be used by bridge-domain. If this index has to be used as a bridge-domain on any port, the DMM session should be un-configured.
- More than one DMM session on a single EFP with same direction (UP or DOWN), with different level, is not supported.
- DOWN MEP DMM with untagged encapsulation (encapsulation default without any cfm encapsulation configuration) over Xconnect is not supported. Also, Xconnect DMM with **encapsulation dot1ad** command and without **rewrite ingress tag** command is not supported.

  The following encapsulations for xconnect DMM are not supported:

  - dot1ad without rewrite
  - untagged for DOWN MEP
  - default without CFM encapsulation command for DOWN MEP
- The following delays are observed for 2DM:
  - Queuing delay from where DMM is originated and terminated.
  - Queuing delay of DMR packet at the node where DMM is looped back.
  - Queuing delay when DMR packet is received at the node where DMM was originated.
- Do not use **clock** command for DMM or SLM, as it results in junk values in delay, as time stamping is done at the BCM level.
- When you configure DMM and SLM with different frame sizes, the latency may vary.
- Offloading is not supported for xconnect.
- There is no special group for DMM over Xconnect feature in TCAM; FP entries are seen in TCAM, under storm-control slice.

Information About ITU-T Y.1731 Performance Monitoring

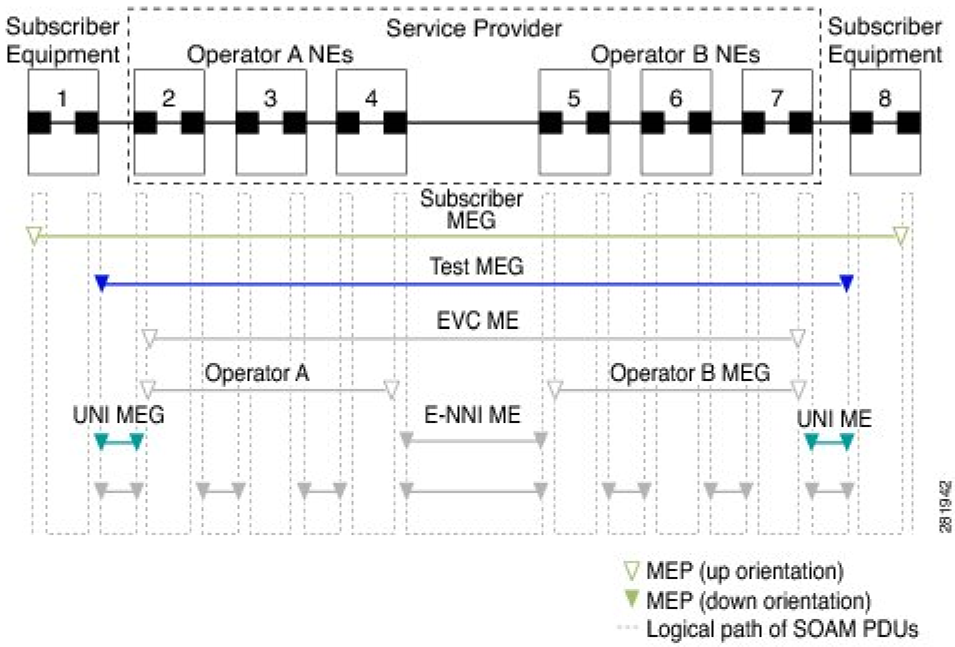
When service providers sell connectivity services to a subscriber, a Service Level Agreement (SLA) is reached between the buyer and seller of the service. The SLA defines the attributes offered by a provider and serves as a legal obligation on the service provider. As the level of performance required by subscribers rises, service providers need to monitor the performance parameters being offered. Various standards, such as IEEE 802.1ag and ITU-T Y.1731, define the methods and frame formats used to measure performance parameters.

ITU-T Y.1731 performance monitoring provides standards-based Ethernet performance monitoring as outlined in the ITU-T Y-1731 specification and interpreted by the Metro Ethernet Forum (MEF). It includes the measurement of Ethernet frame delay, frame delay variation, frame loss, and throughput.

To measure SLA parameters such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the end point of the maintenance region, where the Maintenance End Point (MEP) responds to the synthetic frame.

The following figure illustrates Maintenance Entities (ME) and MEP typically involved in a point-to-point metro ethernet deployment for the Y.1731 standard.

Figure 6: A Point-to-Point Metro Ethernet Deployment with Typical Maintenance Entities and Maintenance Points



Frame Delay and Frame-Delay Variation

Ethernet frame Delay Measurement (ETH-DM) is used for on-demand Ethernet Operations, Administration & Maintenance (OAM) to measure frame delay and frame-delay variation.

Ethernet frame delay and frame delay variation are measured by sending periodic frames with ETH-DM information to the peer MEP in the same maintenance entity. Peer MEPs perform frame-delay and frame-delay variation measurements through this periodic exchange during the diagnostic interval.

Ethernet frame delay measurement supports hardware-based timestamping in the ingress direction.

These are the two methods of delay measurement, as defined by the ITU-T Y.1731 standard, One-way ETH-DM (1DM) and Two-way ETH-DM (2DM). However, the Cisco ASR 901 router supports only Two-way ETH-DM.

Two-way Delay Measurement

Two-way frame delay and variation can be measured using DMM and Delay Measurement Reply (DMR) frames.

Note Starting with Cisco IOS Release 15.4(2)S, the DMM sessions are enhanced from 32 to 100.

In two-way delay measurements, the sender MEP transmits a frame containing ETH-DM request information and TxTimeStampf, where TxTimeStampf is the timestamp of the time at which the DMM is sent.

When the receiver MEP receives the frame, it records RxTimeStampf, where RxTimeStampf is the timestamp of the time at which the frame with ETH-DM request information is received.

The receiver MEP responds with a frame containing ETH-DM reply information and TxTimeStampb, where TxTimeStampb is the timestamp of the time at which the frame with ETH-DM reply information is sent.

When the sender MEP receives this frame, it records RxTimeStampb, where RxTimeStampb is the timestamp of the time at which the frame containing ETH-DM reply information is received.

Two-way frame delay is calculated as:

Frame delay = (RxTimeStampb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

Note Discard the frame delay and frame-delay variation measurements when known network topology changes occur or when continuity and availability faults occur.

For more information on ITU-T Y.1731 performance monitoring, see Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations in the *IP SLAs Configuration Guide* .

Frame Loss Ratio

Ethernet Frame Loss Ratio (ETH-LM: FLR), also known as frame loss, measures the availability of synthetic frames in the network. Availability is defined in terms of the ratio of frames lost to frames sent, or Frame Loss Ratio (FLR).

Ethernet Synthetic Loss Measurement (ETH-SLM) is used to collect counter values applicable for ingress and egress synthetic frames where the counters maintain a count of transmitted and received synthetic frames between a pair of MEPs.

ETH-SLM transmits synthetic frames with ETH-SLM information to a peer MEP and similarly receives synthetic frames with ETH-SLM information from the peer MEP. Each MEP performs frame loss measurements, which contribute to unavailable time. A near-end frame loss refers to frame loss associated with ingress data frames. A far-end frame loss refers to frame loss associated with egress data frames. Both near-end and far-end frame loss measurements contribute to near-end severely errored seconds and far-end severely errored seconds, which together contribute to unavailable time. ETH-SLM is measured using SLM and SLR frames.

There are the two methods of frame loss measurement, defined by the ITU-T Y.1731 standard ETH-LM and ETH-SLM. However, the Cisco ASR 901 router supports only single-ended ETH-SLM.

Single-ended ETH-SLM

Each MEP transmits frames with the ETH-SLM request information to its peer MEP and receives frames with ETH-SLR reply information from its peer MEP to carry out synthetic loss measurements.

On-Demand and Concurrent Operations

On-demand IP SLAs SLM operations enable users without configuration access to perform real-time troubleshooting of Ethernet services. There are two operational modes for on-demand operations: direct mode that creates and runs an operation immediately and referenced mode that starts and runs a previously configured operation.

- In the direct mode, a single command can be used to create multiple pseudo operations for a range of class of service (CoS) values to be run, in the background, immediately. A single command in privileged EXEC mode can be used to specify frame size, interval, frequency, and duration for the direct on-demand operation. Direct on-demand operations start and run immediately after the command is issued.
- In the referenced mode, you can start one or more already-configured operations for different destinations, or for the same destination, with different CoS values. Issuing the privileged EXEC command creates a pseudo version of a proactive operation that starts and runs in the background, even while the proactive operation is running.
- After an on-demand operation is completed, statistical output is displayed on the console. On-demand operation statistics are not stored and are not supported by the statistic history and aggregation functions.
- After an on-demand operation is completed, and the statistics handled, the direct and referenced on-demand operation is deleted. The proactive operations are not deleted and continue to be available to be run in referenced mode, again.

A concurrent operation consists of a group of operations, all configured with the same operation ID number, that run concurrently. Concurrent operations are supported for a given EVC, CoS, and remote MEP combination, or for multiple MEPs for a given multipoint EVC, for delay or loss measurements.

The Cisco ASR 901 router also supports burst mode for concurrent operations, one-way dual-ended, single-ended delay and delay variation operations, and single-ended loss operations.

Supported Interfaces

The Cisco ASR 901 router supports ITU-T Y.1731 performance monitoring on the following interfaces:

- DMM and SLM support on the EVC bridge domain (BD)
- DMM and SLM support on the Port-Channel EVC BD
- DMM and SLM support on the EVC cross connect
- DMM and SLM support on the Port-Channel EVC cross connect
- DMM and SLM support on the EVC BD for both the up and down MEPs
- SLM support on the EVC cross connect for both the up and down MEPs

Note SLM and DMM can be configured for the same EVCs over CFM session. The combined number of CFM, DMM, and SLM sessions must be within the scale limits, otherwise DMM/SLM probes might get dropped resulting in a few incomplete measurements.

Benefits of ITU-T Y.1731 Performance Monitoring

Combined with IEEE-compliant CFM, Y.1731 performance monitoring provides a comprehensive fault management and performance monitoring solution for service providers. This comprehensive solution in turn lessens service providers' operating expenses, improves their SLAs, and simplifies their operations.

How to Configure ITU-T Y.1731 Performance Monitoring

Configuring Two-Way Delay Measurement

Note To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

Complete the following steps to configure two-way delay measurement.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 10`	Configures an IP SLA operation and enters IP SLA configuration mode. • *operation-number*—Identifies the IP SLAs operation you want to configure.

Step 4	**ethernet y1731 delay DMM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}}
	Example:
	`Router(config-ip-sla)# ethernet y1731 delay`
	`DMM domain xxx evc yyy mpid 101 cos 4 source mpid 100`
		Configures two-way delay measurement and enters IP SLA Y.1731 delay configuration mode.
		• **DMM**—Specifies that the frames sent are Delay Measurement Message (DMM) synthetic frames.
		• domain *domain-name*—Specifies the name of the Ethernet maintenance Operations, Administration & Maintenance (OAM) domain.
		• **evc** *evc-id*—Specifies the EVC identification name.
		• **vlan** *vlan-id*—Specifies the VLAN identification number. The range is from 1 to 4096.

	Command or Action	Purpose
		• **mpid** *target-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191. • **mac-address** *target-address*—Specifies the MAC address of the MEP at the destination. • **cos** *cos*—Specifies, for this MEP, the class of service (CoS) that will be sent in the Ethernet message. The range is from 0 to 7. • **source**—Specifies the source MP ID or MAC address. • **mpid** *source-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191. • **mac-address** *source-address*—Specifies the MAC address of the MEP being configured.
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored. • *seconds*—Specifies the length of time in seconds. The range is from 1 to 65535. The default is 900.
Step 6	**distribution** {**delay** | **delay-variation**} {**one-way** | **two-way**} *number-of-bins boundary*[,...,*boundary*] **Example:** `Router(config-sla-y1731-delay)# distribution delay-variation two-way 5 5000, 10000,15000,20000,-1`	(Optional) Specifies measurement type and configures bins for statistics distributions kept. • **delay**—Specifies that the performance measurement type is delay. This is the default value, along with delay variation. • **delay-variation**—Specifies that the performance measurement type is delay variation. This is the default value, along with delay. • **one-way**—Specifies one-way measurement values. This is the default for a dual-ended operation. • **two-way**—Specifies two-way measurement values. This is the default for a single-ended operation. • *number-of-bins*—Specifies the number of bins kept during an aggregate interval. The range is from 1 to 10. The default is 10.

	Command or Action	Purpose
		• *boundary* [,...,*boundary*]—Lists upper boundaries for bins in microseconds. Minimum number of boundaries required is one. Maximum allowed value for the uppermost boundary is -1 microsecond. Multiple values must be separated by a comma (,). The default value is 5000,10000,15000,20000,25000,30000,35000,40000,45000, -1.
Step 7	**frame interval** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# frame interval 100`	(Optional) Sets the gap between successive frames. • *milliseconds*—Specifies the length of time in milliseconds (ms) between successive synthetic frames. The range is from 100 to 10000. The default is 1000.
Step 8	**frame offset** *offset-value* **Example:** `Router(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets a value for calculating delay variation values. • *offset-value*—The range is from 1 to 10. The default is 1.
Step 9	**frame size** *bytes* **Example:** `Router(config-sla-y1731-delay)# frame size 32`	(Optional) Configures padding size for frames. • *bytes*—Specifies the padding size, in four-octet increments, for the synthetic frames. The range is from 64 to 384. The default is 64.
Step 10	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation. • *intervals-stored*—Specifies the number of statistics distributions. The range is from 1 to 10. The default is 2.
Step 11	**max-delay** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# max-delay 5000`	(Optional) Sets the amount of time an MEP waits for a frame. • *milliseconds*—Specifies the maximum delay in milliseconds (ms). The range is from 1 to 65535. The default is 5000.
Step 12	**owner** *owner-id* **Example:** `Router(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation. • *owner-id*—Specifies the name of the SNMP owner. The value is from 0 to 255 ASCII characters.

	Command or Action	Purpose
Step 13	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits IP SLA Y.1731 delay configuration mode and enters privileged EXEC mode.

What to Do Next

After configuring two-way delay measurement, see the Scheduling IP SLAs Operations, on page 176 to schedule the operation.

Configuring Two-Way Delay Measurement on Xconnect (EoMPLS)

Complete the following steps to configure two-way delay measurement on xconnect.

Before you begin

CFM configuration on the interface is mandatory to achieve DMM without CCM exchange.

Port-channel with static mac-address is supported at both the responder and source end.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 11`	Configures an IP SLA operation and enters IP SLA configuration mode. • *operation-number*—Identifies the IP SLAs operation you want to configure.

Step 4	**ethernet y1731 delay DMM domain** *domain-name* {**evc** *evc-id***mac-address** *target-address* **cos** *cos* **source mac-address** *source-address*}}
	Example:
	`Router(config-ip-sla)# ethernet y1731 delay`
	`DMM domain cisco evc evc10 mac-address`
		Configures two-way delay measurement and enters IP SLA Y.1731 delay configuration mode.

	Command or Action	Purpose
	`7cad.74dc.e3d6 cos 0 source mac-address 18e7.280b.5883`	
Step 5	**max-delay***delay-period* **Example:** `Router(config-sla-y1731-delay)# max-delay 500`	Configures the maximum length of time a Maintenance Endpoint (MEP) in an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation waits for a synthetic frame.
Step 6	**frame interval** *interval* **Example:** `Router(config-sla-y1731-delay)# frame interval 100`	Configures the rate at which an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation sends synthetic frames.
Step 7	**distribution delay-variation two-way** *number-of-bins boundary [,...,boundary]* **Example:** `Router(config-sla-y1731-delay)# distribution delay-variation two-way 5 5000,10000,15000,20000,-1`	Configures the statistics distributions for an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation.
Step 8	**ip slaschedule** *operation-number* **life forever start-time now** **Example:** `Router(config-sla-y1731-delay)# ip sla schedule 11 life forever start-time now`	Configures the scheduling parameters for an individual IP SLA's operation.
Step 9	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits IP SLA Y.1731 delay configuration mode and enters privileged EXEC mode.

Example: Verifying Y.1731 Two Way ETH-DM on Xconnect (EoMPLS)

To verify whether the local mep is up, use the **show ethernet cfm maintenance-points local** command as given in the following example:

```
Router# show ethernet cfm maintenance-points local

!The output should show the source mac-address (for example, the mac-address used in the
configuration example, which is: 18e7.280b.5883)
```

To verify whether the remote mep is learnt or not, use the **show ethernet cfm maintenance-points remote** command as given in the following example:

```
Router# show ethernet cfm maintenance-points remote

!The output should show the destination mac-address (for example, the mac-address used in
the configuration example, which is: 7cad.74dc.e3d6)
```

To verify whether the dmm is working properly, use the **show ip sla summary** command as given in the following example:

```
Router# show ip sla summary | in 11

*11          y1731-delay Domain:cisco Evc:ev -           OK          56 seconds ag
```

To verify whether the destination is sending replies or not, use the **show ip sla statistics** command as given in the following example:

```
Router# show ip sla statistics 11 details | in Number of measurements

Number of measurements Initiated: 527
Number of measurements completed: 527
```

To verify whether the xconnect is up, use the **show mpls l2transport** command as given in the following example:

```
Router# show mpls l2transport vc 100

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi0/11         Eth VLAN 100               2.2.2.2         100        UP
```

Example: Configuring Y.1731 Two Way ETH-DM on Xconnect (EoMPLS)

The topology used in the following configuration example is as follows:

Router1:(gigabitethernet 0/2)----------------------(gigabitethernet 0/8)-xconnect

Router2: gigabitethernet(0/10)------------------(gigabitethernet 0/10)

Router3: (gigabitethernet 0/11)(xconnect) down mep --------------------------(gigabitethernet 0/11)

Router4 (down mep)

```
Router1
! configuration to be applied on this router is given below

configure  terminal
interface vlan100
ip address 192.1.1.1 255.255.255.0
no shut
exit

ethernet evc evc10
interface gigabitethernet 0/2
service instance 1 ethernet
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
bridge-domain 100
```

```
Router 2
! configuration to be applied on this router is given below

configure terminal
interface loopback 0
ip address 2.2.2.2 255.255.255.255

mpls ip

interface vlan 40
ip address 10.8.8.2 255.255.255.0
mpls ip
exit


interface gigabitethernet 0/10
service instance 1 ethernet
encapsularion dot1q 40
rewrite ingress tag pop1 symmetric
bridge-domain 40


interface gigabitethernet 0/8
service instance 1 ethernet
encapsulation dot1q 100
xconnect 3.3.3.3 100 encapsulation mpls
mtu 1500
exit

router ospf 1
router-id 2.2.2.2
network 10.8.8.0 0.0.0.2555 area 0
network 2.2.2.2 0.0.0.0 area 0


Router 3
! configuration to be applied on this router is given below

configure terminal
ethernet cfm ieee
ethernet cfm global
ethernet cfm domain cisco level 6
service test evc evc10 direction down
continuity-check
continuity-check interval 1s

interface loopback 0
ip address 3.3.3.3 255.255.255.255

mpls ip

interface vlan 40
ip address 10.8.8.3 255.255.255.0
mpls ip
exit


interface gigabitethernet 0/10
service instance 1 ethernet
encap dot1q 40
rewrite ingress tag pop1 symmetric
bridge-domain 40
```

```
interface gigabitethernet 0/11
service instance 1 ethernet
encapsulation dot1q 100
xconnect 2.2.2.2 100 encapsulation mpls
mtu 1500
cfm mep domain cisco mpid 101
dmm responder hardware timestamp

exit

router ospf 1
router-id 3.3.3.3
network 10.8.8.0 0.0.0.2555 area 0
network 3.3.3.3 0.0.0.0 area 0


Router 4
! configuration to be applied on this router is given below

configure  terminal

ethernet cfm ieee
ethernet cfm global
ethernet cfm domain cisco level 6
service test evc evc10 vlan 100 direction down
continuity-check
continuity-check interval 1s

interface vlan100
ip address 192.1.1.2 255.255.255.0
no shut
exit

ethernet evc evc10
interface gig 0/2
service instance 1 ethernet
encap dot1q 100
rewrite ingress tag pop 1 symmetric
bridge-domain 100
cfm mep domain cisco mpid 100
```

Configuring Single-Ended Synthetic Loss Measurement

Note To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

Complete the following steps to configure a single-ended SLM.

Before you begin

Class of Service (CoS)-level monitoring must be enabled on MEPs associated to the Ethernet frame loss operation using the **monitor loss counter** command on the devices at both ends of the operation.

Note Cisco IOS Y.1731 implementation allows monitoring of frame loss for frames on an EVC regardless of the CoS value (any CoS or Aggregate CoS cases). See the "Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations" section for configuration information.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config)# ip sla 11`	Configures an IP SLA operation and enters IP SLA configuration mode. • *operation-number*—Identifies the IP SLAs operation you want to configure.

Step 4	**ethernet y1731 loss SLM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}}
	Example:
	`Router(config-ip-sla)# ethernet y1731 loss`
	`SLM domain xxx evc yyy mpid 101 cos 4 source mpid 100`
		Configures a single-ended synthetic loss measurement and enters IP SLA Y.1731 loss configuration mode.
		• **SLM**—Specifies that the frames sent are Synthetic Loss Measurement (SLM) frames.
		• domain *domain-name*—Specifies the name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
		• **evc** *evc-id*—Specifies the EVC identification name.
		• **vlan** *vlan-id*—Specifies the VLAN identification number. The range is from 1 to 4096.
		• **mpid** *target-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191.
		• **mac-address** *target-address*—Specifies the MAC address of the MEP at the destination.

	Command or Action	Purpose
		• **cos** *cos*—Specifies, for this MEP, the class of service (CoS) that will be sent in the Ethernet message. The range is from 0 to 7. • **source**—Specifies the source MP ID or MAC address. • **mpid** *source-mp-id*—Specifies the maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191. • **mac-address** *source-address*—Specifies the MAC address of the MEP being configured.
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-loss)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored. • *seconds*—Specifies the length of time in seconds. The range is from 1 to 65535. The default is 900.
Step 6	**availability algorithm** {**sliding-window** | **static-window**} **Example:** `Router(config-sla-y1731-loss)# availability algorithm static-window`	(Optional) Specifies availability algorithm used. • **sliding-window**—Specifies a sliding-window control algorithm. • **static-window**—Specifies static-window control algorithm.
Step 7	**frame consecutive** *value* **Example:** `Router(config-sla-y1731-loss)# frame consecutive 10`	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status. • *value*—Specifies the number of consecutive measurements. The range is from 1 to 10. The default is 10.
Step 8	**frame interval** *milliseconds* **Example:** `Router(config-sla-y1731-loss)# frame interval 100`	(Optional) Sets the gap between successive frames. • *milliseconds*—Specifies the length of time in milliseconds (ms) between successive synthetic frames. The range is from 100 to 10000. The default is 1000.
Step 9	**frame size** *bytes* **Example:** `Router(config-sla-y1731-loss)# frame size 32`	(Optional) Configures padding size for frames. • *bytes*—Specifies the padding size, in four-octet increments, for the synthetic frames. The range is from 64 to 384. The default is 64.

	Command or Action	Purpose
Step 10	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-loss)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation. • *intervals-stored*—Specifies the number of statistics distributions. The range is from 1 to 10. The default is 2.
Step 11	**owner** *owner-id* **Example:** `Router(config-sla-y1731-loss)# owner admin`	(Optional) Configures the owner of an IP SLAs operation. • *owner-id*—Specified the name of the SNMP owner. The value is from 0 to 255 ASCII characters.
Step 12	**exit** **Example:** `Router(config-sla-y1731-loss)# exit`	Exits IP SLA Y.1731 loss configuration mode and enters IP SLA configuration mode.
Step 13	**exit** **Example:** `Router(config-ip-sla)# exit`	Exits IP SLA configuration mode and enters global configuration mode.
Step 14	**ip sla reaction-configuration** *operation-number* [**react** {**unavailableDS** | **unavailableSD** | **loss-ratioDS** | **loss-ratioSD**}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** }] [**threshold-value** *upper-threshold lower-threshold*] **Example:** `Router(config)# ip sla reaction-configuration 11 react unavailableDS`	(Optional) Configures proactive threshold monitoring for frame loss measurements. • *operation-number*—Identifies the IP SLAs operation for which reactions are to be configured. • **react**—(Optional) Specifies the element to be monitored for threshold violations. • **unavailableDS**—Specifies that a reaction should occur if the percentage of destination-to-source Frame Loss Ratio (FLR) violates the upper threshold or lower threshold. • **unavailableSD**—Specifies that a reaction should occur if the percentage of source-to-destination FLR violates the upper threshold or lower threshold. • **loss-ratioDS**—Specifies that a reaction should occur if the one-way destination-to-source loss-ratio violates the upper threshold or lower threshold. • **loss-ratioSD**—Specifies that a reaction should occur if the one way source-to-destination loss-ratio violates the upper threshold or lower threshold.

	Command or Action	Purpose
		• **threshold-type average** [*number-of-measurements*]—(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the **action-type** keyword. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The range is from 1 to 16. • **threshold-type consecutive** [*occurrences*]—(Optional) When a threshold violation for the monitored element is met consecutively for a specified number of times, perform the action defined by the **action-type** keyword. The default number of 5 consecutive occurrences can be changed using the *occurrences* argument. The range is from 1 to 16. • **threshold-type immediate**—(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the **action-type** keyword. • **threshold-value** *upper-threshold lower-threshold*—(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements.
Step 15	**ip sla logging traps** **Example:** `Router(config)# ip sla logging traps`	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 16	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

What to Do Next

After configuring this MEP, see the Scheduling IP SLAs Operations, on page 176 to schedule the operation.

Scheduling IP SLAs Operations

Complete the following steps to schedule an IP SLAs operation.

Before you begin

- All IP SLAs operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multi-operation group must be the same.
- List of one or more operation ID numbers to be added to a multi-operation group is limited to a maximum of 125 characters, including commas (,).

Procedure

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

Step 3	Do one of the following:
	• **ip sla schedule** *opertion-number* **start-time now**
	• **ip sla schedule** *opertion-number*
	Example:
	`Router(config)# ip sla schedule 10 start-time now`
	Example:
	`Router(config)# ip sla group schedule 1 3,4,6-9`
		Configures the scheduling parameters for an individual IP SLAs operation or Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled for a multi-operation scheduler.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits the global configuration mode and enters the privileged EXEC mode.

Verifying the Frame Delay and Synthetic Loss Measurement Configurations

Example: Verifying Sender MEP for a Two-Way Delay Measurement Operation

The following sample output shows the configuration, including default values, of the sender MEP for a two-way delay measurement operation:

```
Router# show ip sla configuration 10

IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: xxx
Vlan: yyy
Target Mpid: 101
Source Mpid: 100
CoS: 4
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

Example: Verifying Receiver MEP for a Two-Way Delay Measurement Operation

The following sample output shows the configuration of the receiver MEP for a two-way delay measurement operation:

Note The Cisco ASR 901 router supports hardware-based timestamping. Enable the hardware-based timestamping using the **dmm responder hardware timestamp** command on the receiver MEP.

```
Router-1# show running interface gigabitethernet0/0
```

```
interface GigabitEthernet0/0
 no ip address
 negotiation auto
 service instance 1310 ethernet ssvc1310
  encapsulation dot1q 1310
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1310
  cfm mep domain sdmm mpid 1310
   dmm responder hardware timestamp
```

Example: Verifying Sender MEP for a Synthetic Loss Measurement Operation

The following sample output shows the configuration, including default values, of the sender MEP for a single-ended SLM operation with a start-time of now:

```
Router# show ip sla configuration 11

IP SLAs Infrastructure Engine-III
Entry number: 11
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Loss Operation
Frame Type: SLM
Domain: xxx
Vlan: 12
Target Mpid: 34
Source Mpid: 23
CoS: 4
   Request size (Padding portion): 0
   Frame Interval: 1000
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): ActiveThreshold (milliseconds): 5000
Statistics Parameters
  Aggregation Period: 900
  Frame consecutive: 10
  Availability algorithm: static-window
History
  Number of intervals: 2
```

Example: Verifying Ethernet CFM Performance Monitoring

To view the Ethernet CFM performance monitoring activities, use the **show ethernet cfm pm** command.

```
Router# show ethernet cfm pm session summary
Number of Configured Session : 4
Number of Active Session: 4
Number of Inactive Session: 0
Router# show ethernet cfm pm session detail 1
Session ID: 1
Sla Session ID: 2002
Level: 5
```

```
Service Type: BD-V
Service Id: 1000
Direction: Down
Source Mac: 4055.3989.736d
Destination Mac: 4055.3989.6c01
Session Version: 0
Session Operation: On-demand
Session Status: Active
MPID: 1000
Tx active: yes
Rx active: yes
RP monitor Tx active: yes
RP monitor Rx active: yes
Timeout timer: stopped
Last clearing of counters: *13:39:29.070 IST Mon Mar 18 2013
DMMs:
   Transmitted: 0
DMRs:
   Rcvd: 0
1DMs:
   Transmitted: 0
   Rcvd: 0
LMMs:
   Transmitted: 0
LMRs:
   Rcvd: 0
VSMs:
   Transmitted: 0
VSRs:
   Rcvd: 0
SLMs:
   Transmitted: 517100
SLRs:
   Rcvd: 517098
```

Example: Verifying History for IP SLAs Operations

To view the history collected for IP SLAs operations, use the **show ip sla history** command.

Note The **show ip sla history full** command is not supported for the ITU-T Y.1731 operations.

```
Router# show ip sla history interval-statistics
Loss Statistics for Y1731 Operation 2001
Type of operation: Y1731 Loss Measurement
Latest operation start time: *13:48:39.055 IST Tue Mar 19 2013
Latest operation return code: OK
Distribution Statistics:
Interval 1
 Start time:  *13:48:39.055 IST Tue Mar 19 2013
 End time:  *13:48:59.055 IST Tue Mar 19 2013
 Number of measurements initiated: 198
 Number of measurements completed: 198
 Flag: OK
Forward
  Number of Observations 19
  Available indicators: 19
  Unavailable indicators: 0
  Tx frame count: 190
```

```
  Rx frame count: 190
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
  Timestamps forward:
    Min - *13:48:58.084 IST Tue Mar 19 2013
    Max - *13:48:58.084 IST Tue Mar 19 2013
Backward
  Number of Observations 19
  Available indicators: 19
  Unavailable indicators: 0
  Tx frame count: 190
  Rx frame count: 190
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
  Timestamps backward:
    Min - *13:48:58.084 IST Tue Mar 19 2013
    Max - *13:48:58.084 IST Tue Mar 19 2013
```

How to Configure IP SLAs Y.1731 On-Demand and Concurrent Operations

Configuring Direct On-Demand Operation on a Sender MEP

Class of Service (CoS)-level monitoring must be enabled on MEPs associated to the Ethernet frame loss operation using the **monitor loss counter** command on the devices at both ends of the operation.

Note Cisco IOS Y.1731 implementation allows monitoring of frame loss for frames on an EVC regardless of the CoS value (any CoS or Aggregate CoS cases).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ip sla on-demand ethernet slm domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos*{**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} {**continuous** [**interval** *milliseconds*] | **burst** [**interval** *milliseconds*] [**number** *number-of-frames*] [**frequency** *seconds*]}[**size** *bytes*] **aggregation** *seconds* {**duration** *seconds* |**max** *number-of-packets*}	Creates and runs an on-demand operation in direct mode. Repeat this step for each on-demand operation to be run.

	Command or Action	Purpose

	Example:
	
	`Router# ip sla on-demand ethernet SLM domain xxx`
	`vlan 12 mpid 34 cos 4 source mpid 23 continuous`
	`aggregation 10 duration 60`	

Configuring Referenced On-Demand Operation on a Sender MEP

Before you begin

Single-ended and concurrent Ethernet delay, or delay variation, and frame loss operations to be referenced must be configured.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ip sla on-demand ethernet slm** *operation number* {**duration** *seconds* | **max** *number-of-packets*} **Example:** `Router# ip sla on-demand ethernet slm 11`	Creates and runs a pseudo operation of the operation being referenced, in the background. Repeat this step for each on-demand operation to be run.

Configuring IP SLAs Y.1731 Concurrent Operation on a Sender MEP

To configure concurrent Ethernet delay, and delay variation, and frame loss operations, see the How to Configure ITU-T Y.1731 Performance Monitoring, on page 164.

Configuration Examples for IP SLAs Y.1731 On-Demand Operations

Example: On-Demand Operation in Direct Mode

```
Router# ip sla on-demand ethernet slm domain md5 evc evc1000 mpid 1000 cos 1 source mpid
1001 continuous aggregation 30 duration 31
```

```
Loss Statistics for Y1731 Operation 3313031511
Type of operation: Y1731 Loss Measurement
Latest operation start time: *13:21:23.995 IST Tue Mar 19 2013
Latest operation return code: OK
Distribution Statistics:
Interval
 Start time:  *13:21:23.995 IST Tue Mar 19 2013
 End time:  *13:21:53.988 IST Tue Mar 19 2013
 Number of measurements initiated: 30
 Number of measurements completed: 30
 Flag: OK
Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
  Timestamps forward:
    Min - *13:21:53.030 IST Tue Mar 19 2013
    Max - *13:21:53.030 IST Tue Mar 19 2013
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
  Timestamps backward:
    Min - *13:21:53.030 IST Tue Mar 19 2013
    Max - *13:21:53.030 IST Tue Mar 19 2013
```

Example: On-Demand Operation in Referenced Mode

```
Router# configure terminal
Router(config)# ip sla 2002
Router(config-ip-sla)# ethernet y1731 loss SLM domain md5 evc evc1000 mpid 1001 cos 3 source
 mpid 1000
Router(config-sla-y1731-loss)# aggregate interval 30
Router(config-sla-y1731-loss)# end
Router# ip sla on-demand ethernet slm 2002 duration 31
Loss Statistics for Y1731 Operation 3313031511
Type of operation: Y1731 Loss Measurement
Latest operation start time: *13:21:23.995 IST Tue Mar 19 2013
Latest operation return code: OK
Distribution Statistics:
Interval
 Start time:  *13:21:23.995 IST Tue Mar 19 2013
 End time:  *13:21:53.988 IST Tue Mar 19 2013
 Number of measurements initiated: 30
 Number of measurements completed: 30
 Flag: OK
Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
```

```
  Timestamps forward:
    Min - *13:21:53.030 IST Tue Mar 19 2013
    Max - *13:21:53.030 IST Tue Mar 19 2013
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.0000%
  Timestamps backward:
    Min - *13:21:53.030 IST Tue Mar 19 2013
    Max - *13:21:53.030 IST Tue Mar 19 2013
```

Additional References

The following sections provide references to ITU-T Y.1731 Performance Monitoring.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference
IEEE CFM	Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network
Using OAM	Using Ethernet Operations, Administration, and Maintenance
IEEE CFM and Y.1731 commands	Cisco IOS Carrier Ethernet Command Reference

Standards

Standard	Title
IEEE 802.1ag	802.1ag - Connectivity Fault Management
ITU-T Y.1731	ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks
MEF 17	Service OAM Requirements & Framework - Phase 1

MIBs

MIB	MIBs Link
CISCO-IPSLA-ETHERNET-MIB CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for ITU-T Y.1731 Performance Monitoring

Table 15: Feature Information for ITU-T Y.1731 Performance Monitoring, on page 184 lists the features in this module and provides links to specific configuration information.

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 Table 15: Feature Information for ITU-T Y.1731 Performance Monitoring, on page 184 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 15: Feature Information for ITU-T Y.1731 Performance Monitoring

Feature Name	Releases	Feature Information
Y.1731 Performance Monitoring	15.3(2)S	This feature was introduced on the Cisco ASR 901 router. The following sections provide information about this feature:
Ethernet Synthetic Loss Measurement in Y.1731	15.3(2)S	This feature was introduced on the Cisco ASR 901 router. The following sections provide information about this feature:

Feature Name	Releases	Feature Information
Y.1731 Performance Monitoring	15.3(3)S	The Cisco ASR 901 router supports ITU-T Y.1731 performance monitoring on the following interfaces: –SLM support on the EVC cross connect –SLM support on the Port-Channel EVC cross connect –DMM and SLM support on the EVC BD for both the up and down MEPs –SLM support on the EVC cross connect for both the up and down MEPs
Y1731 Two Way ETH-DM on Xconnect (EoMPLS)	15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 11

Configuring Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, to respond to link failures, and to improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing. Effective with Cisco IOS Release 15.4(1)S, the Cisco ASR 901 supports REP over port-channel.

Understanding Resilient Ethernet Protocol

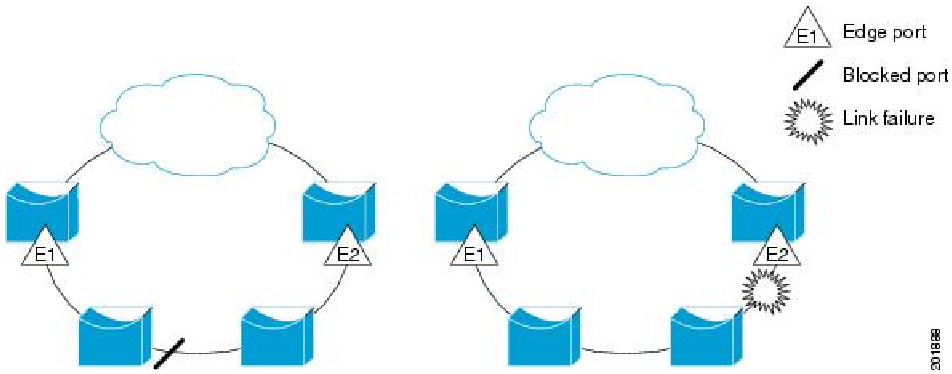
This section contains the following topics:

Overview

An REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have only two ports belonging to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces.

The following figure shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a network failure, as shown on the right of the diagram, the blocked port returns to the forwarding state to minimize network disruption.

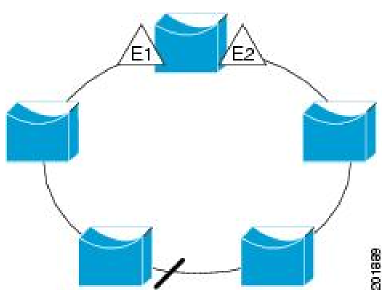
Figure 7: REP Open Segments



The segment shown in the above figure is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a host cannot access its usual gateway because of a failure, REP unblocks all ports to ensure that connectivity is available through the other gateway.

The segment shown in the following figure, with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

Figure 8: REP Ring Segment



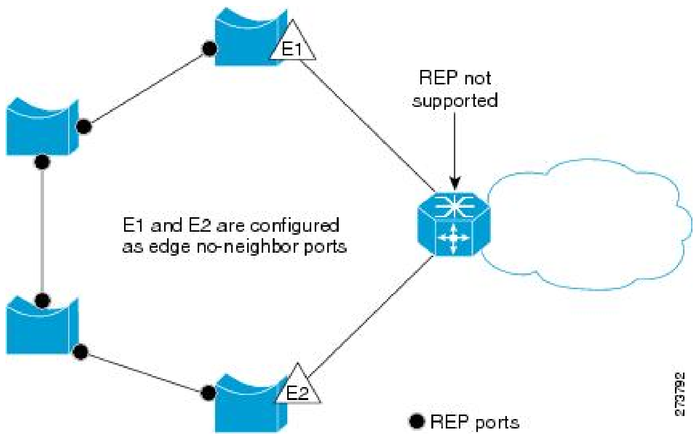
REP segments have these characteristics:

- If all ports in the segment are operational, one port (referred to as the *alternate* port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

In access ring topologies, the neighboring switch might not support REP, as shown in the following figure. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

Figure 9: No-neighbor Topology



Restrictions

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.
- BFD and REP together are not recommended on Cisco ASR 901 Router while sharing the same link.
- Layer 3 over REP with VLAN load balancing is not recommended on Cisco ASR 901 Router.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- The neighbor does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked. By default, REP packets are sent to a BPDU class MAC address. The packets are dropped by devices not running REP.

Fast Convergence

Because REP runs on a physical link basis and not a per-VLAN basis, only one hello message is required for all VLANs, reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time on fiber interfaces is less than 200 ms for the local segment with 200 VLANs configured. Convergence for VLAN load balancing is 300 ms or less.

VLAN Load Balancing (VLB)

One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. The primary edge port always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- Enter the port ID of the interface. To identify the port ID of a port in the segment, use the **show interface rep detail** interface configuration command for the port.

Note Use **rep platform vlb segment** command on every Cisco ASR 901 router participating in the REP segment.

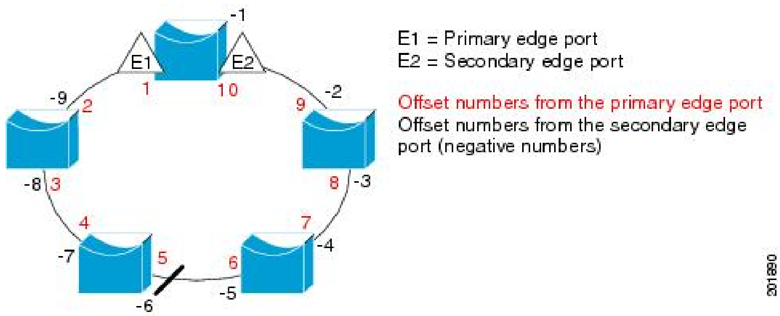
- Enter the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.

Note You configure offset numbers on the primary edge port by identifying the downstream position from the primary (or secondary) edge port. Do not enter an offset value of 1 because that is the offset number of the primary edge port.

Figure 10: Neighbor Offset Numbers in a Segment , on page 191 shows neighbor offset numbers for a segment where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside the ring show the offset numbers from the secondary edge port. Note that you can identify all ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1, and E1 would be -1.

- By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port with the **rep segment** *segment-id* **preferred** interface configuration command.

Figure 10: Neighbor Offset Numbers in a Segment



When the REP segment is complete, all VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the **rep preempt segment** *segment-id* privileged EXEC command on the router that has the primary edge port.
- Configure a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time elapses.

Note When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends a message to alert all interfaces in the segment about the preemption. When the secondary port receives the message, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load balancing configuration, the primary edge port again waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load balancing status does not change. Configuring a new edge port might cause a new topology configuration.

Note The roles of primary and secondary edge ports is Alt when VLB is enabled. Use **show rep topology** command to check the roles of primary and secondary edge ports.

Spanning Tree Interaction

REP does not interact with MSTP, but the two can coexist. A port that belongs to a segment is removed from spanning tree control, and STP BPDUs are not accepted or sent from segment ports.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment, and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. When the segment is configured in both directions to the edge ports, you then configure the edge ports.

REP Ports

Ports in REP segments are in the Failed, Open, or Alternate states. The various states REP ports go through are as follows:

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port changes to alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports.
- When a failure occurs in a link, all ports move to the open state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port reconfigured as a spanning tree port restarts according to the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

For instructions on how to configure REP, see Configuring Resilient Ethernet Protocol, on page 192.

Configuring Resilient Ethernet Protocol

A segment is a collection of ports connected one to the other in a chain and configured with a segment ID. To configure REP segments, you configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment using interface configuration mode. You should configure a service instance with encapsulation corresponding to the REP admin VLAN and associate it to arbitratory bridge domain.

Note The explicit configuration of EFP gives you the flexibility to choose the bridge domain of your choice.

You should configure two edge ports in the segment, one as the primary edge port and the other, by default, the secondary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one to serve as the segment primary edge port. You can also optionally configure where to send segment topology change notices (STCNs) and VLAN load balancing messages.

This section contains the following topics:

Default REP Configuration

By default, REP is disabled on all interfaces. When enabled, the interface is a regular segment port, unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notices (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs at the primary edge port.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the **show rep interface** command output, the Port Role for this port shows as *Fail Logical Open* ; the Port Role for the other failed port shows as *Fail No Ext Neighbor* . When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port election mechanism.
- REP ports must be Layer 2 ports.
- Be careful when configuring REP through a Telnet connection. Since REP blocks all VLANs until another REP interface sends a message to unblock the VLAN, you might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the REP interface.
- If you connect an STP network to the REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.
- You must configure all ports in the segment with the same set of allowed VLANs, or a misconfiguration occurs.
- REP ports follow these rules:
    - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
    - If only one port on a switch is configured in a segment, the port should be an edge port.
    - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
    - If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
- REP interfaces come up and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.
- You should configure service instance with encapsulation corresponding to the REP admin VLAN and associate it to arbitratory Bridge Domain. This explicit configuration of EFP gives you the flexibility to choose the bridge domain of your choice.
- REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.

- You can configure the duration to keep REP interface alive without receiving a hello message from a neighbor using the **rep lsl-age-timer value interface configuration** command. Valid values range from 120 ms to 10000 ms. When this command is configured, the hello timer is set to the age-timer value divided by three. In normal REP operation, three LSL hellos are sent before the age-timer on the peer switch expires.
- You should configure the **rep platform fast-lsl enable** command to support the REP sessions with LSL timers that are less than one second long. This command helps to detect the link failures in copper or microwave ports faster as the link failure detection takes longer time for these ports. Configuring the **rep platform fast-lsl enable** command helps to get optimal performance for copper or microwave ports. When this command is configured, you can expect only subsecond convergence for REP. The subsecond convergence period is also applicable for normal REP sessions, if fast LSL is configured.
- REP ports cannot be configured as one of these port types:
  - SPAN destination port
  - Private VLAN
  - Tunnel port
  - Access port
- There is a maximum of 128 REP segments per router.

Configuring the REP Administrative VLAN

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- There can be only one administrative VLAN on a router and on a segment. However, this is not enforced by the software.
- For VLB to work, **rep platform vlb** has to be configured on every Cisco ASR 901router participating in the segment.

Complete the following steps to configure the REP administrative VLAN:

Procedure

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

	Command or Action	Purpose
Step 3	**rep admin vlan** *vlan-id* **Example:** `Router(config)# rep admin vlan 1`	Configures a REP administrative VLAN. • *vlan-id*--Specify the administrative VLAN. The range is 1–4094. The default is VLAN 1.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show interface** [*interface-id*] **rep** [**detail**] **Example:** `Router# show interface gigabitethernet0/1 rep detail`	Displays the REP configuration and status for a specified interface. • Enter the physical Layer 2 interface or port channel (logical interface) and the optional detail keyword, if desired.
Step 6	**copy running-config startup config** **Example:** `Router# copy running-config startup config`	(Optional) Saves your entries in the router startup configuration file.

Configuring REP Interfaces

For REP operation, you need to enable it on each segment interface and identify the segment ID. This step is required and must be done before other REP configuration. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

Complete these steps to enable and configure REP on an interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface***interface-nameinterface-id* **Example:**	Specifies the interface, and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface port-channel 1`	• Enter the physical Layer 2 interface or port channel ID. The port-channel range is 1 to 8.

Step 4	**service instance** *instance-id* **ethernet encap dot1q** *admin-vlan* **rewrite ingress tag pop 1 symmetric bridge-domain** *bd-id*
	Example:
	`Router(config-if)# service instance 1 ethernet`
	`encap dot1q 1 rewrite ingress tag pop 1 symmetric bridge-domain 1`
		Configures ethernet virtual circuit for the administrative VLAN.

Step 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred** **Example:** `Router(config-if)# rep segment 1 edge preferred`	Enables REP on the interface, and identifies a segment number. The segment ID range is from 1 to 1024. **Note** You must configure two edge ports, including one primary edge port for each segment. These are the optional keywords: • Enter the **edge** keyword to configure the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports. • (Optional) Enter the **no-neighbor** keyword to configure a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port. • On an edge port, enter the **primary** keyword to configure the port as the primary edge port, the port on which you can configure VLAN load balancing. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** privileged EXEC command.

	Command or Action	Purpose
		• Enter the **preferred** keyword to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.
Step 6	**rep lsl-retries** *number-of-retries* **Example:** `Router(config-if)# rep lsl-retries 4`	Use the rep lsl-retries command to configure the REP link status layer (LSL) number of retries before the REP link is disabled.
Step 7	**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**} **Example:** `Router(config-if)# rep stcn segment 2-5`	(Optional) Configures the edge port to send segment topology change notices (STCNs). • Enter **interface** *interface-id* to designate a physical Layer 2 interface or port channel to receive STCNs. • Enter **segment** *id-list* to identify one or more segments to receive STCNs. The range is from 1–1024. • Enter **stp** to send STCNs to STP networks.
Step 8	**rep platform vlb segment** *segment-id* vlan {*vlan-list* | **all**} **Example:** `Router(config)# rep platform vlb segment 1 vlan 100-200`	(Optional) Configures the VLAN list which forms the VLB group. This command should be issued on all Cisco ASR 901 routers participating in VLB for a particular segment and should have a matching VLAN list. This VLAN list should also match with the **rep block** command issued on primary edge port. • Enter **vlan** *vlan-list* to block a single VLAN or a range of VLANs, • Enter **vlan all** to block all VLANs. This is the default configuration.
Step 9	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} **Example:** `Router(config-if)# rep block port 0009001818D68700 vlan all`	(Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways, and configures the VLANs to be blocked on the alternate port. • Enter the **id** *port-id* to identify the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port

	Command or Action	Purpose
		IDs by entering the **show interface** *interface-id* **rep** [**detail**] privileged EXEC command. • Enter a *neighbor-offset* number to identify the alternate port as a downstream neighbor from an edge port. The range is from –256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of **0** is invalid. Enter -1 to identify the secondary edge port as the alternate port. **Note** Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port. • Enter the **preferred** keyword to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing. • Enter **vlan***vlan-list* to block one VLAN or a range of VLANs. • Enter **vlanall** to block all VLANs. **Note** Enter this command only on the REP primary edge port.
Step 10	**rep preempt delay** *seconds* **Example:** `Router(config-if)# rep preempt delay 60`	(Optional) Configures a preempt time delay. Use this command if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is 15 to 300 seconds. The default is manual preemption with no time delay. **Note** Use this command only on the REP primary edge port.
Step 11	**rep lsl-age-timer** *value* **Example:** `Router(config-if) rep lsl-age-timer 5000`	(Optional) Configure a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor. The range is from 120 to 10000 ms in 40-ms increments; the default is 5000 ms (5 seconds).
Step 12	**rep platform fast-lsl enable** **Example:** `Router(config-if)# rep platform fast-lsl enable`	Enables fast Link Status Layer (LSL) configuration to support the REP sessions with LSL timers that are less than one second long. When this command is configured, you can expect only subsecond convergence for REP.

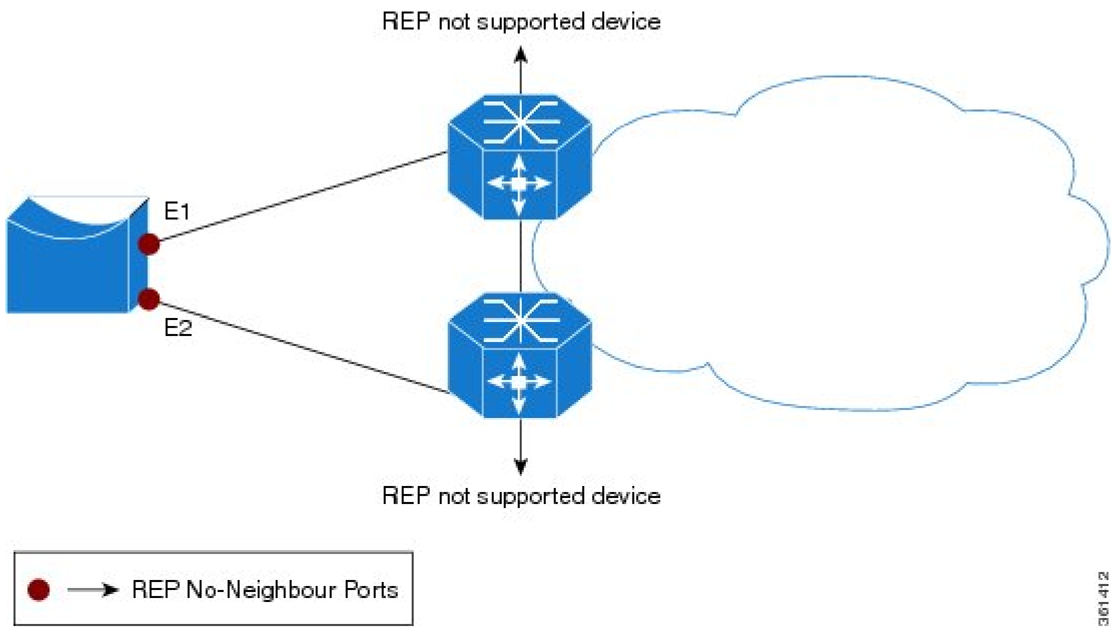
	Command or Action	Purpose
		The subsecond convergence period is also applicable for normal REP sessions, if fast LSL is configured.
Step 13	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 14	**show interface** [*interface-id*] **rep** [**detail**] **Example:** `Router# show interface gigabitethernet0/1 rep detail`	Verifies the REP interface configuration. • Enter the physical Layer 2 interface or port channel (logical interface) and the optional detail keyword, if desired.
Step 15	**show rep topology [segment** *segment-id***] [archive] [detail]** **Example:** `Router# show rep topology segment 1`	Indicates which port in the segment is the primary edge port.
Step 16	**copy running-config startup config** **Example:** `Router# copy running-config startup config`	(Optional) Saves your entries in the router startup configuration file.

Configuring REP as Dual Edge No-Neighbor Port

For REP operation, you need to enable it on each segment interface and identify the segment ID.

Effective with Cisco IOS release 15.4.(1)S, you can configure the non-REP switch facing ports on a single device as dual edge no-neighbor ports. These ports inherit all properties of edge ports, and overcome the limitation of not converging quickly during a failure.

Figure 11: Dual Edge No-neighbor Topology



In access ring topologies, the neighboring switch might not support Figure 11: Dual Edge No-neighbor Topology, on page 200 Figure 12-5 . In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

Complete these steps to enable and configure REP as dual edge no-neighbor port:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface port-channel 1`	Specifies the interface, and enters interface configuration mode. • Enter the physical Layer 2 interface or port channel ID. The port-channel range is 1 to 8.

	Command or Action	Purpose
Step 4	**rep segment** *segment-id***edgeno-neighbor** [**primary** | **preferred** **Example:** `Router(config-if)# rep segment 1 edge no-neighbor preferred`	Enables REP on the interface, and identifies a segment number. The segment ID range is from 1 to 1024. **Note** You must configure two edge ports, including one primary edge port for each segment. These are the optional keywords: • Enter the **edge** keyword to configure the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports. • Enter the **no-neighbor** keyword to configure a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port. • On an edge port, enter the **primary** keyword to configure the port as the primary edge port, the port on which you can configure VLAN load balancing. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** privileged EXEC command. • Enter the **preferred** keyword to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

What to do next

Note For configuring REP LSL timer and VLB, see Configuring REP Interfaces, on page 195.

Cisco ASR 901 Dual Rep Edge No-Neighbor Topology Example

The following configuration example shows a Cisco ASR 901 router running with Dual REP Edge No-Neighbor and two Cisco 7600 series routers running as non-REP devices.

Note This section provides partial configurations intended to demonstrate a specific feature.

ASR_1

```
interface GigabitEthernet0/0
service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1 edge no-neighbor primary
!
interface GigabitEthernet0/1
 service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1 edge no-neighbor preferred
!
interface Vlan1
ip address 172.18.40.70 255.255.255.128
no ptp enable
!
interface Vlan2
ip address 1.1.1.1 255.255.255.0
no ptp enable
!
interface Vlan3
ip address 2.2.2.2 255.255.255.0
no ptp enable
!
interface Vlan3
ip address 4.4.4.2 255.255.255.0
no ptp enable
!
```

```
ip route 3.3.3.0 255.255.255.0 1.1.1.2
ip route 5.5.5.0 255.255.255.0 1.1.1.2
```

7600_1

```
interface Port-channel69
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface GigabitEthernet3/25
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet3/26
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet3/35
ip address 3.3.3.2 255.255.255.0
!
interface GigabitEthernet3/36
ip address 5.5.5.2 255.255.255.0
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 1.1.1.2 255.255.255.0
!
ip route 2.2.2.0 255.255.255.0 1.1.1.1
ip route 4.4.4.0 255.255.255.0 1.1.1.1
```

7600_2

```
interface Port-channel69
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface GigabitEthernet7/25
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
```

```
interface GigabitEthernet7/26
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 1.1.1.3 255.255.255.0
```

Setting up Manual Preemption for VLAN Load Balancing

If you do not enter the **rep preempt delay** *seconds* interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure to complete all other segment configuration before manually preempting VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Note Ethernet over Multiprotocol Label Switching (EoMPLS) is supported on the Cisco ASR 901 router for Cisco IOS Release 15.2(2)SNG and later releases.

Complete these steps on the switch that has the segment primary edge port to manually trigger VLAN load balancing on a segment:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**rep preempt segment** *segment-id* **Example:** `Router# rep preempt segment 1`	Manually triggers VLAN load balancing on the segment. • Enter the segment ID. **Note**

	Command or Action	Purpose
		You will be asked to confirm the action before the command is executed.
Step 4	**end** **Example:** `Router(config)# end`	Returns to the privileged EXEC mode.
Step 5	**show rep topology** **Example:** `Router# show rep topology`	Views the REP topology information.

Configuring SNMP Traps for REP

You can configure the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes. Complete these steps to configure REP traps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp mib rep trap-rate** *value* **Example:** `Router(config)# snmp mib rep trap-rate 500`	Enables the router to send REP traps, and sets the number of traps sent per second. • Enter the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence). **Note** To remove the traps, enter the **no snmp mib rep trap-rate** command.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Displays the running configuration, which you can use to verify the REP trap configuration.
Step 6	**copy running-config startup config** **Example:** `Router# copy running-config startup config`	(Optional) Saves your entries in the router startup configuration file.

Monitoring REP

Complete the following steps to monitor the REP configuration:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface** [*type number*] **rep [detail]** **Example:** `Router# show interface gigabitethernet0/1 rep detail`	(Optional) Displays the REP configuration and status for a specified interface. • Enter the physical Layer 2 interface or port channel (logical interface) and the optional detail keyword, if desired.
Step 3	**show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] **Example:** `Router# show rep topology`	(Optional) Displays REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment. • Enter the optional keywords and arguments, as desired.

Configuration Examples for REP

This section contains the following examples:

Configuring the REP Administrative VLAN: Example

This example shows how to configure the administrative VLAN as VLAN 100.

```
Router# configure terminal
Router(config)# rep admin vlan 100
Router(config-if)# end
```

Configuring a REP Interface: Example

This example shows how to configure an interface as the primary edge port for segment 1, to send Spanning Tree Topology Changes Notification (STCNs) to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery.

```
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# rep
 segment 1 edge primary

Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router (config-if)# rep lsl-age-timer 6000
Router(config-if)# end
```

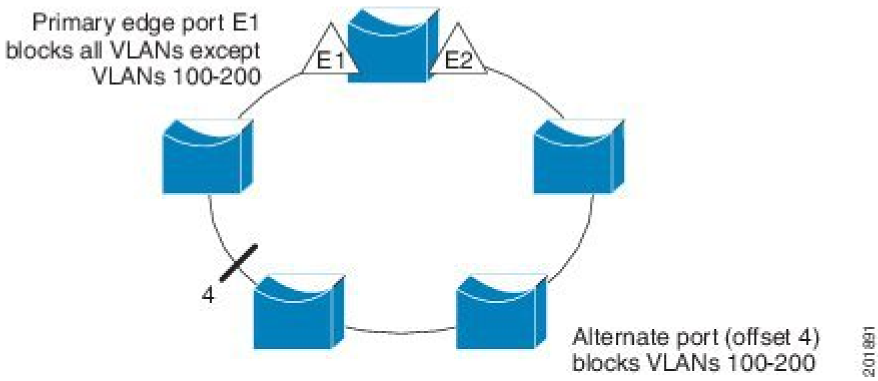
This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Router# configure terminal
Router(conf)# interface gigabitethernet0/1
Router(config-if)# rep segment 1 edge no-neighbor primary
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router(config-if)# rep lsl-age-timer 6000
```

Figure 12: Example of VLAN Blocking, on page 208 shows how to configure the VLAN blocking configuration. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port and all other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 0/1).

```
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# rep
 segment 1 edge primary

Router(config-if)# rep block port 4 vlan 100-200
Router(config-if)# end
Router(config)# rep platform vlb segment 1 vlan 100-200
```

Figure 12: Example of VLAN Blocking



Setting up the Preemption for VLAN Load Balancing: Example

The following is an example of setting the preemption for VLAN load balancing on a REP segment.

```
Router> enable

Router# configure terminal

Router# rep preempt segment 1
```

Router# **end**

Configuring SNMP Traps for REP: Example

This example shows how to configure the router to send REP traps at a rate of 10 traps per second:

```
Router> enable
Router# configure terminal
Router(config)# snmp mib rep trap-rate 10
Router(config)# end
```

Monitoring the REP Configuration: Example

The following is sample output of the **show interface rep detail** command. Use the **show interface rep detail** command on one of the REP interfaces to monitor and verify the REP configuration.

```
Router# show interface gigabitethernet0/1 rep detail

GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
```

```
Preempt Delay Timer: disabled
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

Cisco Cisco ASR 901 Topology Example

The following configuration example shows two Cisco Cisco ASR 901 routers and two Cisco 7600 series routers using a REP ring.

Note This section provides partial configurations intended to demonstrate a specific feature.

ASR_1

```
interface GigabitEthernet0/0
service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1
!
interface GigabitEthernet0/1
 service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1
!
interface GigabitEthernet0/3
 service instance 3 ethernet
  encapsulation dot1q 3
  rewrite ingress tag pop 1 symmetric
  bridge-domain 3
!
interface GigabitEthernet0/4
service instance 4 ethernet
  encapsulation dot1q 4
```

```
  rewrite ingress tag pop 1 symmetric
  bridge-domain 4
!
interface Vlan1
ip address 172.18.40.70 255.255.255.128
no ptp enable
!
interface Vlan2
ip address 1.1.1.1 255.255.255.0
no ptp enable
!
interface Vlan3
ip address 2.2.2.2 255.255.255.0
no ptp enable
!
interface Vlan3
ip address 4.4.4.2 255.255.255.0
no ptp enable
!
ip route 3.3.3.0 255.255.255.0 1.1.1.4
ip route 5.5.5.0 255.255.255.0 1.1.1.4
```

ASR_2

```
interface GigabitEthernet0/0
service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1
interface GigabitEthernet0/1
service instance 1 ethernet
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
 !
rep segment 1
!
interface Vlan1
ip address 172.18.44.239 255.255.255.0
no ptp enable
!
interface Vlan2
ip address 1.1.1.2 255.255.255.0
no ptp enable
```

7600_1

```
interface Port-channel69
switchport
```

```
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface GigabitEthernet3/25
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet3/26
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet3/35
ip address 3.3.3.2 255.255.255.0
!
interface GigabitEthernet3/36
ip address 5.5.5.2 255.255.255.0
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
rep segment 1 edge
interface Vlan1
no ip address
!
interface Vlan2
ip address 1.1.1.4 255.255.255.0
!
ip route 2.2.2.0 255.255.255.0 1.1.1.1
ip route 4.4.4.0 255.255.255.0 1.1.1.1
```

7600_2

```
interface Port-channel69
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
!
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
rep segment 1 edge
!
interface GigabitEthernet7/25
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface GigabitEthernet7/26
switchport
```

```
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2
switchport mode trunk
channel-group 69 mode on
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 1.1.1.3 255.255.255.0
```

CHAPTER 12

Configuring MST on EVC Bridge Domain

This section describes how to configure MST on EVC Bridge Domain.

Overview of MST and STP

Spanning Tree Protocol (STP) is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

For routers to participate in MST instances, you must consistently configure the routers with the same MST configuration information. A collection of interconnected routers that have the same MST configuration comprises an MST region. For two or more routers to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same MST name.

The MST configuration controls the MST region to which each router belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map.

A region can have one or multiple members with the same MST configuration; each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning tree instances. Instances can be identified by any number in the range from 0 to 4094. You can assign a VLAN to only one spanning tree instance at a time.

Overview of MST on EVC Bridge Domain

The MST on EVC Bridge-Domain feature uses VLAN IDs for service-instance-to-MST-instance mapping. EVC service instances with the same VLAN ID (the outer VLAN IDs in the QinQ case) as the one in another MST instance will be mapped to that MST instance.

EVC service instances can have encapsulations with a single tag as well as double tags. In case of double tag encapsulations, the outer VLAN ID shall be used for the MST instance mapping, and the inner VLAN ID is ignored.

A single VLAN per EVC is needed for the mapping with the MST instance. The following service instances without any VLAN ID or with multiple outer VLAN IDs are not supported:

- Untagged (encapsulation untagged) is supported but there is no loop detection on the EVC
- Priority-tagged (encapsulation priority-tagged)
- Multiple outer tags (encapsulation dot1q 200 to 400 second-dot1q 300)

Restrictions and Guidelines

The following restrictions and guidelines apply to MST on EVC bridge domain:

- Cisco IOS Release 15.1(2)SNG supports EVC port-channels.
- With default configuration, Cisco ASR 901 does not run any spanning-tree protocol. Hence all the ports participating in bridge domains are moved to forward state. To enable MSTP, issue **spanning-tree mode mstp** command in the global configuration mode.
- Main interface where the EFP is configured must be up and running with MSTP as the selected Spanning Tree Mode (PVST and Rapid-PVST are not supported).
- The SPT PortFast feature is not supported with EFPs.
- The co-existence of REP and mLACP with MST on the same port is not supported.
- Any action performed on VPORT (which represents a particular VLAN in a physical port) affects the bridge domain and other services.
- Supports 32 MSTs and one CIST (common and internal spanning tree).
- Supports one MST region.
- Scales to 4000 EFPs.
- Untagged EVCs do not participate in MST loop detection.
- Service instances without any VLAN ID in the encapsulation are not supported, because a unique VLAN ID is required to map an EVC to an MST instance.
- Supports EFPs with unambiguous outer VLAN tag (that is, no range, list on outer VLAN, neither default nor untagged).
- Removing dot1q encapsulation removes the EVC from MST.
- Changing the VLAN (outer encapsulation VLAN of EVC) mapping to a different MST instance will move the EVC port to the new MST instance.
- Changing an EVC service instance to a VLAN that has not been defined in MST 1 will result in mapping of EVC port to MST 0.
- The peer router of the EVC port must also be running MST.
- MST is supported only on EVC BD. EVCs without BD configuration will not participate in MST.
- When an MST is configured on the outer VLAN, you can configure any number of service instances with the same outer VLAN as shown in the following configuration example.

```
nPE1#sh run int gi0/5
Building configuration...
Current configuration : 373 bytes
!
interface GigabitEthernet0/5
 description connected to CE1
 no ip address
 service instance 100 ethernet
  encapsulation dot1q 100 second-dot1q 1
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 100 second-dot1q 2
  bridge-domain 101
 !
 service instance 102 ethernet
  encapsulation dot1q 100 second-dot1q 120-140
  bridge-domain 102
 !
end
nPE1#sh run int gi0/6
Building configuration...
Current configuration : 373 bytes
!
interface GigabitEthernet0/6
 description connected to CE1
 no ip address
 service instance 100 ethernet
  encapsulation dot1q 100 second-dot1q 1
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 100 second-dot1q 2
  bridge-domain 101
 !
 service instance 102 ethernet
  encapsulation dot1q 100 second-dot1q 120-140
  bridge-domain 102
 !
end
nPE1#sh span vlan 100
MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     0018.742f.3b80
             Cost        0
             Port        2821 (GigabitEthernet12/5)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     001a.303c.3400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi12/5              Root FWD 20000     128.2821 P2p
Gi12/6              Altn BLK 20000     128.2822 P2p
nPE1#
```

Configuring MST on EVC Bridge Domain

Figure 13: Untagged EVCs not participating in MST loop detection, on page 216 shows an example of the untagged EVCs that do not participate in MST loop detection. When you link your networks together as shown below, a loop is caused since MST is not running on the untagged EVCs.

Figure 13: Untagged EVCs not participating in MST loop detection

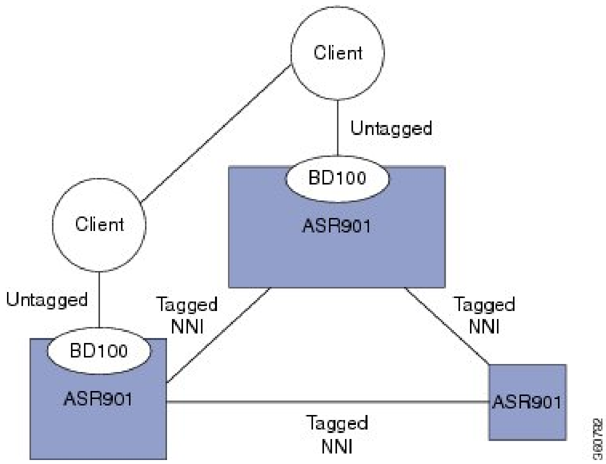
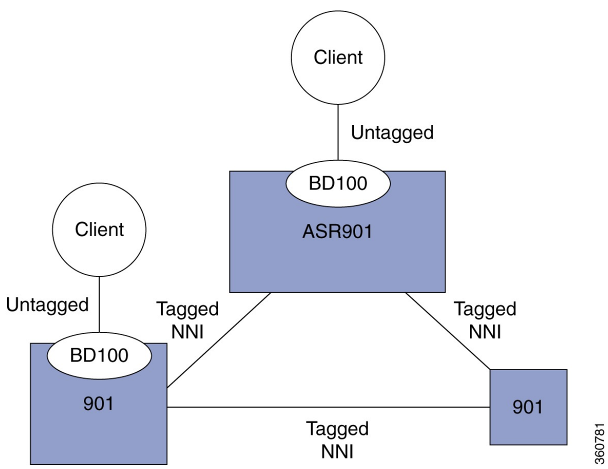


Figure 14: MST with untagged EVCs without loop



Complete the following steps to configure MST on EVC bridge domain.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specifies the gigabit ethernet interface to configure. • *slot/port*—Specifies the location of the interface.
Step 4	**[no] service instance** *id* **Ethernet** [*service-name*] **Example:** `Router(config-if)# service instance 101 ethernet`	Creates a service instance (EVC instance) on an interface and sets the device into the config-if-srv submode.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 13`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**[no] bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 12`	Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.

Configuration Example for MST on EVC Bridge Domain

In the following example, two interfaces participate in MST instance 0, the default instance to which all VLANs are mapped:

```
Router# enable
Router# configure terminal
Router(config)# interface g0/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# interface g0/3
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 2
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# end
```

Verification

Use this command to verify the configuration:

```
Router# show spanning-tree vlan 2
MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     0009.e91a.bc40
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0009.e91a.bc40
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/1        Desg FWD 20000     128.1537 P2p
Gi4/3                Back BLK 20000     128.1540 P2p
```

In this example, interface gi4/1 and interface gi4/3 are connected back-to-back. Each has a service instance (EFP) attached to it. The EFP on both interfaces has an encapsulation VLAN ID of 2. Changing the VLAN ID from 2 to 8 in the encapsulation directive for the EFP on interface gi4/1 stops the MSTP from running in the MST instance to which the old VLAN is mapped and starts the MSTP in the MST instance to which the new VLAN is mapped:

```
Router(config-if)# interface  g4/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encap dot1q 8
Router(config-if-srv)# end
```

Use this command to verify the configuration:

```
Router# show spanning-tree vlan 2
MST1
  Spanning tree enabled protocol mstp
  Root ID    Priority    32769
             Address     0009.e91a.bc40
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0009.e91a.bc40
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/3             Desg FWD 20000     128.1540 P2p
Router# show spanning-tree vlan 8
MST2
  Spanning tree enabled protocol mstp
  Root ID    Priority    32770
             Address     0009.e91a.bc40
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
             Address     0009.e91a.bc40
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi4/1       Desg FWD 20000     128.1537 P2p
```

In this example, interface gi4/3 (with an EFP that has an outer encapsulation VLAN ID of 2 and a bridge domain of 100) receives a new service:

```
Router# enable
Router# configure terminal
Router(config)# interface g4/3
```

```
Router((config-if)# service instance 2 ethernet
Router((config-if-srv)# encap dot1q 2 second-dot1q 100
Router((config-if-srv)# bridge-domain 200
```

Now there are two EFPs configured on interface gi4/3 and both of them have the same outer VLAN 2.

```
interface GigabitEthernet4/3
  no ip address
 service instance 1 ethernet
 encapsulation dot1q 2
 bridge-domain 100
 !
 service instance 2 ethernet
  encapsulation dot1q 2 second-dot1q 100
   bridge-domain 200
```

The preceding configuration does not affect the MSTP operation on the interface; there is no state change for interface gi4/3 in the MST instance it belongs to.

```
Router# show spanning-tree mst 1
##### MST1    vlans mapped:   2
Bridge        address 0009.e91a.bc40  priority      32769 (32768 sysid 1)
Root          this switch for MST1
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi4/3           Desg FWD 20000     128.1540 P2p
```

This example shows MST on port channels:

```
Router# show spanning-tree mst 1
##### MST1 vlans mapped: 3
Bridge address 000a.f331.8e80 priority 32769 (32768 sysid 1)
Root address 0001.6441.68c0 priority 32769 (32768 sysid 1)
port Po5 cost 20000 rem hops 18
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi2/0/0 Desg FWD 20000 128.257 P2p
Po5 Root FWD 10000 128.3329 P2p
Po6 Altn BLK 10000 128.3330 P2p
Router# show spanning-tree vlan 3

MST1
Spanning tree enabled protocol mstp
Root ID Priority 32769
Address 0001.6441.68c0
Cost 20000
Port 3329 (Port-channel5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000a.f331.8e80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi2/0/0 Desg FWD 20000 128.257 P2p
Po5 Root FWD 10000 128.3329 P2p
Po6 Altn BLK 10000 128.3330 P2p
```

Troubleshooting Tips

Table 16: Troubleshooting Scenarios

Problem	Solution
Multiple Spanning Tree Protocol (MSTP) incorrectly or inconsistently formed due to misconfiguration and BPDU loss	To avoid BPDU loss, re-configure these on the following nodes: • Configuration name • Bridge revision • Provider-bridge mode • Instance to VLAN mapping Determine if node A is sending BPDUs to node B. Use the **show spanning-tree mst interface gi1/1 service instance** command for each interface connecting the nodes. Only designated ports relay periodic BPDUs.
MSTP correctly formed, but traffic flooding occurs	Intermittent BPDU loss occurs when the spanning tree appears incorrectly in the show commands, but relays topology change notifications. These notifications cause a MAC flush, forcing traffic to flood until the MAC addresses are re-learned. Use the **debug spanning-tree mst packet full {received | sent}** command to debug topology change notifications. Use the **debug spanning-tree mst packet brief {received | sent}** command on both nodes to check for missing BPDUs. Monitor the timestamps. A time gap greater than or equal to six seconds causes topology change.
MSTP shows incorrect port state	When the spanning tree protocol (STP) attempts to change the port state, it uses L2VPN. Check the value of the sent update. If the value is Yes, then STP is awaiting an update from L2VPN.
Packet forwarding does not match the MSTP state	Complete the following steps to verify and troubleshoot: **1.** Shut down redundant links, remove MSTP configuration, and ensure that basic bridging works. **2.** Check the state of each port as calculated by MSTP, and compare it with the packet counts transmitted and received on ports and EFPs controlled by MSTP. Normal data packets should be sent/received only on ports in the forwarding (FWD) state. BPDUs should be sent/received on all ports controlled by MSTP. **3.** Ensure that BPDUs are flowing and that root bridge selection is correct and check the related scenarios. **4.** Use the show l2vpn bridge-domain detail command to confirm the status of the members of the bridge domain. Ensure that the relevant bridge domain members are active. **5.** Check the forwarding state as programmed in hardware.

CHAPTER 13

Multiprotocol Label Switching

Configuring Multiprotocol Label Switching

Several technologies such as pseudowires utilize MPLS for packet transport. For information on how to configure MPLS, see the MPLS Configuration Guide, Cisco IOS Release 15.1S .

The MPLS feature is supported on the Cisco ASR 901 series routers with the following prerequisites and restrictions:

- The Cisco ASR 901 router does not necessarily support all of the commands listed in the Release *15.1(2)S* documentation.
- In Cisco ASR 901 router, **mpls ip** is configured only on switch virtual interface (SVI). The router supports only a maximum of 60 MPLS enabled SVI interfaces.
- If port channel is configured on an MPLS core, the encapsulation ID should be the same as the bridge domain.
- The maximum number of Label Distribution Protocol (LDP) labels supported in Cisco ASR 901 router is 4000.
- MPLS byte switched counters are not supported.
- For MPLS network, the maximum number of labeled prefixes is 4000.
- For MPLS network with Fast Reroute (FRR), the maximum number of labeled prefixes is 1600.
- For MPLS network with FRR, the maximum number of VRF prefixes is 1600.
- For MPLS network with FRR, the maximum number of labeled and VRF prefixes together is 1600.
- The maximum number of prefix scalability at the global level (without MPLS) is 12000.
- The maximum number of prefix scalability for the global and VRF domain combination is 12000. Here, the VRF scale should not exceed 4000 and the overall IPv4 prefix should not exceed 12000.
- The system scalability is affected if non-MPLS (IGP’s) or MPLS scenarios exceed the prefix scalability.
- MPLS labelled packet load balance over the port channel is not supported.

- The option to disable MPLS time-to-live (TTL) propagation, with the **no mpls ip propagate-ttl** command, is not supported.

CHAPTER 14

Configuring EoMPLS

The Cisco ASR 901 router supports EoMPLS, a subset of AToM that uses a tunneling mechanism to carry Layer 2 Ethernet traffic. Ethernet Over MPLS (EoMPLS) encapsulates Ethernet frames in MPLS packets and forwards them across the MPLS network. In addition to dot1q, untagged, and default encapsulation support for an Ethernet Virtual Connection (EVC) with cross connect, effective with Cisco IOS Release 15.4(2)S, the Cisco ASR 901 router supports dot1ad encapsulation for the EVC with cross connect.

Understanding EoMPLS

EoMPLS encapsulates Ethernet frames in MPLS packets and forwards them across the MPLS network. Each frame is transported as a single packet, and the PE routers connected to the backbone add and remove labels, as appropriate, for packet encapsulation:

- The ingress PE router receives an Ethernet frame and encapsulates the packet by removing the preamble, the Start Frame Delimiter (SFD), and the frame check sequence (FCS). The rest of the packet header is not changed.
- The ingress PE router adds a point-to-point virtual connection (VC) label and a label-switched path (LSP) tunnel label for normal MPLS routing through the MPLS backbone.
- The network core router uses the LSP tunnel label to move the packet through the MPLS backbone and does not distinguish Ethernet traffic from other types of packets in the MPLS backbone.
- At the other end of the MPLS backbone, the egress PE router receives the packet and de-encapsulates the packet by removing the LSP tunnel label, if present. The PE router also removes the VC label from the packet.
- The PE router updates the header, if necessary, and sends the packet out of the appropriate interface to the destination switch.

The MPLS backbone uses the tunnel labels to transport a packet between the PE routers. The egress PE router uses the VC label to select the outgoing interface for the Ethernet packet. Because EoMPLS tunnels are unidirectional, for bidirectional EoMPLS, you should configure one tunnel in each direction.

The point-to-point VC requires you to configure VC endpoints at the two PE routers. Only the PE routers at the ingress and egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 traffic. Other routers do not have table entries for these VCs.

Restrictions for EoMPLS

- When configuring an EoMPLS pseudowire on the Cisco ASR 901 1 Router, you cannot configure an IP address on the same interface as the pseudowire.
- EoMPLS xconnect with VLAN range is not supported.
- EoMPLS xconnect port with double-tagged encapsulation is not supported.
- When port channel is configured on the MPLS core, the encapsulation ID should be equal to the bridge domain.
- To configure cross-connect with dot1ad encapsulation on an EVC, the interface should be a dot1ad NNI port. This means that a service instance with dot1q encapsulation cannot be configured on the port.
- Port-based cross-connect cannot be configured on the dot1ad NNI port interface.
- The encapsulation dot1ad command with cross-connect is not supported on the port channel.
- The dot1ad encapsulation with cross connect is not supported for double tag (QinQ).
- In case of encapsulation dot1ad over cross-connect, push operation at egress is not possible on cross-connect port in scenarios which requires pushing an additional dot1ad tag on the incoming dot1ad tag.
- The maximum number of cross-connect sessions supported on the Cisco ASR 901 Router is 1000. In case of pseudowire redundancy, a maximum of 500 sessions for primary and 500 sessions for backup pseudowire are supported.
- Default EFP under xconnect and untagged EFP under bridge domain on the same interface are not supported.
- Encapsulation is supported only on bridge domain and cross-connect.
- The **rewrite** command in the default EVC encapsulation is rejected.
- Default encapsulation with cross-connect is not supported on the port-channel interface.
- Untagged EFPs are supported only on the port with default encapsulation.
- Layer 3 routing is not supported. Layer 2 VPN is supported on the default encapsulation EFP.
- DSCP based classification for marking is not supported.

Configuring EoMPLS

Complete the following steps to configure EoMPLS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specify the interface, and enter interface configuration mode. Valid interfaces are physical ports. Perform 4 if you want to configure dot1ad encapsulation for an EVC with cross-connect. Go to 5 if you want to configure dot1q encapsulation for an EVC with cross-connect.
Step 4	**ethernet dot1ad nni** **Example:** `Router(config-if)# ethernet dot1ad nni`	Configures a dot1ad NNI port when you want to configure the dot1ad encapsulation for an EVC with cross-connect.
Step 5	**service instance** *instance-id* **ethernet** **Example:** `Router(config-if)# service instance 101 ethernet`	Configure a service instance and enter service instance configuration mode. • The *instance-id* —The service instance identifier, an integer from 1 to 4000. • (Optional) **ethernet** *name* —The name of a previously configured EVC. You do not need to use an EVC name in a service instance.
Step 6	**encapsulation** {**dot1q** *vlan-id* | **dot1ad** *vlan-id* | **untagged** | **default** } **Example:** `Router(config-if-srv)# encapsulation dot1q 51`	Configure encapsulation type for the service instance. • **dot1q**—Configures 802.1Q encapsulation. • **dot1ad**—Configures 802.1ad encapsulation. • **untagged**—Maps to untagged VLANs. Only one EFP per port can have untagged encapsulation. • **default**—Configures default encapsulation to match all the ingress frames on the port.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)#rewrite ingress tag pop 1 symmetric`	(Optional) Specifies that encapsulation modification to occur on packets at ingress. • **pop 1**—Removes the outermost tag. • **symmetric**—Configures the packet to undergo the reverse of the ingress action at egress. If a tag is removed at ingress, it is added at egress. **Note**

	Command or Action	Purpose
		Although the **symmetric** keyword appears to be optional, you must enter it for **rewrite** to function correctly.
Step 8	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 192.168.1.8 101 encapsulation mpls`	Configures cross-connect pseudowire by specifying the IP address of remote peer and the virtual circuit ID.

EoMPLS Configuration Example

The followingis a sample configuration of dot1q encapsulation with cross-connect:

```
interface Loopback0
 description for_mpls_ldp
 ip address 99.99.99.99 255.255.255.255
!
interface GigabitEthernet0/10
 description Core_facing
 no negotiation auto
 service instance 150 ethernet
  encapsulation dot1q 150
  rewrite ingress tag pop 1 symmetric
  bridge-domain 150
!
interface GigabitEthernet0/11
 description CE_facing
 service instance 501 ethernet
  encapsulation dot1q 501
  rewrite ingress tag pop 1 symmetric
  xconnect 111.0.1.1 501 encapsulation mpls
!
interface FastEthernet0/0
 ip address 10.104.99.74 255.255.255.0
 full-duplex
!
interface Vlan1
!
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 mpls ip
!
router ospf 7
 network 99.99.99.99 0.0.0.0 area 0
 network 150.0.0.0 0.0.0.255 area 0
!
no ip http server
ip route 10.0.0.0 255.0.0.0 10.104.99.1
!
logging esm config
!
mpls ldp router-id Loopback0 force
!
```

```
!
end
```

The following is a sample configuration of dot1ad encapsulation with cross-connect:

```
!
interface GigabitEthernet0/1
  negotiation auto
  ethernet dot1ad nni
service instance 45 ethernet
  encapsulation dot1ad 45
  rewrite ingress tag pop 1 symmetric
  xconnect 13.13.13.13 45 encapsulation mpls
!
```

Configuring EVC Default Encapsulation with xconnect

Complete the following steps to configure EVC default encapsulation for xconnect.

Note When default encapsulation is configured on xconnect, the Cisco ASR 901 router does not support untagged encapsulation on the bridge domain of the same interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/4`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**service instance** *instance-id* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Creates a service instance on an interface and defines the matching criteria. • *instance-id*—Integer that uniquely identifies a service instance on an interface.

	Command or Action	Purpose
Step 5	**encapsulation default** **Example:** `Router(config-if)# encapsulation default`	Configures the default service instance. Configures default encapsulation to match all the ingress frames on the port.

Step 6	**xconnect** *peer-ip-address vc-id* **encapsulation mpls**
	Example:
	`Router(config-if-srv)# xconnect 1.1.1.1`
	`100 encapsulation mpls`
		Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire.
		• *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
		• *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers.
		• **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire.
		• **mpls**—Specifies MPLS as the tunneling method.

Verifying EVC Default Encapsulation with xconnect

To verify the configuration of EVC default encapsulation with xconnect, use the **show** command shown below.

```
Router# show running-config interface gigabitEthernet 0/4
Building configuration...
Current configuration : 181 bytes
!
interface GigabitEthernet0/4
no ip address
negotiation auto
no keepalive
service instance 1 ethernet
  encapsulation default
  xconnect 2.2.2.2 100 encapsulation mpls
!
end
```

Configuration Example for EVC Default Encapsulation with Xconnect

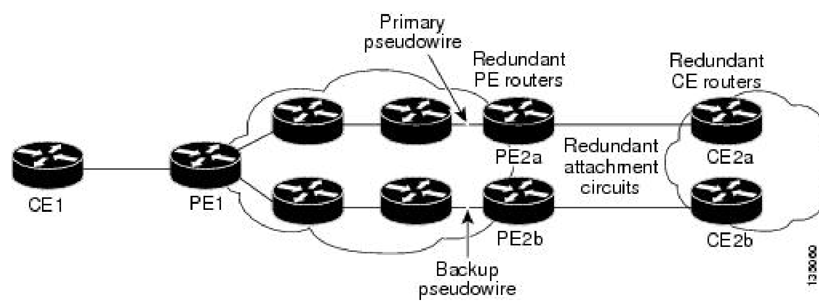
```
!
interface GigabitEthernet0/4
  service instance 10 ethernet
    encapsulation default
    xconnect 1.1.1.1 100 encapsulation mpls
!
```

Configuring Pseudowire Redundancy

Pseudowire (PW) Redundancy enables you to configure a backup pseudowire in case the primary pseudowire fails. When the primary pseudowire fails, the PE router can switch to the backup pseudowire. Traffic can be switched back to the primary pseudowire after the path is operational again.

You can configure the network with redundant pseudowires and redundant network elements, as shown in the following figure.

Figure 15: Configuring Redundant Pseudowires



Configuration Commands

Complete the following steps to configure pseudowire redundancy:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface GigabitEthernet0/2**	Specifies an interface to configure.
Step 3	**service instance 101 ethernet**	Configures a service instance and enters the service instance configuration mode.
Step 4	**encapsulation dot1q 101**	Configures the encapsulation type for the service instance.
Step 5	**rewrite ingress tag pop 1 symmetric**	Specifies the encapsulation modification to be performed on packets at ingress. • **pop 1**—Removes the outermost tag. • **symmetric—**Configures the packet to undergo the reverse of the ingress action at egress. If a tag is removed at ingress, it is added at egress. **Note** Although the **symmetric** keyword seems to be optional, you must enter it for **rewrite** to function correctly.

	Command or Action	Purpose
Step 6	**xconnect 11.205.1.1 141 encapsulation mpls**	Binds the VLAN attachment circuit to an AToM pseudowire for EoMPLS.
Step 7	**backup peer 13.205.3.3 1141**	Specifies a backup peer for redundancy.
Step 8	**end**	Returns to privileged EXEC mode. • **show mpls l2t vc id** • **show mpls l2t vc detail** • **show mpls infrastructure lfd pseudowire internal** Use these commands to display pseudowire information.

Port-Based EoMPLS

The port mode allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire ethernet frame without the preamble or frame check sequence (FCS) is transported as a single packet. To configure port mode, use the xconnect command in the main interface mode and specify the destination address and the VC ID. The syntax and semantics of the xconnect command are the same as for all other transport types. Each interface is associated with one unique pseudowire VC label.

Complete the following steps to configure port-based EoMPLS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router> configure terminal`	Enters the global configuration mode.
Step 3	**interface GigabitEthernet slot/port** **Example:** `Router(config)# interface GigabitEthernet 0/2` **Example:**	Specifies an interface to configure.

	Command or Action	Purpose
	`Router(config-if)#`	
Step 4	**xconnect peer-router-id vcid encapsulation mpls** **Example:** `Router(config)#` **`xconnect 10.0.0.1 123 encapsulation mpls`**	Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as that for all other Layer 2 transports.

What to do next

Feature Information for Configuring EoMPLS

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 17: Feature Information for EoMPLS

Feature Name	Releases	Feature Information
Configuring EoMPLS	15.1(2)SNI	This feature was introduced on the Cisco ASR 901 Routers.
802.1ad for EVC Cross Connect	15.4(2)S	This feature was introduced on the Cisco ASR 901 Routers.

CHAPTER 15

Configuring MPLS VPNs

A Virtual Private Network (VPN) is an IP-based network that delivers private network services over a public infrastructure. VPNs allow you to create a set of sites that can communicate privately over the Internet or other public or private networks.

Understanding MPLS VPNs

A conventional VPN consists of a full mesh of tunnels or permanent virtual circuits (PVCs) connecting all of the sites within the VPN. This type of VPN requires changes to each edge device in the VPN in order to add a new site. MPLS VPNs, also known as Layer 3 VPNs, are easier to manage and expand than conventional VPNs because they use layer 3 communication protocols and are based on a peer model. The peer model enables the service provider and customer to exchange Layer 3 routing information, enabling service providers to relay data between customer sites without customer involvement. The peer model also provides improved security of data transmission between VPN sites because data is isolated between improves security between VPN sites.

The Cisco ASR 901 supports the following MPLS VPN types:

- Basic Layer 3 VPN—Provides a VPN private tunnel connection between customer edge (CE) devices in the service provider network. The provider edge (PE) router uses Multiprotocol Border Gateway Protocol (MP-BGP) to distribute VPN routes and MPLS Label Distribution Protocol (LDP) to distribute Interior Gateway Protocol (IGP) labels to the next-hop PE router.
- Multi-VRF CE—Multi-VRF CE extends limited PE functionality to a CE router in an MPLS-VPN model. A CE router now has the ability to maintain separate VRF tables in order to extend the privacy and security of an MPLS-VPN down to a branch office rather than just at the PE router node.

Note Cisco ASR 901 does not support VRF on TDM interfaces.

Configuring MPLS VPNs

Layer 3 VPNs allow you to establish VPNs in a routed environment, improving the flexibility and ease of maintenance of VPNs. For instructions on how to configure layer 3 VPNs, see the MPLS Configuration Guide, Cisco IOS Release 15.1S .

The following restrictions apply to MPLS VPNs:

- When the port channel is on core, bridge ID must be equal to the encapsulation ID.
- Equal Cost Multipath (ECMP) is not supported for swap cases.
- ECMP is not supported for MPLS-labeled prefixes due to hardware limitation and only one MPLS path can be configured at a time.

Configuration Examples for MPLS VPN

This section contains the following sample configurations involving three routers:

PE1 Configuration

```
Current configuration : 3326 bytes
!
! Last configuration change at 20:37:37 UTC Thu Sep 29 2011
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!card type command needed for slot/vwic-slot 0/0
no logging console
!
no aaa new-model
ip source-route
ip cef
!
ip vrf customer_2
rd 1:2
route-target export 1:2
route-target import 1:2
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback2
no ip address
!
interface Loopback100
ip address 111.0.0.1 255.255.255.255
!
interface GigabitEthernet0/0
no negotiation auto
!
interface GigabitEthernet0/1
no negotiation auto
!
interface GigabitEthernet0/2
no negotiation auto
!
interface GigabitEthernet0/3
no negotiation auto
!
interface GigabitEthernet0/4
no negotiation auto
!
interface GigabitEthernet0/5
media-type sfp
no negotiation auto
cdp enable
service instance 2 ethernet
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
 bridge-domain 2
!
!
interface GigabitEthernet0/6
no negotiation auto
service instance 10 ethernet
 encapsulation dot1q 20
 bridge-domain 120
!
!
interface GigabitEthernet0/7
load-interval 30
media-type sfp
no negotiation auto
cdp enable
service instance 300 ethernet
 encapsulation dot1q 300
 rewrite ingress tag pop 1 symmetric
 bridge-domain 300
```

```
!
!
interface GigabitEthernet0/8
no negotiation auto
!
interface GigabitEthernet0/9
load-interval 30
no negotiation auto
service instance 10 ethernet
 encapsulation dot1q 301
 rewrite ingress tag pop 1 symmetric
 bridge-domain 301
!
!
interface GigabitEthernet0/10
no negotiation auto
ethernet dot1ad nni
service instance 1 ethernet
 encapsulation dot1ad 30
 rewrite ingress tag pop 1 symmetric
!
!
interface GigabitEthernet0/11
no negotiation auto
!
interface ToP0/12
no negotiation auto
!
interface FastEthernet0/0
no ip address
full-duplex
!
interface Vlan1
!
interface Vlan2
ip vrf forwarding customer_2
ip address 2.2.1.1 255.255.255.0
!
interface Vlan300
ip address 1.0.0.1 255.255.255.0
mpls ip
!
interface Vlan301
ip address 11.0.0.1 255.255.255.0
mpls ip
!
router ospf 22
router-id 1.0.0.1
redistribute connected subnets
network 1.0.0.0 0.0.0.255 area 23
network 11.0.0.0 0.0.0.255 area 23
!
router bgp 1
bgp log-neighbor-changes
neighbor 111.0.1.1 remote-as 1
neighbor 111.0.1.1 update-source Loopback100
!
address-family ipv4
 redistribute connected
 neighbor 111.0.1.1 activate
 neighbor 111.0.1.1 send-community both
exit-address-family
!
address-family vpnv4
```

```
 neighbor 111.0.1.1 activate
 neighbor 111.0.1.1 send-community both
exit-address-family
!
address-family ipv4 vrf cust
 redistribute static
 aggregate-address 190.0.0.0 255.0.0.0 summary-only
 redistribute connected
 neighbor 2.2.1.2 remote-as 100
 neighbor 2.2.1.2 activate
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
!
logging esm config
cdp run
!
mpls ldp router-id Loopback100 force
!
!
control-plane
!
!
line con 0
line con 1
transport preferred lat pad telnet rlogin udptn mop ssh
transport output lat pad telnet rlogin udptn mop ssh
line vty 0 4
login
!
exception data-corruption buffer truncate
exception crashinfo buffersize 128
!
end
```

Provider Configuration

```
Router_1#show running-config interface gigabitEthernet 4/15
Building configuration...
Current configuration : 80 bytes
!
interface GigabitEthernet4/15
 ip address 9.0.0.1 255.255.255.0
 mpls ip
end
Router_1#show running-config interface gigabitEthernet 4/16
Building configuration...
Current configuration : 91 bytes
!
interface GigabitEthernet4/16
 ip address 1.0.0.2 255.255.255.0
 mpls ip
end
Router_1#
mpls ldp router-id Loopback2 force
Router_1#show running-config partition router bgp 1
Building configuration...
Current configuration : 664 bytes
!
Configuration of Partition - router bgp 1
```

```
!
!
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 100.0.0.1 remote-as 1
 neighbor 100.0.0.1 update-source Loopback2
 neighbor 100.0.1.1 remote-as 1
 neighbor 100.0.1.1 update-source Loopback2
 !
 address-family ipv4
  no synchronization
  neighbor 100.0.0.1 activate
  neighbor 100.0.0.1 send-community both
  neighbor 100.0.1.1 activate
  neighbor 100.0.1.1 send-community both
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 100.0.0.1 activate
  neighbor 100.0.0.1 send-community both
  neighbor 100.0.1.1 activate
  neighbor 100.0.1.1 send-community both
 exit-address-family
!
!
end
Router_1#
Router_1#show running-config partition router ospf 1
Building configuration...
Current configuration : 197 bytes
!
Configuration of Partition - router ospf 1
!
!
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 1.0.0.0 0.0.0.255 area 0
 network 9.0.0.0 0.0.0.255 area 0
!
!
end
```

PE2 Configuration

Interface details

```
Router_3#show running-config interface gigabitEthernet 6/3
Building configuration...
Current configuration : 79 bytes
!
interface GigabitEthernet6/3
 ip address 9.0.0.2 255.255.255.0
 mpls ip
end
Router_3#show running-config interface gigabitEthernet 6/6
Building configuration...
Current configuration : 107 bytes
!
interface GigabitEthernet6/6
```

```
 ip vrf forwarding customer_red
 ip address 20.20.30.100 255.255.255.0
end
Router_3#show running-config interface gigabitEthernet 6/2
Building configuration...
Current configuration : 136 bytes
!
interface GigabitEthernet6/2
 ip vrf forwarding customer_green
 ip address 20.20.30.99 255.255.255.0
 speed nonegotiate
 mpls ip
end
Router_3#
```

OSPF and BGP details

```
Router_3#show running-config partition router bgp 1
Building configuration...
Current configuration : 1061 bytes
!
Configuration of Partition - router bgp 1
!
!
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 35.35.35.35 remote-as 1
 neighbor 35.35.35.35 update-source Loopback1
 neighbor 100.0.0.1 remote-as 1
 neighbor 100.0.0.1 update-source Loopback1
 !
 address-family ipv4
  no synchronization
  redistribute connected
  neighbor 35.35.35.35 activate
  neighbor 35.35.35.35 send-community both
  neighbor 100.0.0.1 activate
  neighbor 100.0.0.1 send-community both
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 35.35.35.35 activate
  neighbor 35.35.35.35 send-community both
  neighbor 100.0.0.1 activate
  neighbor 100.0.0.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf customer_green
  redistribute static
  aggregate-address 191.0.0.0 255.0.0.0 summary-only
  no synchronization
  redistribute connected
  neighbor 20.20.30.199 remote-as 200
  neighbor 20.20.30.199 activate
 exit-address-family
 !
 address-family ipv4 vrf customer_red
  redistribute static
  aggregate-address 191.0.0.0 255.0.0.0 summary-only
  no synchronization
  redistribute connected
  neighbor 20.20.30.200 remote-as 100
```

```
  neighbor 20.20.30.200 activate
 exit-address-family
!
!
end
Router_3#show running-config partition router ospf 1
Building configuration...
Current configuration : 220 bytes
!
Configuration of Partition - router ospf 1
!
!
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 9.0.0.0 0.0.0.255 area 0
 network 20.20.30.0 0.0.0.255 area 0
 bfd all-interfaces
!
!
end
Router_3#
```

Loop Back details

```
Router_3#show interfaces Loopback 1
Loopback1 is up, line protocol is up
  Hardware is Loopback
  Internet address is 100.0.1.1/24
  MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive set (10 sec)
  Last input 20:14:17, output never, output hang never
  Last clearing of "show interface" counters 22:18:00
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     21 packets output, 1464 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
Router_3#show run | i Loopback
interface Loopback1
interface Loopback60
 neighbor 35.35.35.35 update-source Loopback1
 neighbor 100.0.0.1 update-source Loopback1
mpls ldp router-id Loopback1 force
Router_3#
```

CHAPTER 16

Configuring MPLS OAM

This chapter describes how to configure multiprotocol label switching (MPLS) operations, administration and maintenance (OAM) in the Cisco ASR 901 router.

Understanding MPLS OAM

MPLS OAM helps service providers monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network. The Cisco ASR 901 router supports the following MPLS OAM features:

LSP Ping

MPLS LSP ping uses MPLS echo request and reply packets, similar to Internet Control Message Protocol (ICMP) echo request and reply messages, to validate an LSP. ICMP echo request and reply messages validate IP networks; MPLS OAM echo and reply messages validate MPLS LDP networks. The LSP ping and trace functions use IPv4 UDP packets with UDP port number 3503. You can use MPLS LSP ping to validate IPv4 LDP or Forwarding Equivalence Classes (FECs) by using the **ping mpls** privileged EXEC command. The MPLS echo request packet is sent to a target router by using the label stack associated with the FEC to be validated.

The source address of the LSP echo request is the IP address of the LDP router generating the LSP request. The destination IP address is a 127.x.y.z/8 address, which prevents the IP packet from being switched to its destination if the LSP is broken. The 127.0.0.x destination address range prevents the OAM packets from exiting the egress provider-edge router, which keeps them from leaking from the service-provider network to the customer network.

In response to an MPLS echo request, an MPLS echo reply is forwarded as an IP packet by using IP, MPLS, or a combination of both. The source address of the MPLS echo-reply packet is an address obtained from the router generating the echo reply. The destination address is the source address of the router that originated the MPLS echo-request packet. The MPLS echo-reply destination port is the echo-request source port.

LSP Traceroute

MPLS LSP traceroute also uses MPLS echo request and reply packets to validate an LSP. You can use MPLS LSP traceroute to validate LDP IPv4 by using the **trace mpls** privileged EXEC command. The traceroute time-to-live (TTL) settings force expiration of the TTL along an LSP. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4) to discover the downstream mapping of each successive hop. The transit router processing the MPLS echo request returns an MPLS echo reply containing information about the transit hop in response to the TTL-expired MPLS packet. The MPLS echo reply destination port is sent to the echo request source port.

LSP Ping over Pseudowire

The LSP Ping over Pseudowire is used for detecting faults in the data plane or forwarding path for pseudowire services. The connectivity verification model for pseudowires consists of:

- Advertising the VCCV capability
- Verifying the data plane connectivity

Advertising the VCCV capability is done as part of MPLS Label Mapping message. This consists of Control Channel (CC) type which is a bitmask that indicates the type of control channel that can be used to verify connectivity. The Cisco ASR 901 router supports the following CC type:

- MPLS Router Alert Label (Type 2) : The control channel is created out of band and uses the router alert label (RA).

Note The Cisco ASR 901 router does not support Control Channel Type 1 and 3.

Connectivity verification type defines a bitmask that indicates the types of CV packets and protocols that can be sent on the specified control channel.

The LSP ping over pseudowire uses the same label stack as used by the pseudowire data path. Basically it contains the virtual circuit (VC) label and tunnel labels.

How to Configure MPLS OAM

This section contains the following topics:

Note On Cisco ASR 901 , for a default MTU of 1500 bytes, IOS supports MPLS ping up to 1486 bytes. For MPLS ping with size more than 1486 bytes to work in Cisco ASR 901 , the MTU setting on the SVI has to be adjusted to be more than 1500 bytes.

Using LSP Ping for LDP IPv4 FEC

When you enter the **ping mpls** privileged EXEC command to begin an LSP ping operation, the keyword that follows specifies the Forwarding Equivalence Class (FEC) that is the target of the LSP ping to which you want to verify connectivity.

Command	Purpose
ping mpls ipv4 *destination-address destination-mask*	To verify LSP path from Cisco ASR 901 to remote peer. The keywords have these meanings: • *destination-address destination-mask* —Specify the address and network mask of the target FEC.

Using LSP Traceroute for LDP IPv4 FEC

The LSP traceroute originator sends incremental MPLS echo requests to discover the downstream mapping of each successive hop. When the originating provider edge router receives the reply from the intermediate router, it forms another MPLS echo request with the same target FEC and the time-to-live is incremented by one.

Command	Purpose
traceroute mpls ipv4 *destination-address destination-mask*	To configure LSP IPv4 traceroute. • *destination-address destination-mask* is the address and network mask of the target FEC.

Using LSP Ping for Pseudowire

Use the **ping mpls pseudowire** command to verify the AToM pseudowire path.

Command	Purpose
ping mpls pseudowire *ipv4-address* **vc_id** *vc-id-value*	To verify AToM pseudowire path from the Cisco ASR 901 router to remote peer. • *ipv4-address* is the ip address of the remote peer. • **vc_id** is the virtual circuit id.

Using LSP Traceroute over Pseudowire

Use the **traceroute mpls pseudowire** command to verify the pseudowire path and the next hop details at the remote peer.

Command	Purpose
traceroute mpls pseudowire *ipv4-address* **vc_id** *vc-id-value segment*	To verify AToM pseudowire path from the Cisco ASR 901 router to remote peer and next hop details at remote peer. • *ipv4-address* is the ip address of the remote peer. • **vc_id** is the virtual circuit id.

Displaying AToM VCCV capabilities

Use the **show mpls l2transport** command to display the AToM VCCV capabilities.

Command	Purpose
show mpls l2transport binding vc_id *vc-id-value*	To display AToM VCCV capabilities negotiated between the peers. • **vc_id** is the virtual circuit id.

CHAPTER 17

Configuring Routing Protocols

Configuring Routing Protocols

In addition to static routing, the Cisco ASR 901 supports the following routing protocols:

- OSPF—An Interior Gateway Protocol (IGP) designed for IP networks that supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. For more information on how to configure OSPF, see the IP Routing: OSPF Configuration Guide, Cisco IOS Release 15.1S .
- IS-IS—An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains. For more information on how to configure IS–IS, see the IP Routing: ISIS Configuration Guide, Cisco IOS Release 15.1S .
- BGP—An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems). For more information on how to configure BGP, see the IP Routing: BGP Configuration Guide, Cisco IOS Release 15.1S .

For information about Bidirectional Forwarding Detection (BFD) including sample routing configurations with BFD, see Configuring BFD, on page 247.

Note Cisco ASR 901 router supports IP routing on SVI interfaces.

Note Cisco ASR 901 router does not support IGP fast timers.

Note Cisco ASR 901 router does not support CLNS routing.

Note The maximum number of prefixes supported in Cisco ASR 901 router is 12000.

Note The maximum number of SVI's supported in Cisco ASR 901 router is 250.

Changing Default Hashing Algorithm for ECMP

The hashing algorithm for ECMP is changed from Cisco IOS Release 15.3(2)S onwards. You can use the following commands to configure various types of ECMP hash configurations for improved load distribution of IP traffic.

- **asr901-ecmp-hash-config global-type**
- **asr901-ecmp-hash-config ipv4-type**
- **asr901-ecmp-hash-config ipv6-type**
- **asr901-ecmp-hash-config mpls-to-ip**

For detailed information on these commands, see the Cisco ASR 901 Series Aggregation Services Router Command Reference guide at the following location: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/cr/b_cr_for_asr901s.html.

CHAPTER 18

Configuring Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels.

Understanding BFD

Cisco supports the BFD asynchronous mode, in which two routers exchange BFD control packets to activate and maintain BFD neighbor sessions. To create a BFD session, you must configure BFD on both systems (or BFD peers). After you enable BFD on the interface and the router level for the appropriate routing protocols, a BFD session is created, BFD timers are negotiated, and the BFD peers begin to send BFD control packets to each other at the negotiated interval.

Configuring BFD

This section contains the following topics:

For more information about BFD, refer to the IP Routing: BFD Configuration Guide, Cisco IOS Release 15.1S .

Note Cisco ASR 901 supports BFD echo mode.

BFD Configuration Guidelines and Restrictions

- The minimum time interval supported for BFD is 50 ms.
- The maximum number of stable sessions supported for BFD with 50 ms interval is 4.
- BFD and REP together are not recommended on Cisco ASR 901 Router while sharing the same link.

- After enabling BFD on an interface, if you configure an IPV4 static route with BFD routing through this interface, and if the IPV4 BFD session does not get established, unconfigure BFD on the given interface, and configure it again. The BFD session comes up.
- When you move the BFD configuration saved in flash memory to the running configuration, BFD session is re-established.
- When BFD is configured on a port from which more than 70% of line rate data traffic is egressing, there is a drop in control packets including BFD packets. To avoid BFD packet drop, you have to configure QoS policies that give higher priority for both CPU generated BFD packets and BFD echo reply packets.

Configuring BFD for OSPF

This section describes how to configure BFD on the Cisco ASR 901 router.

Configuring BFD for OSPF on One of More Interfaces

Complete these steps to configure BFD for OSPF on a single interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan1**	Specifies an interface to configure.
Step 4	**ip ospf bfd**	Enables BFD for OSPF on the interface.
Step 5	**bfd interval 50 min_rx 50 multiplier 3**	Specifies the BFD session parameters.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

What to do next

Note You can also use the **show bfd neighbors** and **show ip ospf** commands to display troubleshooting information about BFD and OSPF.

Configuring BFD for OSPF on All Interfaces

Complete these steps to configure BFD for OSPF on all interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf 100**	Creates a configuration for an OSPF process.
Step 4	**bfd all-interfaces**	Enables BFD globally on all interfaces associated with the OSPF routing process.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

What to do next

Note You can disable BFD on a single interface using the **ip ospf bfd disable** command when configuring the relevant interface.

Configuring BFD for BGP

Complete these steps to configure BFD for BGP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-tag*	Specifies a BGP process and enter router configuration mode.
Step 4	**neighbor** *ip-address* **fall-over bfd**	Enables support for BFD failover.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.
Step 6	**show bfd neighbors [details]** **Example:** `show ip bgp neighbor`	Use the following commands to verify the BFD configuration: • **show bfd neighbors [details]**—Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. • **show ip bgp neighbor**—Displays information about BGP and TCP connections to neighbors.

Configuring BFD for IS-IS

This section describes how to configure BFD for IS-IS routing.

Configuring BFD for IS-IS on a Single Interface

Complete these steps to configure BFD for IS-IS on a single interface.

Procedure

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

	Command or Action	Purpose
Step 3	**interface vlan1**	Enters interface configuration mode.
Step 4	**ip router isis [tag]**	Enables support for IPv4 routing on the interface.
Step 5	**isis bfd**	Enables BFD on the interfaces.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

What to do next

Note You can use the **show bfd neighbors** and **show clns interface** commands to verify your configuration.

Configuring BFD for IS-IS for All Interfaces

Complete these steps to configure BFD for IS-IS on all interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan1**	Enters interface configuration mode.
Step 4	**ip router isis [tag]**	Enables support for IPv4 routing on the interface.
Step 5	**bfd all-interfaces**	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits the interface.

	Command or Action	Purpose
Step 7	**interface vlan1** **Example:** `Router(config-if) ip router isis [tag]`	If you want to enable BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process, complete the following steps: • Use the interface command to enter interface configuration mode. • Use the **ip router isis** command to enables support for IPv4 routing on the interface.
Step 8	**exit** **Example:** `Router(config)# exit`	Exit configuration mode.

What to do next

Note You can use the **show bfd neighbors** and **show clns interface** commands to verify your configuration.

Configuring BFD for Static Routes

Complete these steps to configure BFD for static routes.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 150**	Specifies an interface and enters interface configuration mode.
Step 4	**ip address 10.201.201.1 255.255.255.0**	Configures an IP address for the interface.
Step 5	**bfd interval 50 min_rx 50 multiplier 3**	Enables BFD on the interface.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode.
Step 7	**ip route static bfd Vlan150 150.0.0.2**	Specifies neighbors for the static routes in BFD.
Step 8	**ip route 77.77.77.0 255.255.255.0 Vlan150**	Specifies the exit interface for the static route in BFD.

What to do next

Note You can use the **show ip static route** command to verify your configuration.

Configuration Examples for BFD

The following section contains sample configurations for each routing protocol using BFD.

Note This section provides partial configurations intended to demonstrate a specific feature.

BFD with OSPF on All Interfaces

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
 service instance 150 ethernet
  encapsulation untagged
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
router ospf 7
 network 99.99.99.99 0.0.0.0 area 0
 network 150.0.0.0 0.0.0.255 area 0
 bfd all-interfaces
```

BFD with OSPF on Individual Interfaces

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
```

```
 service instance 150 ethernet
  encapsulation untagged
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 ip ospf bfd
!
router ospf 7
 network 99.99.99.99 0.0.0.0 area 0
 network 150.0.0.0 0.0.0.255 area 0
```

BFD with BGP

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
 service instance 150 ethernet
  encapsulation untagged
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 150.0.0.2 remote-as 2
 neighbor 150.0.0.2 fall-over bfd
```

BFD with IS-IS on All Interfaces

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
 service instance 150 ethernet
  encapsulation untagged
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
router isis
 net 49.0001.2222.2222.2222.00
 bfd all-interfaces
!
```

BFD with IS-IS on Individual Interfaces

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
 service instance 150 ethernet
  encapsulation untagged
```

```
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 isis bfd
!
router isis
 net 49.0001.2222.2222.2222.00
!
```

BFD with Static Routes

```
interface GigabitEthernet0/10
 description Core_facing
 negotiation auto
 service instance 150 ethernet
  encapsulation untagged
  bridge-domain 150
 !
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
ip route static bfd Vlan150 150.0.0.2
ip route 77.77.77.0 255.255.255.0 Vlan150 150.0.0.2
```

CHAPTER 19

Configuring T1/E1 Controllers

This chapter provides information about configuring the T1/E1 controllers on Cisco ASR 901 router.

Configuring the Card Type

Perform a basic card type configuration by enabling the router, enabling an interface, and specifying the card type as described below. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

To select and configure a card type, complete the following steps:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**card type** {**e1** | **t1**} *slot subslot* **Example:** `Router(config)# card type e1 0 0`	Sets the card type. The command has the following syntax: • *slot*—Slot number of the interface. • *subslot*—Sub slot number of the interface. When the command is used for the first time, the configuration takes effect immediately. A subsequent change in the card type does not take effect unless you enter the reload command or reboot the router. **Note** When you are using the card type command to change the configuration of an installed card, you must first enter the **no card type** {**e1** | **t1**} *slot subslot* command. Then enter the **card type** {**e1** | **t1**} *slot subslot* command for the new configuration information.
Step 4	**exit** **Example:** `Router(config)# exit`	Exit configuration mode.

Configuring E1 Controllers

Perform a basic E1 controller configuration by specifying the E1 controller, entering the clock source, specifying the channel-group, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

To configure the E1 controllers, complete the following steps in the global configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**controller e1** *slot/port*
	Example:
	`Router(config)# controller e1 0/0`
	`Router(config-controller)#`
		Specifies the controller that you want to configure.

Step 4	**framing** {**crc4** | **no-crc4**} **Example:** `Router(config-controller)# framing crc4`	Specifies the framing type.
Step 5	**linecode hdb3** **Example:** `Router(config-controller)# linecode hdb3`	Specifies the line code format.

Step 6	**channel-group** *channel-no* **timeslots** *timeslot-list* **speed** {**64**}
	Example:
	`Router(config-controller)# channel-group 0`
	`timeslots 1-31 speed 64`
		Specifies the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created. The syntax is:
		• *channel-no*—ID number to identify the channel group. The valid range is from 0–30.
		• *timeslot-list*—Timeslots (DS0s) to include in this channel-group. The valid time slots are from 1–31.
		• **speed {64}**—The speed of the DS0.
		The example configures the channel-group and time slots for the E1 controller:
		Note
		When you are using the channel-group channel-no timeslots timeslot-list {64} command to change the configuration of an installed card, you must enter the no channel-group channel-no timeslots timeslot-list speed {64} command first. Then enter the channel-group channel-no timeslots timeslot-list {64} command for the new configuration information.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config)# exit`	Exits controller configuration mode.

Step 8	**interface serial** *slot/port:channel*
	Example:
	`Router(config)# interface serial 0/0:1`
	`Router(config-if)#`
		Configures the serial interface. Specify the E1 slot, port number, and channel-group.
		When the prompt changes to Router(config-if), you have entered interface configuration mode.
		Note
		To see a list of the configuration commands available to you, enter ? at the prompt or press the Help key while in the configuration mode.

Step 9	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Specifies PPP encapsulation on the interface.
Step 10	**keepalive** [**period** [*retries*]] **Example:** `Router(config-if)# keepalive [period [retries]]`	Enables keepalive packets on the interface and specifies the number of times keepalive packets are sent without a response before the router disables the interface.
Step 11	**end** **Example:** `Router# end`	Exits interface configuration mode.

Support for Unframed E1

Effective with Cisco IOS Release 15.4(3)S, support is available for unframed E1, enabling the use of *timeslot 0* for data to utilize the full capacity (2.048 Mbps) of E1 controllers, against the previous maximum bandwidth limit of 1.984 Mbps.

As *timeslot 0* is used for data, a few alarms are not supported. The following table provides information on supported and unsupported alarms:

Table 18: Supported and Unsupported Alarms

Alarm	Support
AIS	Yes
LOF	No
LOS	Yes

Alarm	Support
RAI	No

Note Support for Unframed E1 is available only on Cisco ASR 901 Routers using the *AdvancedMetroIPAccess* license.

Configuring Support for Unframed E1 Controller

To configure support for an unframed E1 controller, perform this task.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller e1** *slot port* **Example:** `Router(config)# controller e1 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**channel-group** *group-number* **unframed** **Example:** `Router(config-controller)# channel-group 0 unframed`	Enables support for an unframed E1 controller on the controller interface. **Note** This command is supported only on an E1 controller.

Configuring T1 Controllers

Use the following steps to perform a basic T1 controller configuration: specifying the T1 controller, specifying the framing type, specifying the line code form, specifying the channel-group and time slots to be mapped, configuring the cable length, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

To configure the T1 interfaces, complete the following steps in the global configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.
Step 3	**controller t1** *slot/subslot* **Example:** `Router(config-controller)# controller t1 0/0`	Specifies the controller that you want to configure. The command has the following syntax: • *slot*—Slot number of the interface. The slot number should be 0. • *subslot*—Subslot number of the interface. The supported range for subslot is 0 to 15.
Step 4	**framing esf** **Example:** `Router(config-controller)# framing esf`	Specifies the framing type.
Step 5	**linecode** *line-code* **Example:** `Router(config-controller)# linecode b8zs`	Specifies the line code format.

Step 6	**channel-group** *group-no* **timeslots 1-24 speed** *speed*
	Example:
	`Router(config-controller)# channel-group 0`
	`timeslots 1-24 speed 64`
		Specifies the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.
		• The default speed of the channel-group is 64.
		• The supported range for channel-group is 0 to 23.

	Command or Action	Purpose
Step 7	**cablelength {long [-15db | -22.5db | -7.5db | 0db] short [110ft | 220ft | 330ft| 440ft | 550ft | 600ft]}** **Example:** `Router(config-controller)#  cablelength long -15db`	Configures the cable length.
Step 8	**exit** **Example:** `Router(config-controller)#  exit`	Exits controller configuration mode.
Step 9	**interface serial** *slot/port* :**channel** **Example:** `Router(config)#  interface serial 0/1:0`	Configures the serial interface. Specify the T1 slot (always 0), port number, and channel-group.
Step 10	**encapsulation ppp** **Example:** `Router(config-if)#  encapsulation ppp`	Enters the following command to configure PPP encapsulation.
Step 11	**keepalive** [*period* [*retries*]] **Example:** `Router(config-if)#  keepalive 5 6`	Enables keepalive packets on the interface and specify the number of times that keepalive packets will be sent without a response the interface is brought down:
Step 12	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Verifying Support for Unframed E1 Controller

To verify support for an unframed E1 controller, use the following **show** command:

```
Router# show controllers e1 0/0

E1 0/0 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  alarm-trigger is not set
  Framing is unframed, Line Code is HDB3, Clock Source is Internal.
  Data in current interval (19 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
  Data in Interval 1:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Data in Interval 2:
```

```
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
```

Troubleshooting Controllers

This line card supports local and network T1/E1 loopback modes, and remote T1 loopback modes for testing, network fault isolation, and agency compliance. You can test T1/E1 lines in local and network loopback modes. You can also test T1 lines in remote mode.

Note The ASR901 supports activating or deactivating payload and line loopback modes using FDL in ESF framing mode as defined in the T1.403 ANSI standard. The implementation confirms to ANSI T1.403-1999, sections 9.4.2.1 and 9.4.2.2. The ASR901 only accepts remotely initiated loopback requests and does not support initiation of FDL remote loopback requests.

Note Bit-error-rate testing and loopbacks are used to resolve problems and test the quality of T1/E1 links.

Troubleshooting E1 Controllers

To troubleshoot the E1 line card, complete the following steps in the controller configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**controller e1***slot/subslot* **Example:** `Router(config-controller)# controller e1 0/0`	Sets the controller type. The command has the following syntax: • *slot*—Slot number of the interface. • *subslot*—0.

	Command or Action	Purpose
Step 4	**loopback {local | network {line| payload}}** **Example:** `Router(config-controller)# loopback network line`	Sends the packets from a port in local loopback to the remote end. • **local**—Configures the line card to loop the transmitted traffic back to the line card as E1 received traffic and transmits AIS to the remote receiver. • **line**—Configures the E1 line card to loop the received traffic back to the remote device after passing them through the line loopback mode of the framer. The framer does not re-clock or reframe the incoming traffic. • **payload**—Configures the E1 line card to loop the received traffic back to the remote device after passing them through the payload loopback mode of the framer. The framer re-clocks and reframes the incoming traffic before sending it to the network.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the controller configuration mode.

Troubleshooting T1 Controllers

To troubleshoot the T1 line card, complete the following steps in the controller configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**controller t1** *slot/subslot* **Example:**	Sets the controller type. The command has the following syntax: • *slot*—Slot number of the interface.

	Command or Action	Purpose
	`Router(config-controller)# controller t1 0/0`	• *subslot*—0.
Step 4	**loopback {diagnostic | local {line| payload}}** **Example:** `Router(config-controller)# loopback local line`	Sends the packets from a port in local loopback to the remote end. • **diagnostic**—Configures the line card to loop data from the transmit path to the receiver path. • **line**—Configures the T1 line card to loop the received traffic back to the remote device after passing them through the line loopback mode of the framer. The framer does not re-clock or reframe the incoming traffic. • **payload**—Configures the T1 line card to loop the received traffic back to the remote device after passing them through the payload loopback mode of the framer. The framer re-clocks and reframes the incoming traffic before sending it to the network.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the controller configuration mode.

CHAPTER 20

Configuring Pseudowire

Cisco Pseudowire Emulation Edge-to-Edge (PWE3) allows you to transport traffic using traditional services such as E1/T1 over a packet-based backhaul technology such as MPLS or IP. A pseudowire (PW) consists of a connection between two provider edge (PE) devices that connects two attachment circuits (ACs), such as ATM VPIs/VCIs or E1/T1 links.

Understanding Pseudowires

Pseudowires (PWs) manage encapsulation, timing, order, and other operations in order to make it transparent to users; the PW tunnel appears as an unshared link or circuit of the emulated service.

There are limitations that impede some applications from utilizing a PW connection.

Cisco supports the following standards-based PWE types:

Structure-Agnostic TDM over Packet

SAToP encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing. The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the PEs. For example, a T1 attachment circuit is treated the same way for all delivery methods, including: PE on copper, multiplex in a T3 circuit, mapped into a virtual tributary of a SONET/SDH circuit, or carried over a network using unstructured Circuit Emulation Service (CES). Termination of specific carrier layers used between the PE and circuit emulation (CE) is performed by an appropriate network service provider (NSP).

For instructions on how to configure SAToP, see Configuring Structure-Agnostic TDM over Packet, on page 273.

For a sample SAToP configuration, see Configuration Examples for Pseudowire, on page 297.

Structure-Aware TDM Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured (NxDS0) TDM signals as PWs over PSNs.

Emulation of NxDS0 circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

For instructions on how to configure CESoPSN, see Configuring Circuit Emulation Service over Packet-Switched Network, on page 277.

For a sample CESoPSN configuration, see Configuration Examples for Pseudowire, on page 297.

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 901 implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

For instructions on how to create an EoMPLS PW, see Configuring Transportation of Service Using Ethernet over MPLS, on page 281.

Limitations

- When configuring an EoMPLS pseudowire on the Cisco ASR 901 , you cannot configure an IP address on the same interface as the pseudowire.
- Layer 2 Tunneling Protocol, version 2 and 3 (L2TPv2 and L2TPv3) is not supported on the Cisco ASR 901 series routers.
- The maximum number of CEM groups supported under each controller is four.

Hot Standby Pseudowire Support for ATM/IMA

The Hot Standby Pseudowire Support for Inverse Multiplexing over ATM (IMA) feature improves the availability of pseudowires by detecting failures and handling them with minimal disruption to the service. This feature allows the backup pseudowire to be in a “hot standby” state, so that it can immediately take over if the primary pseudowire fails.

A backup pseudowire is provisioned and corresponding entries are populated to hardware tables. When the primary pseudowire goes down, the backup pseudowire is used to switch the packets.

This feature supports the following transport types:

- ATM AAL5 in VC mode
- ATM in VP mode
- ATM in port mode

Configuring Pseudowire

This section describes how to configure pseudowire on the Cisco ASR 901 . The Cisco ASR 901 supports pseudowire connections using CESoPSN. The following sections describe how to configure pseudowire connections.

For full descriptions of each command, see the *Cisco ASR 901 Series Aggregation Services Command Reference Guide*.

For pseudowire configuration examples, see Configuration Examples for Pseudowire, on page 297.

Configuring Pseudowire Classes

A pseudowire class allows you to create a single configuration template for multiple pseudowire connections. You can apply pseudowire classes to all pseudowire types.

Complete the following steps to configure a pseudowire class:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class class-name** **Example:** `Router(config)# pseudowire-class newclass`	Creates a new pseudowire class.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw-class)# encapsulation mpls`	Sets an encapsulation type.

	Command or Action	Purpose
Step 5	**interface cem** *slot/port* **Example:** `Router(config)# interface cem0/0`	Configures the pseudowire interface to use for the new pseudowire class. This example shows a CESoPSN interface.
Step 6	**cem** *group-number* **Example:** `Router(config-if)# cem 0`	Defines a CEM channel.
Step 7	**xconnect** *ip* **pw-class** *pseudowire-class* **Example:** `Router(cfg-if-cem)# xconnect 1.1.1.1 40 pw-class myclass`	Binds an attachment circuit to the CESoPSN interface to create a CESoPSN pseudowire. Use the **pw-class** parameter to specify the pseudowire class that the CESoPSN pseudowire interface uses.

What to do next

Note You cannot use the encapsulation **mpls** parameter with the **pw-class** parameter.

Note The use of the **xconnect** command can vary depending on the type of pseudowire you configure.

Configuring CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires.

Note Cisco IOS release 15.3(3)S automatically enables forward-alarm ais configuration (under the config-controller configuration mode). To disable this configuration, use the **no forward-alarm ais** command.

- The forward-alarm ais configuration is applicable only for CESoP. It is not supported for SAToP.
- You must run the **no forward-alarm ais** command before using CESoP with controllers in loopback (either through loopback command under controller or by using a physical loopback jack).
- Though the **forward-alarm ais** command (and its no form) was not supported in previous releases, the Cisco ASR 901 router behaved as if this command was configured under the controller interface.

Complete the following steps to configure a CEM class:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class cem** *cem-class-name* **Example:** `Router(config)# class cem mycemclass`	Creates a new CEM class
Step 4	**payload-size** *size* **Example:** `Router(config-cem-class)# payload-size 512`	Specifies the payload for the CEM class.
Step 5	**dejitter-buffer** *size* **Example:** `Router(config-cem-class)# dejitter-buffer 10`	Specifies the dejitter buffer for the CEM class.
Step 6	**idle-pattern** *size* **Example:** `Router(config-cem-class)# idle-pattern 0x55`	Specifies the idle-pattern for the CEM class.
Step 7	**exit** **Example:** `Router(config-cem-class)# exit`	Returns to the config prompt.
Step 8	**interface cem** *slot/port* **Example:** `Router(config)# interface cem 0/0`	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.

	Command or Action	Purpose
Step 9	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 10	**cem group-number** **Example:** `Router(config-if)# cem 0`	Enters the CEM configuration mode.
Step 11	**cem class** *cem-class-name* **Example:** `Router(config-if-cem)# cem class mycemclass`	Specifies the CEM class name.
Step 12	**xconnect** *ip-address encapsulation* **mpls** **Example:** `Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls`	Binds an attachment circuit to the CEM interface to create a pseudowire

Configuring a Backup Peer

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 901 diverts traffic to the backup PW.

Complete the following steps to configure a backup peer:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *name slot/port* **Example:** `Router(config)# interface cem0/0`	Configures the pseudowire interface to use for the new pseudowire class.

	Command or Action	Purpose
Step 4	**cem** *group-number* **Example:** `Router(config-if)# cem 0`	Defines a CEM channel.
Step 5	**xconnect** *peer-loopback-ip-address* **encapsulation mpls** **Example:** `Router(config-if-cem)# xconnect 10.10.10.20 encapsulation mpls`	Binds an attachment circuit to the CEM interface to create a pseudowire.
Step 6	**backup peer** *peer-router-ip-address vcid* [**pw-class** *pw-class-name*] **Example:** `Router(config-if-cem-xconn)# backup peer 10.10.10.12 10 344`	Defines the address and VC of the backup peer.
Step 7	**backup delay** *enable-delay* [*disable-delay* | **never**] **Example:** `Router(config-if-cem-xconn)# backup delay30 never`	Specifies the delay before the router switches pseudowire traffic to the backup peer VC. Where: • *enable-delay* —Time before the backup PW takes over for the primary PW. • *disable-delay* —Time before the restored primary PW takes over for the backup PW. • **never**—Disables switching from the backup PW to the primary PW.

Configuring Structure-Agnostic TDM over Packet

Complete the following steps to configure Structure-Agnostic TDM over Packet (SAToP) on the Cisco ASR 901:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**controller {t1|e1}** *slot/port* **Example:** `Router(config)# controller t1 0/4`	Configures the T1 or E1 interface.
Step 4	**cem-group** *group-number* **unframed** **Example:** `Router(config-if)# cem-group 4 unframed`	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the **unframed** parameter to assign all the T1 timeslots to the CEM channel.
Step 5	**interface cem** *slot/port* **Example:** `Router(config)# interface cem 0/4`	Configures the pseudowire interface to use for the new pseudowire class.
Step 6	**no ip address** **Example:** `Router(config)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 7	**cem** *group-number* **Example:** `Router(config-if)# cem 4`	Defines a CEM group.
Step 8	**xconnect** *ip-address* **encapsulation mpls** **Example:** `Router(config-if-cem)# xconnect 30.30.30.2 304 encapsulation mpls`	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.
Step 9	**exit** **Example:** `Router(cfg-if-cem-xconn)# exit`	Exits configuration mode.

What to do next

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 30.30.30.2 255.255.255.255 1.2.3.4.**

Configuring a SAToP Pseudowire with UDP Encapsulation

Complete the following steps to configure a SAToP pseudowire with UDP encapsulation:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *pseudowire-class-name* **Example:** `Router(config)# pseudowire-class udpClass`	Creates a new pseudowire class.
Step 4	**encapsulation udp** **Example:** `Router(config-pw-class)# encapsulation udp`	Specifies the UDP transport protocol.
Step 5	**ip local interface loopback** *interface-number* **Example:** `Router(config-pw-class)# ip local interface Loopback 1`	Configures the IP address of the provider edge (PE) router interface as the source IP address for sending tunneled packets.
Step 6	**ip tos value** *value-number* **Example:** `Router(config-pw-class)# ip tos value 100`	Specifies the type of service (ToS) level for IP traffic in the pseudowire.
Step 7	**ip ttl** *number* **Example:** `Router(config-pw-class)# ip ttl 100`	Specifies a value for the time-to-live (TTL) byte in the IP headers of Layer 2 tunneled packets.
Step 8	**controller** {**e1** | **t1**} *slot/port* **Example:**	Enters E1/T1 controller configuration mode.

	Command or Action	Purpose
	`Router(config)# controller [e1|t1] 0/0`	
Step 9	**cem-group** *group-number* **unframed** **Example:** `Router(config-controller)# cem-group 4 unframed`	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the unframed parameter to assign all the T1 timeslots to the CEM channel.
Step 10	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration.
Step 11	**interface cem** *slot/port* **Example:** `Router(config)# interface CEM0/4`	Selects the CEM interface where the CEM circuit (group) is located (where slot/subslot is the SPA slot and subslot and port is the SPA port where the interface exists).
Step 12	**no ip address** **Example:** `Router(config)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 13	**cem** *group-number* **Example:** `Router(config-if)# cem 4`	Defines a CEM channel.
Step 14	**xconnect peer-router-id vcid** {*pseudowire-class name*} **Example:** `Router(config-if-cem)# xconnect 30.30.30.2 305 pw-class udpClass`	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 30.30.30.2. **Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the cross-connect address (LDP router-ID or loopback address) to the next hop IP address, such as **ip route 30.30.30.2 255.255.255.255 1.2.3.4**.
Step 15	**udp port local** {*local-udp-port*} **remote** {*remote-udp-port*} **Example:** `Router(config-if-cem-xconn)# udp port local 49150 remote 55000`	Specifies a local and remote UDP port for the connection. Valid port values for SAToP pseudowires using UDP are from 49152–57343.

	Command or Action	Purpose
Step 16	**exit** **Example:** `Router(config-if-cem-xconn)# exit`	Exits the CEM interface.
Step 17	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode.

Configuring Circuit Emulation Service over Packet-Switched Network

Complete the following steps to configure Circuit Emulation Service over Packet-Switched Network (CESoPSN):

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller** {**e1** | **t1**} *slot/port* **Example:** `Router(config)# controller [e1 | t1] 0/0`	Enters configuration mode for an E1 or T1 controller.
Step 4	**cem-group 5 timeslots** *timeslot* **Example:** `Router(config-controller)# cem-group 5 timeslots 1-24`	Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel and specific timeslots to the CEM channel. • *timeslot*—The timeslot value for T1 interface is between 1 to 24 and for E1 interface, its between 1 to 31.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration.

	Command or Action	Purpose
Step 6	**interface** *CEM slot/port* **Example:** `Router(config)# interface CEM0/5`	Defines a CEM channel.
Step 7	**cem** *group-number* **Example:** `Router(config-if-cem)# cem 5`	Defines a CEM channel.
Step 8	**xconnect** *ip-address* **encapsulation mpls** **Example:** `Router(config-if-cem)# xconnect 30.30.30.2 305 encapsulation mpls`	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 30.30.30.2. **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 30.30.30.2 255.255.255.255 1.2.3.4.**
Step 9	**exit** **Example:** `Router(config-if-cem-xconn)# exit`	Exits the CEM interface.
Step 10	**end** **Example:** `Router(config-if-cem)# end`	Exits configuration mode.

Configuring a CESoPSN Pseudowire with UDP Encapsulation

Complete the following steps to configure a CESoPSN pseudowire with UDP encapsulation:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**pseudowire-class** *pseudowire-class-name* **Example:** `Router(config)# pseudowire-class udpClass`	Creates a new pseudowire class.
Step 4	**encapsulation udp** **Example:** `Router(config-pw-class)# encapsulation udp`	Specifies the UDP transport protocol.
Step 5	**ip local interface loopback** *interface-number* **Example:** `Router(config-pw-class)# ip local interface loopback1`	Configures the IP address of the provider edge (PE) router interface as the source IP address for sending tunneled packets.
Step 6	**ip tos value** *value-number* **Example:** `Router(config-pw-class)# ip tos value 100`	Specifies the type of service (ToS) level for IP traffic in the pseudowire.
Step 7	**ip ttl** *number* **Example:** `Router(config-pw-class)# ip ttl 100`	Specifies a value for the time-to-live (TTL) byte in the IP headers of Layer 2 tunneled packets.
Step 8	**exit** **Example:** `Router(config-pw-class)# exit`	Exits pseudowire-class configuration mode.
Step 9	**controller** {**e1** | **t1**} *slot/port* **Example:** `Router(config)# controller e1 0/0`	Enters E1/T1 controller configuration mode.
Step 10	**cem-group number timeslots** *number* **Example:** `Router(config-controller)#` **`cem-group 5 timeslots 1-24`**	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the unframed parameter to assign all the T1 timeslots to the CEM channel.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration.
Step 12	**interface cem** *slot/port* **Example:** `Router(config)# interface cem 0/5`	Selects the CEM interface where the CEM circuit (group) is located (where slot/subslot is the SPA slot and subslot and port is the SPA port where the interface exists).
Step 13	**no ip address** **Example:** `Router(config)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 14	**cem** *group-number* **Example:** `Router(config-if)# cem 5`	Defines a CEM channel.
Step 15	**xconnect peer-router-id vcid** {**pseudowire-class** *name*} **Example:** `Router(config-if-cem)# xconnect 30.30.30.2 305 pw-class udpClass`	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 30.30.30.2. **Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the cross-connect address (LDP router-ID or loopback address) to the next hop IP address, such as **ip route 30.30.30.2 255.255.255.255 1.2.3.4**.
Step 16	**udp port local** *local_udp_port* **remote** *remote_udp_port* **Example:** `Router(config-if-cem-xconn)# udp port local 49150 remote 55000`	Specifies a local and remote UDP port for the connection. Valid port values for CESoPSN pseudowires using UDP are from 49152–57343.
Step 17	**end** **Example:** `Router(config-if-cem)# end`	Exits the configuration mode.

QoS for CESoPSN over UDP and SAToP over UDP

Cisco ASR 901 router supports IP DSCP and IP Precedence via service-policy and Type of Service (ToS) setting in pseudowire-class.

The ToS setting in pseudowire-class is optional. If a quality of service (QoS) policy with DSCP and IP Precedence value is applied on the cem circuit that has a ToS setting (via pseudowire-class), then the DSCP IP Precedence setting at the service policy is applied. Hence, the service-policy overrides the Qos configuration that is set through the pseudowire-class.

Example

```
Router(config)#pseudowire-class pw-udp
Router(config-pw-class)#ip tos value tos-value
Router(config)#policy-map policy-Qos
Router(config-pmap)#class class-default
Router(config-pmap-c)#set ip precedence precedence-value
Router(config-pmap-c)#set ip dscp dscp-value
Router(config-pmap-c)#set qos-group qos-group-value
Router(config)#interface cem 0/0
Router(config-if)#cem 0
Router(config-if-cem)#service-policy input policy-Qos
Router(config-if-cem)#xconnect 180.0.0.201 29 pw-class pw-udp
Router(cfg-if-cem-xconn)#udp port local 49152 remote 49152
```

The **set qos-group** command is used to set the mpls experimental bit for the vc label, if no action on egress is copied to the outer mpls label experimental bit.

For details on configuring QoS in Cisco ASR 901, see Configuring QoS, on page 385.

Configuring Transportation of Service Using Ethernet over MPLS

Ethernet over MPLS PWs allow you to transport Ethernet traffic over an existing MPLS network. For an overview of Ethernet over MPLS pseudowires, see Transportation of Service Using Ethernet over MPLS, on page 268.

Complete the following steps to configure an Ethernet over MPLS pseudowire:

Procedure

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

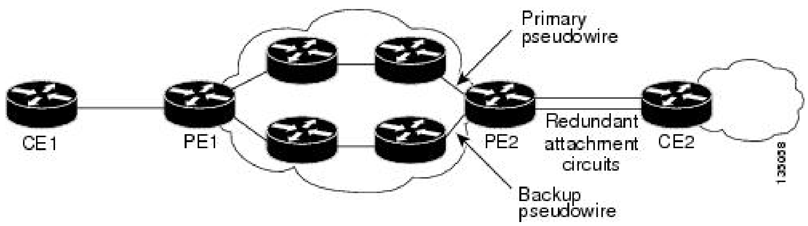
	Command or Action	Purpose
Step 3	**interface GigabitEthernetslot/port** **Example:** `Router(config)# interface GigabitEthernet0/2`	Specifies an interface to configure.
Step 4	**service instance instance-number ethernet** **Example:** `Router(config-if)# service instance 101 ethernet`	Configures a service instance and enters the service instance configuration mode.
Step 5	**encapsulation dot1q encapsulation-type** **Example:** `Router(config-if-srv)# encapsulation dot1q 101`	Configures encapsulation type for the service instance.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation modification to occur on packets at ingress as follows: • **pop 1**—Pop (remove) the outermost tag. • **symmetric—**Configure the packet to undergo the reverse of the ingress action at egress. If a tag is popped at ingress, it is pushed (added) at egress. **Note** Although the **symmetric** keyword appears to be optional, you must enter it for **rewrite** to function correctly.
Step 7	**xconnect ip-address encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 11.205.1.1 141 encapsulation mpls`	Binds the VLAN attachment circuit to an Any Transport over MPLS (AToM) pseudowire for EoMPLS.
Step 8	**end** **Example:** `Router(config-if-srv)# end`	Returns to privileged EXEC mode.

Configuring L2VPN Pseudowire Redundancy

The Cisco Cisco ASR 901 router supports the L2VPN pseudowire redundancy feature that provides backup service for circuit emulation (CEM) pseudowires. This feature enables the network to detect a failure, and reroute the Layer 2 (L2) service to another endpoint that can continue to provide the service. This feature also provides the ability to recover from a failure: either the failure of the remote PE router, or of the link between the PE and the CE routers.

Configure pseudowire redundancy by configuring two pseudowires for the CEM interface: a primary pseudowire and a backup (standby) pseudowire. If the primary pseudowire goes down, the router uses the backup pseudowire in its place. When the primary pseudowire comes back up, the backup pseudowire is brought down and the router resumes using the primary.

The following figure shows an example of pseudowire redundancy.



Note You must configure the backup pseudowire to connect to a different router than the primary pseudowire.

Complete the following steps to configure pseudowire redundancy on a CEM interface.

Procedure

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

	Command or Action	Purpose
Step 4	**cem-group** *group-number* **{unframed | timeslots}** *timeslot* **Example:** `Router(config-controller)# cem-group 5 timeslots 30`	Creates a CEM interface and assigns it a CEM group number.
Step 5	**framing {sf | esf}** **Example:** `Router(config-controller)# framing esf`	Selects the T1 framing type.
Step 6	exit **Example:** `Router(config-controller)# exit`	Exits the controller configuration mode.
Step 7	**interface cem** *slot/port* **Example:** `Router(config)# interface cem 0/0`	Configures the pseudowire interface to use for the new pseudowire class.
Step 8	**cem** *group-number* **Example:** `Router(config-if)# cem 0`	Configures the pseudowire interface to use for the new pseudowire class.
Step 9	**xconnect** *peer-router-id vcid* **{encapsulation mpls | pw-class** *pw-class-name***}** **Example:** `Router(config-if)# xconnect 10.10.10.11 344 encapsulation mpls`	Configures a pseudowire to transport TDM data from the CEM circuit across the MPLS network. • *peer-router-id* is the IP address of the remote PE peer router. • *vcid* is a 32-bit identifier to assign to the pseudowire. The same vcid must be used for both ends of the pseudowire. • **encapsulation mpls** sets MPLS for tunneling mode. • *pw-class-name* specifies a pseudowire class that includes the encapsulation mpls command. **Note** The peer-router-id and vcid combination must be unique on the router.
Step 10	**backup peer** *peer-router-ip-address vcid* **[pw-class** *pw-class-name***]** **Example:**	Specifies a redundant peer for the pseudowire VC.

	Command or Action	Purpose
	`Router(config-if-xcon)# backup peer 10.10.10.11 344 pw-class pwclass1`	The pseudowire class name must match the name specified when you created the pseudowire class, but you can use a different pw-class in the backup peer command than the name used in the primary xconnect command.
Step 11	**backup delay** *enable-delay* **{***disable-delay* **| never}** **Example:** `Router(config-if-xcon)# backup delay 30 60`	• enable delay—Specifies how long (in seconds) the backup pseudowire VC should wait to take over, after the primary pseudowire VC goes down. The range is 0 to 180. • disable delay—Specifies how long the primary pseudowire should wait, after it becomes active to take over for the backup pseudowire VC. The range is 0 to 180 seconds. If you specify the never keyword, the primary pseudowire VC never takes over for the backup.

Example: Pseudowire Redundancy

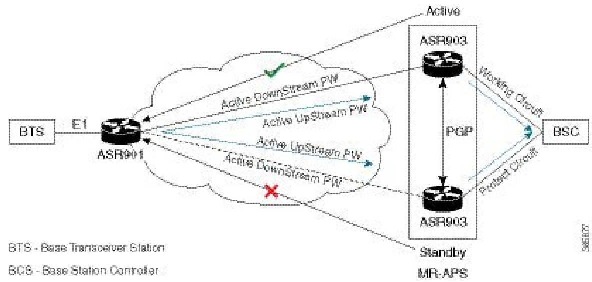
This example shows pseudowire redundancy configured for a CEM circuit (group). In the example, the xconnect command configures a primary pseudowire for CEM group 0. The backup peer command creates a redundant pseudowire for the group.

```
int cem 0/1
no ip address
cem 0
xconnect 10.10.10.1 1 encap mpls
backup peer 10.10.10.2 200
exit
```

Pseudowire Redundancy with Uni-directional Active-Active

Pseudowire redundancy active-active feature supports replication of packets from the upstream and to send the packets to both the primary and backup pseuduowires. The peer routers forward the packets received to the working and protect circuits. The BSC receives the same packets on any of the circuits and changes the Rx link, thus ensuring the packet is not dropped.

Figure 16: Pseudowire Redundancy with Unidirectional Active-Active



Restrictions

- Provides support of maximum number of 8 E1 circuits with enabled MR-APS feature.
- Supports only SAToP or CESoSPN. This feature does not support UDP encapsulation like SAToUDP or CESoUDP.

Configuring Pseudowire Redundancy Active-Active at Interface

```
enable
configure terminal
pseudowire-class mraps
encapsulation mpls
exit
interface cem 0/0
cem 0
xconnect 10.10.10.11 3 encapsulation mpls pw-class mraps
backup peer 10.10.10.12 3 pw-class mraps
redundancy all-active replicate
exit
```

Verifying the Pseudowire Redundancy Active-Active Configuration

You can use the following commands to verify your pseudowire redundancy active-active configuration:

- **show xconnect all** - Displays the information about xconnect attachment circuits and pseudowires (PWs).

```
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 CE0/0:0(SATOP E1)            UP mpls 10.10.10.11:3            UP
UP sec   ac CE0/0:0(SATOP E1)            UP mpls 10.10.10.12:3            UP
```

- **show mpls l2transport vc** *3 detail*- Displays the information about Any Transport over MPLS (AToM) virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router.

```
Router#  show mpls l2transport vc 3 detail

Local interface: CE0/0 up, line protocol up, SATOP E1 0 up
  Destination address: 10.10.10.11, VC ID: 3, VC status: up
    Output interface: Vl1509, imposed label stack {21 52}
    Preferred path: not configured
    Default path: active
    Next hop: 150.9.1.2
  Create time: 1d21h, last status change time: 00:04:06
    Last label FSM state change time: 00:04:06
  Signaling protocol: LDP, peer 10.10.10.11:0 up
    Targeted Hello: 10.10.10.13(LDP Id) -> 10.10.10.11, LDP is UP
    Graceful restart: configured and enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 62, remote 52
    Group ID: local 35, remote 27
    MTU: local 0, remote 0
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 21016/45208 (used), PWID: 2
  VC statistics:
    transit packet totals: receive 41364, send 41364
    transit byte totals:   receive 10589184, send 10589184
    transit packet drops:  receive 0, seq error 0, send 0

Local interface: CE0/0 up, line protocol up, SATOP E1 0 up
  Destination address: 10.10.10.12, VC ID: 3, VC status: up
    Output interface: Vl1510, imposed label stack {35 18}
    Preferred path: not configured
    Default path: active
    Next hop: 150.10.1.2
  Create time: 1d21h, last status change time: 00:00:56
    Last label FSM state change time: 00:00:56
  Signaling protocol: LDP, peer 10.10.10.12:0 up
    Targeted Hello: 10.10.10.13(LDP Id) -> 10.10.10.12, LDP is UP
    Graceful restart: configured and enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
```

```
   MPLS VC labels: local 63, remote 18
    Group ID: local 35, remote 27
    MTU: local 0, remote 0
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 78374/4263 (used), PWID: 3
  VC statistics:
    transit packet totals: receive 0, send 41365
    transit byte totals:   receive 0, send 10589440
    transit packet drops:  receive 0, seq error 0, send 0
```

- **show ssm id**— Displays the Segment Switching Manager (SSM) information.

```
Router# show ssm id

SSM Status: 3 switches
  Switch-ID 4263 State: Open
    Segment-ID: 78374 Type: AToM[17]
      Switch-ID:                    4263
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
    Class:                        SSS
      State:                        Ready
    Class:                        ADJ
      State:                        Active

    Segment-ID: 123381 Type: E1 SATOP[26]
      Switch-ID:                    4263
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
      Circuit status:               UP      [1]
      All active:                   Replicate packets
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
     adjacency = 0x12A6DD80 [complete] RAW CEM0/0:0
      AC Encap [0 bytes]
      1stMem: 123381 2ndMem: 53792 ActMem: 123381

  Switch-ID 45208 State: Open
    Segment-ID: 53792 Type: E1 SATOP[26]
      Switch-ID:                    45208
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
      Circuit status:               UP      [1]
      All active:                   Replicate packets
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
      adjacency = 0x12A6DD80 [complete] RAW CEM0/0:0
      AC Encap [0 bytes]
      1stMem: 123381 2ndMem: 53792 ActMem: 123381

    Segment-ID: 21016 Type: AToM[17]
      Switch-ID:                    45208
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
    Class:                        SSS
      State:                        Ready
    Class:                        ADJ
      State:                        Active
```

Configuring Hot Standby Pseudowire Support for ATM/IMA

This section describes how to configure ATM/IMA pseudowire redundancy:

Note Both the primary and backup pseudowires must be provisioned for the Hot Standby Pseudowire Support feature to work.

Configuring ATM/IMA Pseudowire Redundancy in PVC Mode

Complete the following steps to configure pseudowire redundancy in permanent virtual circuit (PVC) mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface ATM0/IMA1`	Selects the interface. • *interface-name*— Name of the interface
Step 4	**pvc** *vpi/vci* **l2transport** **Example:** `Router(config-if)# pvc 90/90 l2transport`	Create or assigns a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC. • *vpi*— ATM network virtual path identifier (VPI) for this PVC. • *vci*— ATM network virtual channel identifier (VCI) for this PVC.
Step 5	**encapsulation** {**aal0** | **aal5**} **Example:** `Router(config-if)# encapsulation aal0`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM virtual circuit (VC), VC class , VC, bundle, or permanent virtual circuit (PVC) range.
Step 6	**xconnect** *peer-ip-address vc-id encapsulation* **mpls**	Binds an attachment circuit to a pseudowire.

	Command or Action	Purpose
	Example: `Router(config-if-srv)# xconnect 192.168.1.12 100 encapsulation mpls`	• *peer-ip-address*— IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vcid*— 32-bit identifier of the VC between the routers at each end of the layer control channel. • *encapsulation*— Specifies the tunneling method to encapsulate the data in the pseudowire.
Step 7	**backup peer** *peer-router-ip-addr vcid* **Example:** `Router(config-if-xconn)# backup peer 170.0.0.201 200`	Specifies a redundant peer for a pseudowire virtual circuit (VC). • *peer-router-id*— IP address of the remote peer router. • *vcid*— 32-bit identifier of the VC between the routers at each end of the layer control channel.

Configuring ATM/IMA Pseudowire Redundancy in PVP Mode

Complete the following steps to configure pseudowire redundancy in permanent virtual path (PVP) mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface ATM0/IMA1`	Selects the interface. • *interface-name*— Name of the interface.
Step 4	**atm pvp** *vpi l2transport* **Example:** `Router(config-if)# atm pvp 90 l2transport`	Creates a permanent virtual path (PVP) used to multiplex (or bundle) one or more virtual circuits (VCs).

	Command or Action	Purpose
		• *vpi*— ATM network virtual path identifier (VPI) of the VC to multiplex on the permanent virtual path. • *l2transport*— Specifies that the PVP is for the Any Transport over MPLS (AToM) ATM cell relay feature or the ATM Cell Relay over L2TPv3 feature.
Step 5	**xconnect** *peer-ip-address vc-id encapsulation* **mpls** **Example:** `Router(config-if)# xconnect 192.168.1.12 100 encapsulation mpls`	Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vcid*—32-bit identifier of the VC between the routers at each end of the layer control channel. • *encapsulation*—Specifies the tunneling method to encapsulate the data in the pseudowire.
Step 6	**backup peer** *peer-router-ip-addr vcid* **Example:** `Router(config-if-xconn)# backup peer 170.0.0.201 200`	Specifies a redundant peer for a pseudowire virtual circuit (VC). • *peer-router-id*—IP address of the remote peer router. • *vcid*—32-bit identifier of the VC between the routers at each end of the layer control channel.

Configuring ATM/IMA Pseudowire Redundancy in Port Mode

Complete the following steps to configure pseudowire redundancy in port mode.

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface ATM0/IMA1`	Selects the interface. • *interface-name*— Name of the interface
Step 4	**xconnect** *peer-ip-address vc-id encapsulation* **mpls** **Example:** `Router(config-if)# xconnect 192.168.1.12 100 encapsulation mpls`	Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire. • *peer-ip-address*— IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vcid*— 32-bit identifier of the VC between the routers at each end of the layer control channel. • *encapsulation*— Specifies the tunneling method to encapsulate the data in the pseudowire.
Step 5	**backup peer** *peer-router-ip-addr vcid* **Example:** `Router(config-if-xconn)# backup peer 170.0.0.201 200`	Specifies a redundant peer for a pseudowire virtual circuit (VC). • *peer-router-ip-addr*— IP address of the remote peer router. • *vcid*— 32-bit identifier of the VC between the routers at each end of the layer control channel.

Verifying Hot Standby Pseudowire Support for ATM/IMA

To verify the configuration of Hot Standby Pseudowire Support for ATM/IMA, use the **show** commands as shown in the following examples.

```
Router# show mpls l2transport vc 90
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/IMA1       ATM VPC CELL 90            2.2.2.2         90         STANDBY
AT0/IMA1       ATM VPC CELL 90            180.0.0.201     90         UP
Router# show mpls l2transport vc detail
ASR901-PE2#sh mpls l2 vc 90 deta
Local interface: AT0/IMA1 up, line protocol up, ATM VPC CELL 90 up
  Destination address: 2.2.2.2, VC ID: 90, VC status: standby
    Output interface: Vl500, imposed label stack {22 17}
    Preferred path: not configured
    Default path: active
    Next hop: 150.1.1.201
  Create time: 5d02h, last status change time: 2d17h
    Last label FSM state change time: 5d02h
  Signaling protocol: LDP, peer 2.2.2.2:0 up
    Targeted Hello: 170.0.0.201(LDP Id) -> 2.2.2.2, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
```

```
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LrdRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: DOWN(standby)
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: DOWN(standby)
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 17, remote 17
    Group ID: local 0, remote 0
    MTU: local n/a, remote n/a
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 28683/16387 (used), PWID: 4
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
Local interface: AT0/IMA1 up, line protocol up, ATM VPC CELL 90 up
  Destination address: 180.0.0.201, VC ID: 90, VC status: up
    Output interface: Vl300, imposed label stack {21}
    Preferred path: not configured
    Default path: active
    Next hop: 110.1.1.202
  Create time: 5d02h, last status change time: 2d17h
    Last label FSM state change time: 2d17h
  Signaling protocol: LDP, peer 180.0.0.201:0 up
    Targeted Hello: 170.0.0.201(LDP Id) -> 180.0.0.201, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 16, remote 21
    Group ID: local 0, remote 0
    MTU: local n/a, remote n/a
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 4110/12290 (used), PWID: 3
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
    packet drops:  receive 0, send 0
```

TDM Local Switching

Time Division Multiplexing (TDM) Local Switching allows switching of layer 2 data between two CEM interfaces on the same router.

Note Effective with 15.2(2)SNH1 release, you can configure local switching on the T1 or E1 mode.

Restrictions

- Auto-provisioning is not supported.
- Out-of-band signaling is not supported.
- Redundancy is not supported.
- Interworking with other interface types other than CEM is not supported.
- The same CEM circuit cannot be used for both local switching and cross-connect.
- You cannot use CEM local switching between two CEM circuits on the same CEM interface.
- Local switching is not supported in unframed mode.
- Local switching with channelized CEM interface is not supported.
- Modifications to payload size, dejitter buffer, idle pattern, and service policy CEM interface parameters are not supported.

Configuring TDM Local Switching on a T1/E1 Mode

To configure local switching on a T1 or E1 mode, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name slot/port* **Example:** `Router(config)# interface cem0/3`	Selects the CEM interface to configure the pseudowire.

	Command or Action	Purpose
Step 4	**connect** *connection-name interface-name slot/portinterface-name slot/port* **Example:** `Router(config)# connect myconn CEM0/0 0 CEM0/1 0`	Configures a local switching connection between the first and the second CEM interfaces. The no form of this command unconfigures the connection.

Verifying Local Switching

To verify local switching on a T1/E1 mode, use the show connection, show connection all, show connection id or show connection name command.

```
Router# show connection
ID   Name            Segment 1                            Segment 2                State

======================================================================================


1      myconn          CE0/0 CESP 0           CE0/1 CESP 0
  UP
Router# show connection all
ID     Name                 Segment 1                      Segment 2
  State

======================================================================================


1      myconn               CE0/0 CESP 0                   CE0/1 CESP 0
   UP
2    myconn 1     CE0/1 CESP 1        CE0/0 CESP 1         UP
Router# show connection name myconn
Connection: 1 - myconn
Current State: UP
 Segment 1: CEM0/0 CESoPSN Basic 0 up
 Segment 2: CEM0/1 CESoPSN Basic 0 up
Router# show connection id 1
Connection: 1 - myconn
 Current State: UP
 Segment 1: CEM0/0 CESoPSN Basic 0 up
 Segment 2: CEM0/1 CESoPSN Basic 0 up
```

Configuration Example for Local Switching

The following is a sample configuration of local switching:

```
!
controller T1 0/0
 cem-group 0 timeslots 1-24
!
controller T1 0/1
 cem-group 0 timeslots 1-24
!
!
interface CEM0/0
```

```
 no ip address
 cem 0
 !
!
interface CEM0/1
 no ip address
 cem 0
 !
!
connect myconn CEM0/0 0 CEM0/1 0
 !
```

Configuration Examples of Hot Standby Pseudowire Support for ATM/IMA

This section provides sample configuration examples of Hot Standby Pseudowire Support for ATM/IMA on the Cisco ASR 901 router:

Example: Configuring ATM/IMA Pseudowire Redundancy in PVC Mode

The following is a sample configuration of ATM/IMA pseudowire redundancy in PVC mode.

```
!
interface ATM0/IMA1
pvc 90/90 l2transport
encapsulation aal0
xconnect 192.168.1.12 100 encapsulation mpls
backup peer 170.0.0.201 200
!
```

Example: Configuring ATM/IMA Pseudowire Redundancy in PVP Mode

The following is a sample configuration of ATM/IMA pseudowire redundancy in PVP mode.

```
!
 interface ATM0/IMA1
 atm pvp 90 l2transport
xconnect 192.168.1.12 100 encapsulation mpls
   backup peer 170.0.0.201 200
 !
```

Example: Configuring ATM/IMA Pseudowire Redundancy in Port Mode

The following is a sample configuration of ATM/IMA pseudowire redundancy in port mode.

```
!
 interface ATM0/IMA1
 xconnect 192.168.1.12 100 encapsulation mpls
       backup peer 170.0.0.201 200
 !
```

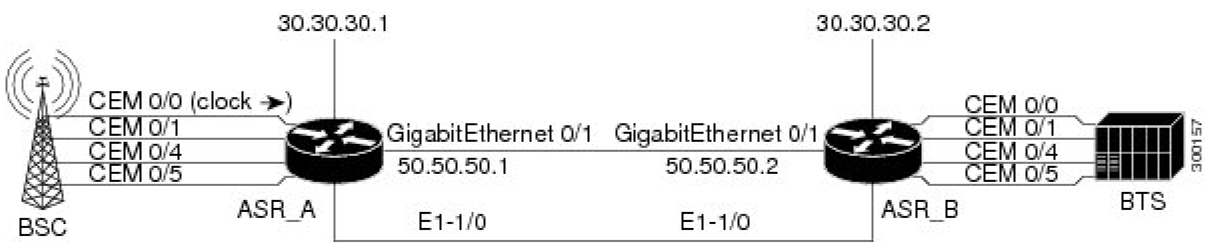
Configuration Examples for Pseudowire

This section contains the following examples:

Example: TDM over MPLS Configuration-Example

Figure 17: TDM over MPLS Configuration, on page 297 shows a TDM over MPLS configuration. The configuration uses CESoPSN for E1.

Figure 17: TDM over MPLS Configuration



ASR_A

```
!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname asr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
enable password xxx
!
no aaa new-model
clock timezone est -5
!
ip cef
!
controller E1 0/0
clock source internal
cem-group 0 timeslots 1-31
description E1 CESoPSN example
!
controller E1 0/1
clock source internal
cem-group 1 unframed
description E1 SATOP example
!
controller E1 0/4
clock source internal
cem-group 4 unframed
description E1 SATOP example
!
controller E1 0/5
```

```
clock source internal
cem-group 5 timeslots 1-24
description E1 CESoPSN example
!
interface Loopback0
ip address 30.30.30.1 255.255.255.255
!
interface GigabitEthernet0/1
no negotiation auto
service instance 2 ethernet
encapsulation untagged
bridge-domain 100
!
!
interface CEM0/0
no ip address
cem 0
xconnect 30.30.30.2 300 encapsulation mpls
!
!
interface CEM0/1
no ip address
cem 1
xconnect 30.30.30.2 301 encapsulation mpls
!
!
interface CEM0/4
no ip address
cem 4
xconnect 30.30.30.2 304 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 5
xconnect 30.30.30.2 305 encapsulation mpls
!
!
interface Vlan100
ip address 50.50.50.1 255.255.255.0
mpls ip
!
router ospf 1
network 50.50.50.0 0.0.0.255 area 0
network 30.30.30.1 0.0.0.0 area 0
!
no ip http server
no ip http secure-server
!
line con 0
password xxx
login
line aux 0
password xxx
login
no exec
line vty 0 4
password xxx
login
!
network-clock input-source 1 external 0/0/0  e1 crc4
end
```

ASR_B

```
!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname asr_B
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
enable password xxx
!
no aaa new-model
clock timezone est -5
!
ip cef
!
controller E1 0/0
clock source internal
cem-group 0 timeslots 1-31
description E1 CESoPSN example
!
controller E1 0/1
clock source internal
cem-group 1 unframed
description E1 SATOP example
!
controller E1 0/4
clock source internal
cem-group 4 unframed
description T1 SATOP example
!
controller E1 0/5
clock source internal
cem-group 5 timeslots 1-24
description T1 CESoPSN example
!
interface Loopback0
ip address 30.30.30.2 255.255.255.255
!
interface GigabitEthernet0/1
no negotiation auto
service instance 2 ethernet
encapsulation untagged
bridge-domain 100
!
!
interface CEM0/0
no ip address
cem 0
xconnect 30.30.30.1 300 encapsulation mpls
!
!
interface CEM0/1
no ip address
cem 1
xconnect 30.30.30.1 301 encapsulation mpls
!
!
interface CEM0/4
no ip address
```

```
cem 4
xconnect 30.30.30.1 304 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 5
xconnect 30.30.30.1 305 encapsulation mpls
!
!
interface Vlan100
ip address 50.50.50.2 255.255.255.0
mpls ip
!
router ospf 1
network 50.50.50.0 0.0.0.255 area 0
network 30.30.30.2 0.0.0.0 area 0
!
no ip http server
no ip http secure-server
!
line con 0
password xxx
login
line aux 0
password xxx
login
no exec
line vty 0 4
password xxx
login
!
network-clock input-source 1 controller e1 0/0
end
```

Example: CESoPSN with UDP

The following configuration uses CESoSPN with UDP encapsulation.

Note This section provides a partial configuration intended to demonstrate a specific feature.

```
interface Loopback0
ip address 2.2.2.8 255.255.255.255
!
pseudowire-class udpClass
encapsulation udp
protocol none
ip local interface Loopback 0
!
controller E1 0/13
clock source internal
cem-group 0 timeslots 1-31
!
interface cem 0/13
cem 0
xconnect 2.2.2.9 200 pw-class udpClass
udp port local 50000 remote 55000
```

Example: Ethernet over MPLS

The following configuration example shows an Ethernet pseudowire (aka EoMPLS) configuration.

```
interface Loopback0
 description for_mpls_ldp
 ip address 99.99.99.99 255.255.255.255
!
interface GigabitEthernet0/10
 description Core_facing
 no negotiation auto
 service instance 150 ethernet
  encapsulation dot1q 150
  rewrite ingress tag pop 1 symmetric
  bridge-domain 150
!
interface GigabitEthernet0/11
 description Core_facing
 service instance 501 ethernet
  encapsulation dot1q 501
  rewrite ingress tag pop 1 symmetric
  xconnect 111.0.1.1 501 encapsulation mpls
!
interface FastEthernet0/0
 ip address 10.104.99.74 255.255.255.0
 full-duplex
!
interface Vlan1
!
interface Vlan150
 ip address 150.0.0.1 255.255.255.0
 mpls ip
!
router ospf 7
 network 99.99.99.99 0.0.0.0 area 0
 network 150.0.0.0 0.0.0.255 area 0
!
no ip http server
ip route 10.0.0.0 255.0.0.0 10.104.99.1
!
logging esm config
!
mpls ldp router-id Loopback0 force
!
!end
```

CHAPTER 21

Configuring Clocking

This chapter provides information about configuring clocking on the Cisco ASR 901 Series Aggregation Services Router.

Configuring Clocking

This chapter provides information about configuring clocking on the Cisco ASR 901 Series Aggregation Services Router.

Restrictions

- External interfaces like Building Integrated Timing Supply (BITS) and 1 Pulse Per Second (1PPS) have only one port. These interfaces can be used as either an input interface or output interface at a given time.
- The *line to external* option is not supported for external Synchronization Supply Unit (SSU).
- Time-of-Day (ToD) is not integrated to the router system time. ToD input or output reflects only the PTP time, not the router system time.
- Revertive and non-revertive modes work correctly only with two clock sources.
- BITS cable length option is supported via **platform timing bits line-build-out** command.
- There is no automatic recovery from out-of-resource (OOR) alarms. OOR alarms must be manually cleared using **clear platform timing oor-alarms** command.
- If copper Gigabit Ethernet port is selected as the input clock source, the link must be configured as a IEEE 802.3 link-slave, using **synce state slave** command.
- BITS reports loss of signal (LOS) only for Alarm Indication Signal (AIS), LOS, and loss of frame (LOF) alarms.
- The **clock source line** command does not support loop timing in T1/E1 controllers. However, the clock can be recovered from T1/E1 lines and used to synchronize the system clock using the **network-clock input-source** *priority* **controller** *E1/T1 0/x* command.
- Adaptive clocking is not supported in Cisco ASR 901 router.
- The **show network-clocks** command is not supported in Cisco ASR 901 Router.

- Do not use **network-clock synchronization** command while configuring 2dmm, as it is not supported. If you proceed with the unsupported configuration, it will show junk values.

Configuring Network Clock for Cisco ASR 901 Router

Cisco ASR 901 router supports time, phase and frequency awareness through ethernet networks; it also enables clock selection and translation between the various clock frequencies.

If Cisco ASR 901 interoperates with devices that do not support synchronization, synchronization features can be disabled or partially enabled to maintain backward compatibility.

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

Configuring Network Clock in Global Configuration Mode

Complete the following steps to configure the network clock in global configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock synchronization automatic** **Example:** `Router(config)# network-clock synchronization automatic`	Enables G.781-based automatic clock selection process. G.781 is the ITU-T Recommendation that specifies the synchronization layer functions.
Step 4	**network-clock eec {1 | 2 }** **Example:** `Router(config)# network-clock eec 1`	Configures the clocking system hardware with the desired parameters. These are the options: • For option 1, the default value is EEC-Option 1 (2048). • For option 2, the default value is EEC-Option 2 (1544).
Step 5	**network-clock synchronization ssm option {1 | 2 {GEN1 | GEN2 } }** **Example:**	Configures the router to work in a synchronized network mode as described in G.781. The following are the options:

	Command or Action	Purpose
	`Router(config)# network-clock synchronization ssm option 2 GEN1`	• Option 1: refers to synchronization networks designed for Europe (E1 framings are compatible with this option). • Option 2: refers to synchronization networks designed for the US (T1 framings are compatible with this option). The default option is 1 and while choosing option 2, you need to specify the second generation message (GEN2) or first generation message (GEN1). **Note** Network-clock configurations that are not common between options need to be configured again.
Step 6	**network-clock hold-off {0 | 50-10000} global** **Example:** `Router(config)# network-clock hold-off 75 global`	Configures general hold-off timer in milliseconds. The default value is 300 milliseconds. **Note** Displays a warning message for values below 300 ms and above 1800 ms.
Step 7	**network-clock external** *slot/card/port* **hold-off {0 | 50-10000}** **Example:** `Router(config)# network-clock external 3/1/1 hold-off 300`	Overrides hold-off timer value for external interface. **Note** Displays a warning message for values above 1800 ms, as waiting longer causes the clock to go into the holdover mode.
Step 8	**network-clock wait-to-restore 0-86400 global** **Example:** `Router(config)# network-clock external wait-to-restore 1000 global`	Sets the value for the wait-to-restore timer globally. The wait to restore time is configurable in the range of 0 to 86400 seconds. The default value is 300 seconds. **Caution** Ensure that you set the wait-to-restore values above 50 seconds to avoid a timing flap.
Step 9	**network-clock input-source priority** { **interface** *interface-name slot/port* | *top slot/port* | {*external slot/card/port* [**t1**{**sf**| **efs**| **d4**} | **e1** [**crc4**| **fas**| **cas**[**crc4**] | **2048k** | **10m**]}} **Example:** `Router(config)# network-clock`	Configures a clock source line interface, an external timing input interface, GPS interface, or a packet-based timing recovered clock as the input clock for the system and defines its priority. Priority is a number between 1 and 250.

	Command or Action	Purpose

	`input-source 1`
	`nterface top 0/12`
	Example:
	`Example for GPS Interface`
	`Router(config)# network-clock`
	`input-source 1`
	`external 0/0/0 10m`
		This command also configures the type of signal for an external timing input interface. These signals are:
		• T1 with Standard Frame format or Extended Standard Frame format.
		• E1 with or without CRC4
		• 2 MHz signal
		• Default for Europe or Option I is e1 crc4 if the signal type is not specified.
		• Default for North America or Option II is t1 esf if signal type is not specified.
		Note
		The no version of the command reverses the command configuration, implying that the priority has changed to undefined and the state machine is informed.

Step 10	**network-clock input-source priority controller** [**t1** | **e1**] *slot/port*
	Example:
	`Router(config)# network-clock`
	`input-source 10`
	`controller e1 0/12`
		Adds the clock recovered from the serial interfaces as one of the nominated sources, for network-clock selection.

Step 11	**network-clock revertive** **Example:** `Router(config)# network-clock revertive`	Specifies whether or not the clock source is revertive. Clock sources with the same priority are always non-revertive. The default value is non-revertive. In non-revertive switching, a switch to an alternate reference is maintained even after the original reference recovers from the failure that caused the switch. In revertive switching, the clock switches back to the original reference after that reference recovers from the failure, independent of the condition of the alternate reference.

Step 12	**network-clock output-source system priority** {*external slot/card/port* [**t1**{**sf**| **efs**| **d4**} | **e1** [**crc4**| **fas**| **cas**[**crc4**] | **2048k** | **10m**]}}
	Example:
	`Router(config)#network-clock`
	`output-source`
	`system 55 external 0/0/0 t1 efs`
		Allows transmitting the system clock to external timing output interfaces.
		This command provides station clock output as per G.781. We recommend that you use the interface level command instead of global commands. Global command should preferably be used for interfaces that do not have an interface sub mode. For more information on configuring network clock in interface level

	Command or Action	Purpose
		mode, see Configuring Network Clock in Interface Configuration Mode , on page 307.

Configuring Network Clock in Interface Configuration Mode

Complete the following steps to configure the network clock in interface configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** **Example:** `Router(config)# interface`	Enters interface configuration mode.
Step 4	**synchronous mode** **Example:** `Router(config-if)# synchronous mode`	Configures the ethernet interface to synchronous mode. **Note** This command is applicable to Synchronous Ethernet capable interfaces. The default value is asynchronous mode.
Step 5	**network-clock hold-off {0 | 50-10000}** **Example:** `Router(config-if)# network-clock hold-off 1000`	Configures hold-off timer for interface. The default value is 300 milliseconds. **Note** Displays a warning for values below 300 ms and above 1800 ms.
Step 6	**network-clock wait-to-restore** *0-86400* **Example:** `Router(config-if)#network-clock wait-to-restore 1000`	Configures the wait-to-restore timer on the SyncE interface. **Caution** Ensure that you set the wait-to-restore values above 50 seconds to avoid timing flap.

Understanding SSM and ESMC

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

Synchronization Status Message

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

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

Ethernet Synchronization Messaging Channel

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

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

Clock Selection Algorithm

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

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

QL-enabled mode

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

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

If no external commands are active, the algorithm selects the reference (for clock selection) with the highest quality level that does not experience a signal fail condition.

If multiple inputs have the same highest quality level, the input with the highest priority is selected.

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

QL-disabled mode

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

- Signal failure
- Priority
- External commands

If no external commands are active, the algorithm selects the reference (for clock selection) with the highest priority that does not experience a signal fail condition.

For multiple inputs having the same highest priority, the existing reference is maintained (if it belongs to this group), otherwise an arbitrary reference from this group is selected.

ESMC behavior for Port Channels

ESMC is an Organization Specific Slow Protocol (OSSP) like LACP of port channel, sharing the same slow protocol type, indicating it is in the same sub-layer as LACP. Hence, ESMC works on the link layer on individual physical interfaces without any knowledge of the port channel. This is achieved by setting the egress VLAN as the default VLAN (VLAN 1) and the interface as a physical interface while sending out the packets from the CPU. So none of the service instance, port channel, or VLAN rules apply to the packet passing through the switch ASIC.

ESMC behavior for STP Blocked Ports

ESMC works just above the MAC layer (below spanning tree protocol), and ignores spanning tree Port status. So, ESMC is exchanged even when the port is in the blocked state (but not disabled state). This is achieved by setting the egress VLAN as the default VLAN (VLAN 1) and the interface as a physical interface while sending out packets from the CPU. So none of the service instance, port channel, or VLAN port state, or rules apply to the packet passing through the switch ASIC.

Configuring ESMC in Global Configuration Mode

Complete the following steps to configure ESMC in global configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock synchronization mode ql-enabled** **Example:**	Configures the automatic selection process QL-enabled mode. • QL is disabled by default.

	Command or Action	Purpose
	`Router(config)# network-clock synchronization mode ql-enabled`	• **ql-enabled** mode can be used only when the synchronization interface is capable to send SSM.
Step 4	**esmc process** **Example:** `Router(config)# esmc process`	Enables the ESMC process. **Note** ESMC can be enabled globally or at the sync-E interface level
Step 5	**network-clock quality-level** {**tx** | **rx**} *value* {**interface** *interface-name slot/sub-slot/port* | **external** *slot/sub-slot/port* | **gps** *slot/sub-slot* | **controller** *slot/sub-slot/port*} **Example:** `Router(config)# network-clock quality-level rx qL-pRC external 0/0/0 e1 crc4`	Forces the QL value for line or external timing output.

Configuring ESMC in Interface Configuration Mode

Complete the following steps to configure ESMC in interface configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** **Example:** `Router(config)# interface`	Enters interface configuration mode.
Step 4	**esmc mode** {**tx** | **rx**} **Example:** `Router(config-if)# esmc mode tx`	Enables the ESMC process at the interface level. The no form of the command disables the ESMC process.

	Command or Action	Purpose

Step 5	**network-clock source quality-level** *value* {**tx** | **rx**}
	Example:
	`Router(config-if)# network-clock source`
	`quality-level <value> tx`
		Configures the QL value for ESMC on a GigabitEthernet port. The value is based on global interworking options:
		• If Option 1 is configured, the available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
		• If Option 2 is configured with GEN 2, the available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.
		• If Option 2 is configured with GEN1, the available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS

Step 6	**esmc mode ql-disabled** **Example:** `Router(config-if)# esmc mode ql-disabled`	Enables the QL-disabled mode.

What to do next

Note By disabling Rx on an interface, any ESMC packet received on the interface shall be discarded. By disabling Tx on an interface, ESMC packets will not be sent on the interface; any pending Switching Message Delay timers (TSM) are also stopped.

Verifying ESMC Configuration

Use the following commands to verify ESMC configuration:

- **show esmc**
- **show network-clock synchronization**

```
Router#show esmc interface gigabitEthernet ?
  <0-1>  GigabitEthernet interface number
Router#show esmc interface gigabitEthernet 0/10
Interface: GigabitEthernet0/10
  Administative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-SEC
    QL Transmit: QL-DNU
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
```

```
Router# show network-clocks synchronization

Symbols:      En - Enable, Dis - Disable, Adis - Admin Disable
              NA - Not Applicable
              *  - Synchronization source selected
              #  - Synchronization source force selected
              &  - Synchronization source manually switched
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Disable
ESMC : Disabled
SSM Option : 1
T0 : GigabitEthernet0/4
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No
Nominated Interfaces
 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
 To0/12               NA          NA/En        1     QL-FAILED NA        NA
 External 0/0/0       10M         NA/Dis       2     QL-FAILED NA        NA
 Gi0/1                NA          Sync/En      20    QL-FAILED -         -
*Gi0/4                NA          Sync/En      21    QL-DNU    -         -
T4 Out
 External Interface   SigType     Input         Prio  Squelch  AIS
 External 0/0/0       E1 CRC4     Internal      1     FALSE    FALSE
```

Managing Synchronization

You can manage the synchronization using the following management commands:

Command	Purpose
network-clock switch force {interface interface_name slot/port | external slot/card/port} Router(config)# network-clock switch force interface GigabitEthernet 0/1 t1	Forcefully selects a synchronization source irrespective of whether the source is available and is within the range.
network-clock switch manual {interface interface_name slot/port | external slot/card/port} `Router(config)# network-clock switch manual interface GigabitEthernet 0/1 t1`	Manually selects a synchronization source, provided the source is available and is within the range.
network-clock clear switch {t0 | external slot/card/port [10m | 2m]} `Router(config)# network-clock clear switch t0`	Clears the forced switch and manual switch commands.

Synchronization Example

Configuration for QL-disabled mode clock selection

```
network-clock synchronization automatic
```

```
network-clock input-source 1 interface ToP0/12
network-clock input-source 2 External 0/0/0 10m
network-clock input-source 20 interface GigabitEthernet0/1
network-clock input-source 21 interface GigabitEthernet0/4
network-clock output-source system 1 External 0/0/0 e1 crc4
!
interface GigabitEthernet0/1
 synchronous mode
 synce state slave
!
interface GigabitEthernet0/4
 negotiation auto
 synchronous mode
 synce state slave
end
```

GPS Configuration

```
10MHz signal
network-clock input-source 1 External 0/0/0 10m
2M signal
network-clock input-source 1 External 0/0/0 2048K
```

Configuring Synchronous Ethernet for Copper Ports

You can configure synchronization on the copper ports using the following commands:

Command	Purpose
Router(config-if)# **synce state slave**	Configures synchronous ethernet copper port as subordinate.
Router(config-if)# **synce state master**	Configures synchronous ethernet copper port as primary.

Note Synchronization on the ethernet copper port is not supported for 10 Mbps speed.

Verifying the Synchronous Ethernet configuration

Use the show network-clock synchronization command to display the sample output.

```
Router# show network-clocks synchronization

Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Disable
ESMC : Disabled
SSM Option : 1
T0 : GigabitEthernet0/4
Hold-off (global) : 300 ms
```

```
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No
Nominated Interfaces
 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
 To0/12               NA          NA/En        1     QL-FAILED NA        NA
 External 0/0/0       10M         NA/Dis       2     QL-FAILED NA        NA
 Gi0/1                NA          Sync/En      20    QL-FAILED -         -
*Gi0/4                NA          Sync/En      21    QL-DNU    -         -
T4 Out
 External Interface   SigType     Input         Prio  Squelch  AIS
 External 0/0/0       E1 CRC4     Internal      1     FALSE    FALSE
```

Use the show network-clock synchronization detail command to display all details of network-clock synchronization parameters at the global and interface levels.

```
Router# show network-clocks synchronization detail
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Disable
ESMC : Disabled
SSM Option : 1
T0 : External 0/0/0 10m
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : Yes
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 3
sm(netsync NETCLK_QL_DISABLE), running yes, state 2A
Last transition recorded: (begin)-> 2A (sf_change)-> 2A
Nominated Interfaces
Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal             NA          NA/Dis       251   QL-SEC    NA        NA
To0/12               NA          NA/En        3     QL-SEC    NA        NA
*External 0/0/0       10M         NA/Dis       1     QL-SEC    NA        NA
Gi0/11               NA          Sync/En      2     QL-DNU    -         -
T4 Out
External Interface   SigType     Input         Prio  Squelch  AIS
External 0/0/0       E1 CRC4     Internal      1     FALSE    FALSE
Interface:
---------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-disabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
```

```
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0
Local Interface: To0/12
Signal Type: NA
Mode: NA(Ql-disabled)
SSM Tx: DISABLED
SSM Rx: ENABLED
Priority: 3
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 2
SNMP parent list index: 0
Local Interface: External 0/0/0
Signal Type: 10M
Mode: NA(Ql-disabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 1
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms :  None
Slot Disabled: FALSE
SNMP input source index: 3
SNMP parent list index: 0
Local Interface: Gi0/11
Signal Type: NA
Mode: Synchronous(Ql-disabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 2
QL Receive: QL-DNU
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE  None
Slot Disabled: FALSE
SNMP input source index: 4
SNMP parent list index: 0
External 0/0/0 e1 crc4's Input:
Internal
```

```
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-disabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 1
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 1
```

Troubleshooting Tips

Note Before you troubleshoot, ensure that all the network clock synchronization configurations are complete.

The following table provides the troubleshooting scenarios encountered while configuring the synchronous ethernet.

Table 19: Troubleshooting Scenarios for Synchronous Ethernet Configuration

Problem	Solution

Clock selection	• Verify that there are no alarms on the interfaces. Use the show network-clock synchronization detail RP command to confirm.
	• Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or non-revertive mode and verify the non-revertive configurations as shown in the following example:
	
	`Router# show network-clocks synchronization`
	
	`Symbols: En - Enable, Dis - Disable, Adis - Admin Disable`
	`NA - Not Applicable`
	`* - Synchronization source selected`
	`# - Synchronization source force selected`
	`& - Synchronization source manually switched`
	`Automatic selection process : Enable`
	`Equipment Clock : 2048 (EEC-Option1)`
	`Clock Mode : QL-Disable`
	`ESMC : Disabled`
	`SSM Option : 1`
	`T0 : GigabitEthernet0/4`
	`Hold-off (global) : 300 ms`
	`Wait-to-restore (global) : 300 sec`
	`Tsm Delay : 180 ms`
	`Revertive : Yes<<<<If it is non revertive then it will show NO here.`
	
	Note
	The above example does not show the complete command output. For complete command output, see the example in Verifying the Synchronous Ethernet configuration, on page 313.
	
	Reproduce the current issue and collect the logs using the **debug network-clock errors**, **debug network-clock event**, and **debug network-clock sm RP** commands.
	
	Note
	We suggest you do not use these **debug** commands without TAC supervision. Contact Cisco technical support if the issue persists.

Incorrect quality level (QL) values when you use the **show network-clock synchronization detail** command.	Use the**network clock synchronization SSM**[option 1 | option 2] command to confirm that there is no framing mismatch. Use the **show run interface** [option 1 | option 2] command to validate the framing for a specific interface. For the SSM option 1 framing should be an E1 and for SSM option 2, it should be a T1.
Error message *%NETCLK-6-SRC_UPD: Synchronization source 10m 0/0/0 status (Critical Alarms(OOR)) is posted to all selection process* is displayed.	Interfaces with alarms or OOR cannot be the part of selection process even if it has higher quality level or priority. OOR should be cleared manually. OOR can be cleared by **clear platform timing oor-alarms** command.

Troubleshooting ESMC Configuration

Use the following debug commands to troubleshoot the PTP configuration on the Cisco ASR 901 router:

Danger We suggest you do not use these debug commands without TAC supervision.

Command	Purpose

`debug esmc error`
`debug esmc event`
`debug esmc packet [interface interface-name>]`
`debug esmc packet rx [interface interface-name]`
`debug esmc packet tx [interface interface-name]`
	Verify whether the ESMC packets are transmitted and received with proper quality-level values.

Configuring PTP for the Cisco ASR 901 Router

Effective from Cisco IOS Release 15.4 (3) S, the Cisco ASR 901 Router supports PTP over Ethernet.

Note Before configuring PTP, you should set the system time to the current time. See Setting System Time to Current Time, on page 322 section for configuration details.

This section contains the following topics:

Restrictions

- In IP mode only unicast static and unicast negotiation modes are supported. Multicast mode is not supported.
- PTP over Ethernet is supported only in multicast mode.
- PTP over Ethernet is not supported in telecom profiles.
- PTP subordinate supports both single and two-step modes. PTP primary supports only two-step mode.
- VLAN 4093 and 4094 are used for internal PTP communication; do not use VLAN 4093 and 4094 in your network.
- VLAN 4094 is used for internal PTP communication; do not use VLAN 4094 in your network.

Note Effective from Cisco IOS Release 15.4 (3) S, VLAN 4093 is not reserved for internal communication. However, every clock-port created picks a VLAN from the free pool list and reserves it internally for PTP usage only.

- Effective from Cisco IOS Release 15.5 (2)S, SVI interface is supported. With this, you can use SVI or Loopback interface in Cisco ASR 901 router instead of ToP interface for configuring 1588 interface/IP address.
- The **1pps output** command is not supported on primary ordinary clock.
- Sync and Delay request rates should be above 32 pps. The optimum value is 64 pps.
- Clock-ports start as primary even when they are configured as subordinate-only. The initial or reset state of the clock is primary. Therefore, the primary clock must have higher priority (priority1, priority2) for the subordinate to accept the primary.
- IEEEv2BMCA is supported only in unicast negotiation mode.
- IEEEv2BMCA is not supported in multicast and unicast modes.
- You should use **no transport ipv4 unicast**command to remove an existing transport configuration before changing the transport configuration from Loopback to VLAN and vice versa.
- You should use **no transport ipv4 unicast** command when there is change in the IP address of the interface on which PTP primary is configured.
- Effective from Cisco IOS Release 15.4 (3) S, VLAN id is reserved for each of the clock-port being configured. Therefore, depending on number of clock-ports, maximum of 20 VLANs can get reserved for internal purpose on Boundary Clock. For finding an internal VLAN for clock-port over PTP configuration, a free VLAN id is searched from 4093 in decreasing order. The free VLAN id remains reserved as long as the corresponding clocking-port is configured and this VLAN id cannot be used for any other purpose.

Note

- You should not use VLAN 4094 on your network as Vlan 4094 is reserved internally to process PTP management packets.
- The **1pps port** is enabled by default to receive output signal.

Precision Time Protocol

The Cisco ASR 901 Router supports the Precision Time Protocol (PTP) as defined by the IEEE 1588-2008 standard. PTP provides accurate time synchronization over packet-switched networks.

The following table provides the description of the nodes within a PTP network.

Network Element	Description
Grandmaster	A network device physically attached to the primary time source. All clocks are synchronized to the grandmaster clock.
Ordinary Clock	An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes: • Primary mode—Distributes timing information over the network to one or more subordinate clocks, thus allowing the subordinate to synchronize its clock to the primary. • Subordinate mode—Synchronizes its clock to a primary clock. You can enable the subordinate mode on up to two interfaces simultaneously in order to connect to two different primary clocks.
Boundary Clock	The device participates in selecting the best primary clock and can act as the primary clock if no better clocks are detected. Boundary clock starts its own PTP session with a number of downstream slaves. The boundary clock mitigates the number of network hops and results in packet delay variations in the packet network between the Grand Master and subordinate.
Transparent Clock	A transparent clock is a device or a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of time calculations.

IEEEV2 Best Master Clock Algorithm Overview

1588-2008 is an IEEE standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Effective from Cisco IOS Release 15.4(3)S, the Cisco ASR 901 Router supports IEEEV2 Best Master Clock Algorithm (BMCA).

Information About Best Master Clock Algorithm

BMCA is used to select the master clock on each link, and ultimately, select the grandmaster clock for the entire Precision Time Protocol (PTP) domain. BCMA runs locally on each port of the ordinary and boundary clocks, and selects the best clock on the link by comparing the local data sets with the received data from the announce messages. BMCA also runs the state decision algorithm to determine the PTP port states.

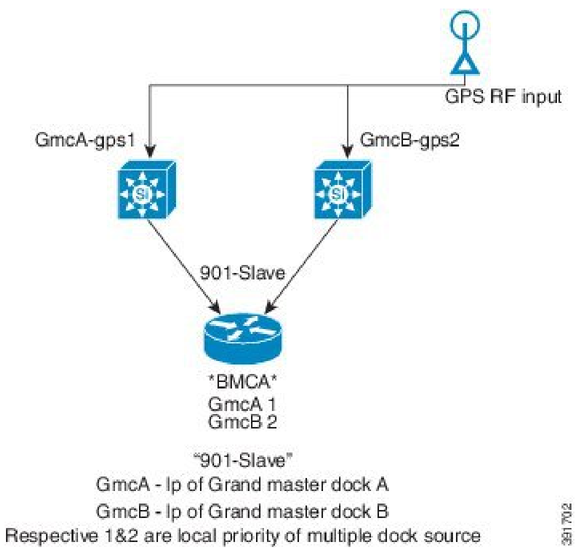
The best master clock is selected based on the following parameters:

- Priority1—User-configurable value ranging from 0 to 255; lower value takes precedence
- ClockClass—Defines the traceability of time or frequency from the grandmaster clock
- ClockAccuracy—Defines the accuracy of a clock; lower value takes precedence
- OffsetScaledLogVariance—Defines the stability of a clock
- Priority2—User-configurable value ranging from 0 to 255; lower value takes precedence
- ClockIdentity—8-byte number, typically in IEEE-EUI64 format, to uniquely identify a clock

By changing the user-configurable values, network administrators can influence the way the grandmaster clock is selected. BMCA provides the mechanism that allows all PTP clocks to dynamically select the best master clock (grandmaster) in an administration-free, fault-tolerant way, especially when the grandmaster clocks changes.

The following figure shows a sample IEEEV2 BMCA topology.

Figure 18: Sample IEEEV2 BMCA Topology



The Cisco ASR 901 Router supports IEEEv2 BMCA in following scenarios:

- IEEEv2BMCA with Slave Ordinary Clock
- IEEEv2BMCA with Hybrid Ordinary Clock
- IEEEv2BMCA with Boundary Clock
- IEEEv2BMCA with Hybrid Boundary clock

For more information on configuring the BMCA in ordinary and boundary clocks, see Configuring PTP Ordinary Clock, on page 322 and PTP Boundary Clock, on page 330.

Setting System Time to Current Time

To set the system time to the current time before configuring PTP, complete the steps given below:

Command	Purpose
Router# calendar set hh : mm : ss day month year Router# calendar set 09:00:00 6 Feb 2013	Sets the hardware clock. • hh : mm : ss—RCurrent time in hours (using 24-hour notation), minutes, and seconds. • day—Current day (by date) in the month. • month—Current month (by name). • year—Current year (no abbreviation).
Router# clock read-calendar	Synchronizes the system clock with the calendar time.
Router# show clock	Verifies the clock setting.

Configuring PTP Ordinary Clock

The following sections describe how to configure a PTP ordinary clock.

Configuring Primary Ordinary Clock

Complete the following steps to configure the a primary ordinary clock:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain* **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock as an ordinary clock and enters clock configuration mode. • *domain*—The PTP clocking domain number. The range is from 0 to 127.
Step 4	**priority1** *priority-value* **Example:** `Router(config-ptp-clk)# priority1 4`	(Optional) Sets the preference level for a clock. • *priority-value*—The range is from 0 to 255. The default is 128.

	Command or Action	Purpose
Step 5	**priority2** *priority-value* **Example:** `Router(config-ptp-clk)# priority2 8`	(Optional) Sets a secondary preference level for a clock. The priority2 value is considered only when the router is unable to use priority1 and other clock attributes to select a clock. • *priority-value*—The range is from 0 to 255. The default is 128.
Step 6	**clock-port** *port-name* **master** **Example:** `Router(config-ptp-clk)# clock-port primary master`	Sets the clock port to PTP primary and enters clock port configuration mode. In primary mode, the port exchanges timing packets with PTP subordinate devices.

Step 7	Do one of the following:
	• **transport ipv4 unicast interface** *interface-type interface-number*
	• **transport ethernet multicast bridge-domain** *bridge-id*
	Example:
	`Router(config-ptp-port)# transport ipv4`
	`unicast interface loopback 0`
		Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.
		• *interface-type*—The type of the interface.
		• *interface-number*—The number of the interface.
		Configures a bridge domain.
		• *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094.
		Note
		Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported. The option of using dynamic IP for PTP over VLAN is generally meant for a subordinate interface. Though the implementation supports dynamic IP assignment on the PTP primary, you must configure the dynamically assigned IP in **“clock source**” command on the PTP subordinate.

Step 8	**clock-destination** *clock-ip-address* **Example:** `Router(config-ptp-port)# clock-destination 8.8.8.1`	Specifies the IP address of a clock destination when the router is in PTP primary mode.
Step 9	**sync interval** *interval* **Example:** `Router(config-ptp-port)# sync interval -5`	(Optional) Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values. The Cisco ASR 901 router supports the following values: • -5—1 packet every 1/32 seconds, or 32 packets per second.

	Command or Action	Purpose
		• -6—1 packet every 1/64 seconds, or 64 packets per second. The default is -6.
Step 10	**announce interval** *interval* **Example:** `Router(config-ptp-port)# announce interval 2`	(Optional) Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second (default).
Step 11	**end** **Example:** `Router(config-ptp-port)# end`	Exits clock port configuration mode and enters privileged EXEC mode.

Configuring Subordinate Ordinary Clock

Complete the following steps to configure a subordinate ordinary clock:

Note PTP redundancy is an implementation on different clock nodes by which the PTP subordinate clock node interacts with multiple primary ports such as grand master, boundary clock nodes, and so on. A new servo mode is defined under PTP to support high PDV scenarios (when the PDVs exceed G.8261 standard profiles). You should use the servo mode high-jitter command to enable this mode on the PTP subordinate. In servo mode, convergence time would be longer than usual, as this mode is meant only for frequency synchronization.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain* **Example:**	Configures the PTP clock as an ordinary clock and enters clock configuration mode.

	Command or Action	Purpose
	`Router(config)# ptp clock ordinary domain 0`	
Step 4	**clock-port** *port-name* **slave** **Example:** `Router(config-ptp-clk)# clock-port subordinate slave`	Sets the clock port to PTP subordinate mode and enters clock port configuration mode. In subordinate mode, the port exchanges timing packets with a PTP primary clock.
Step 5	• **transport ipv4 unicast interface** *interface-type interface-number* or • **transport ethernet multicast bridge-domain** *bridge-id* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0`	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. • *interface-type*—Type of the interface, for example, loopback. • *interface-number*—Number of the interface. Values range from 0 to 2,14,74,83,647. Configures a bridge domain. • *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094. **Note** Effective with Cisco IOS Release 15.5(2)S, VLAN interface (with DHCP assigned IP or static IP) is also supported.
Step 6	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 5.5.5.5`	Specifies the address of a PTP primary clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0, the highest priority. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2. • 3—Assigns a priority value of 3. Repeat this step for each additional primary clock. You can configure up to four primary clocks. **Note** Priority is used as an index for the configured clock sources and is not a criteria for the BMCA.
Step 7	**clock source** *source-address* **Example:** `Router(config-ptp-port)# clock source 8.8.8.1`	Specifies the address of a PTP primary clock.

	Command or Action	Purpose
Step 8	**announce timeout** *value* **Example:** `Router(config-ptp-port)# announce timeout 8`	(Optional) Specifies the number of PTP announcement intervals before the session times out. • *value*—The range is from 1 to 10. The default is 3.
Step 9	**delay-req interval** *interval* **Example:** `Router(config-ptp-port)# delay-req interval 1`	(Optional) Configures the minimum interval allowed between PTP delay request messages. The intervals are set using log base 2 values, as follows: • 5—1 packet every 32 seconds • 4—1 packet every 16 seconds • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second. The default is -6.
Step 10	**sync interval** *interval* **Example:** `Router(config-ptp-port)# sync interval -5`	(Optional) Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values. The Cisco ASR 901 router supports the following values: • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. The default is -6.
Step 11	**end** **Example:**	Exits clock port configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-ptp-port)# end`	

Configuring PTP in Unicast Mode

In unicast mode, the subordinate port and the primary port need to know each other's IP address. Unicast mode has one to one mapping between the subordinate and the primary. One primary can have just one subordinate and vice-versa. Unicast mode is not a good option for scalability.

The command used for configuring Cisco ASR 901 on unicast mode is **clock-port.**

Command	Purpose
Router(config-ptp-clk)# **clock-port**	Configures Cisco ASR 901 on unicast mode. The following options can be configured with this command: • Port Name • **Port Role**

Before configuring Cisco ASR 901 on different modes, you need to configure the loopback address. The following example shows the configuration of loopback address:

Note This loopback address cannot be used for any protocol other than PTP. If a VLAN interface is used instead of loopback, the Vlan IP can be used by other protocols. It does not become dedicated to PTP.

```
Router(config)#int loopback
Router(config-if)#ip address 8.8.8.2 255.255.255.255
Router(config-if)#
no sh

Router#sh run int loopback
Building configuration...

Current configuration : 72 bytes
!
interface loopback
 ip address 8.8.8.2 255.255.255.255
 end
!
```

Note Ensure that this loopback interface is reachable (using ICMP ping) from remote locations, before assigning the interface to PTP. Once the interface is assigned to PTP, it does not respond to ICMP pings. However, If PTP is configured over VLAN, the interface responds to ICMP ping even after it is assigned to PTP.

The following example shows the configuration of Cisco ASR 901 on the unicast mode:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
```

```
Router(config-ptp-clk) clock-port SUBORDINATE slave
Router(config-ptp-port)# transport ipv4 unicast interface loopback 10
Router(config-ptp-port)# clock-source 8.8.8.1
```

Configuring PTP in Unicast Negotiation Mode

In unicast negotiation mode, primary port does not know the subordinate port at the outset. Subordinate port sends negotiation TLV when active and primary port figures out that there is some subordinate port for synchronization. Unicast negotiation mode is a good option for scalability as one primary has multiple slaves.

The command used for configuring Cisco ASR 901 router on unicast negotiation mode is **clock-port.**

Command	Purpose
Router(config-ptp-clk)# clock-port	Configures Cisco ASR 901 router on unicast negotiation mode. The following options can be configured with this command: • Port Name • **Port Role**

The following example shows the configuration of Cisco ASR 901 router on the unicast negotiation mode:

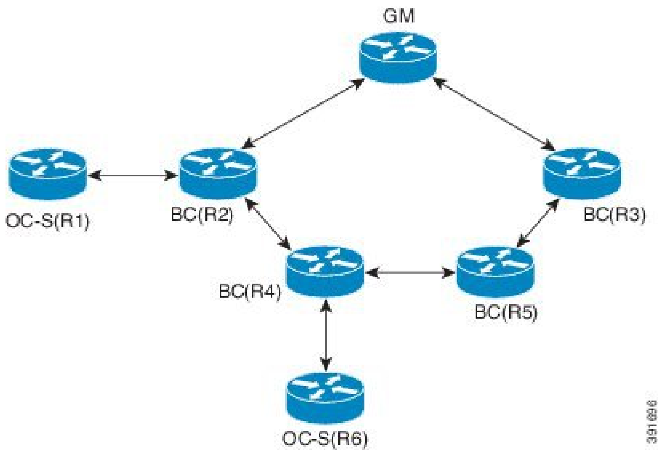
```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk) clock-port SUBORDINATE slave
Router(config-ptp-port)# transport ipv4 unicast interface loopback 23 negotiation
Router(config-ptp-port)# clock-source 8.8.8.1

Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port PRIMARY Master
Router(config-ptp-port)# transport ipv4 unicast interface loopback 23 negotiation
Router(config-ptp-port)# sync interval  <>
Router (config-ptp-port)# announce interval <>
```

Configuring PTP in Multicast Mode

PTP over Ethernet uses multicast MAC addresses for communication of PTP messages between the subordinate clock and the primary clock. The primary sends the announce, synchronization, and delay-response packets using the multicast method. The PTP subordinate receives the multicast announce packets from the primary or multiple primary clocks and determines the best primary one using Best Master Clock Algorithm (BMCA). The subordinate receives and processes the synchronization from the selected primary clock in the same bridge domain.

You should configure the transit nodes as boundary clocks so that the primary and the subordinate clocks can be operated in different bridge domains. This will control the multicast traffic on the network. The following topology is used for configuring PTP in multicast mode.

Figure 19: PTP Topology in Multicast Mode



Before configuring Cisco ASR 901 Router on different modes, you need to configure the bridge domain. The following example shows the configuration of bridge domain and the PTP topology in multicast mode:

Figure 20: Example for PTP Topology in Multicast Mode


```
RouterA #show run interface gigabitethernet0/3

Building configuration...
Current configuration : 202 bytes
!
interface GigabitEthernet0/3
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 999
 !901
end

RouterA# configure terminal
RouterA(config)# ptp clock ordinary domain 0
RouterA(config-ptp-clk)# clock-port PRIMARY master
RouterA(config-ptp-port)# transport ethernet multicast bridge-domain 999

RouterB# show run interface gigabitethernet0/3

Building configuration...
Current configuration : 202 bytes
!
interface GigabitEthernet0/3
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 999
```

```
! end

RouterB# configure terminal
RouterB(config)# ptp clock ordinary domain 0
RouterB(config-ptp-clk)# clock-port SUBORDINATE slave
RouterB(config-ptp-port)# transport ethernet multicast bridge-domain 999
```

Note For PTP over Ethernet support on Cisco ASR 901 Router, the PTP packets received from an external interface should be single tagged with pop1 and double tagged with pop2. Also, the external interface on which the PTP packets are received should have one of the following configurations on EVC.

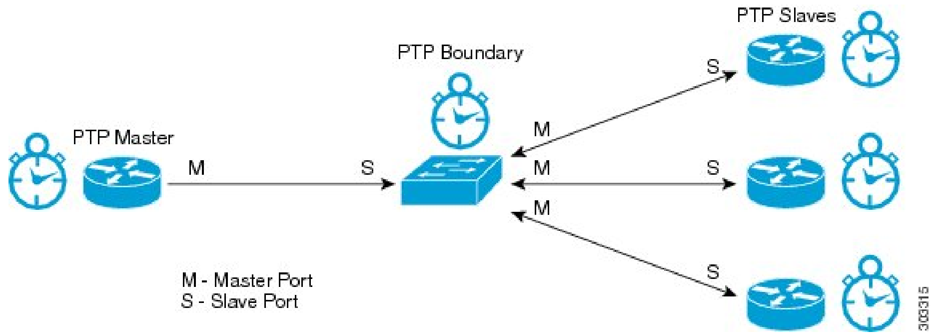
	No pop	pop 1	pop 2
Untag	Yes	—	—
Dot1q	—	Yes	—
QinQ	—	—	Yes
Dot1ad	—	Yes	—
Dot1ad-dot1ad	—	—	Yes
Default	—	—	—
Priority	—	Yes	—

PTP Boundary Clock

A PTP boundary clock (BC) acts as a middle hop between a PTP primary and PTP subordinate. It has multiple ports which can act as a primary or subordinate port as shown in Figure 21: PTP Boundary Clock, on page 331. A PTP boundary clock has one subordinate port and one or more primary ports. A subordinate port acts as a subordinate to a remote PTP primary, while a primary port acts as a primary to a remote PTP subordinate. A PTP boundary clock derives clock from a primary/grand master clock (by acting as a subordinate) and sends the derived clock to the slaves connected to it (by acting as a primary).

PTP boundary clock starts its own PTP session with a number of downstream slaves. The PTP boundary clock mitigates the number of network hops and results in packet delay variations in the packet network between the grand master and subordinate.

Figure 21: PTP Boundary Clock



The Cisco ASR 901 PTP boundary clock has the following capabilities:

- Support for up to 20 clock ports.
- Simultaneous support for static and negotiated clock ports.
- Support for up to 36 slaves and 1 primary.

Note If all clock ports created in PTP boundary clock are static, Cisco ASR 901 supports only 1 primary port and 19 subordinate ports. However, if one or more subordinate ports are configured in unicast negotiation mode, Cisco ASR 901 can support up to 36 subordinates.

- Support for dynamic addition and deletion of clock ports. This capability is supported only on boundary clock primary ports.
- Support for selecting boundary clock as the clock source.

Configuring PTP Boundary Clock

Complete the following steps to configure the PTP boundary clock.

Before you begin

Note If PTP boundary clock is configured before installing the 1588BC license, remove the boundary clock configuration and reconfigure the boundary clock after the license installation.

Note

- The loopback address configured for PTP port can be used only for PTP functionality. This restriction applies only for PTP over loopback. VLAN IP can be used by other protocols.
- The loopback address configured for PTP port does not respond to pings. However, VLAN address (if configured for PTP) will respond to pings.
- A clock port once configured as primary cannot change to subordinate dynamically, and vice versa.
- PTP boundary clock can be configured for only one domain.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock boundary domain** *domain* **Example:** `Router(config)# ptp clock boundary domain 0`	Configures the PTP boundary clock and selects the best primary clock. It also acts as the primary clock if no better clocks are detected. Enters clock configuration mode. • *domain*—The PTP clocking domain number. Valid values are from 0 to 127.
Step 4	**clock-port** *port-name* **slave** **Example:** `Router(config-ptp-clk)# clock-port SUBORDINATE slave`	Sets the clock port to PTP subordinate mode and enters the clock port configuration mode. In subordinate mode, the port exchanges timing packets with a PTP primary clock.

Step 5	Do one of the following:
	• **transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**]
	• **transport ethernet multicast bridge-domain** *bridge-id*
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast`
	`interface loopback 0 negotiation`
		Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.
		• *interface-type*—The type of the interface.
		• *interface-number*—The number of the interface.
		• **negotiation**—(Optional) Enables dynamic discovery of subordinate devices and their preferred format for sync interval and announce interval messages.
		Configures a bridge domain.
		• *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094.
		Note
		Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported.

Step 6	**clock source** *source-address priority* **Example:**	Specifies the address of a PTP primary clock. You can specify a priority value as follows:

	Command or Action	Purpose
	`Router(config-ptp-port)# clock source 5.5.5.5`	• No priority value—Assigns a priority value of 0, the highest priority. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2. • 3—Assigns a priority value of 3. **Note** Priority is used as an index for the configured clock sources and is not a criteria for the BMCA.
Step 7	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 30.30.30.30 1`	Specifies the address of an additional PTP primary clock; repeat this step for each additional primary clock. You can configure up to four primary clocks.
Step 8	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 2.2.2.2 2`	Specifies the address of an additional PTP primary clock; repeat this step for each additional primary clock. You can configure up to four primary clocks.
Step 9	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 50.50.50.50 3`	Specifies the address of an additional PTP primary clock; repeat this step for each additional primary clock. You can configure up to four primary clocks.
Step 10	**clock source** *source-address* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133`	Specifies the address of a PTP primary clock.
Step 11	**clock-port** *port-name* **master** **Example:** `Router(config-ptp-port)# clock-port PRIMARY master`	Sets the clock port to PTP primary mode. In primary mode, the port exchanges timing packets with PTP subordinate devices. **Note** The primary clock-port does not establish a clocking session until the subordinate clock-port is phase aligned.
Step 12	Do one of the following: • **transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**] • **transport ethernet multicast bridge-domain** *bridge-id*	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. • *interface-type*—The type of the interface. • *interface-number*—The number of the interface.

	Command or Action	Purpose
	Example: `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation`	• **negotiation**—(Optional) Enables dynamic discovery of subordinate devices and their preferred format for sync interval and announce interval messages. Configures a bridge domain. • *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094. **Note** Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported. The option of using dynamic IP for PTP over VLAN is generally meant for a subordinate interface. Though the implementation supports dynamic IP assignment on the PTP primary, you must configure the dynamically assigned IP in **"clock source**" command on the PTP subordinate.
Step 13	**exit** **Example:** `Router(config-ptp-port)# exit`	Exits clock port configuration mode.

Verifying PTP modes

Ordinary Clock

Use the **show ptp clock dataset current** command to display the sample output.

```
Router#show ptp clock dataset current
CLOCK [Ordinary Clock, domain 0]
Steps Removed: 1
Offset From Master: 0
```

Use the **show ptp clock dataset default** command to display the sample output.

```
Router#show ptp clock dataset default
CLOCK [Ordinary Clock, domain 0]
Two Step Flag: No
Clock Identity: 0x0:A:8B:FF:FF:5C:A:80
Number Of Ports: 1
Priority1: 128
Priority2: 128
Domain Number: 0
Slave Only: Yes
Clock Quality:
```

```
Class: 13
Accuracy: Greater than 10s
Offset (log variance): 52592
```

Use the **show ptp clock dataset parent domain** command to display the sample output.

```
Router# show ptp clock dataset parent domain 0
CLOCK [Ordinary Clock, domain 0]
Parent Stats: No
Observed Parent Offset (log variance): 65535
Observed Parent Clock Phase Change Rate: 0
Grandmaster Clock:
Identity: 0x0:D0:4:FF:FF:B8:6C:0
Priority1: 128
Priority2: 128
Clock Quality:
Class: 13
Accuracy: Within 1s
Offset (log variance): 52592
```

Use the **show ptp clock dataset time-properties domain** command to display the sample output.

```
Router# show ptp clock dataset time-properties domain 0
CLOCK [Ordinary Clock, domain 0]
Current UTC Offset Valid: TRUE
Current UTC Offset: 33
Leap 59: FALSE
Leap 61: FALSE
Time Traceable: TRUE
Frequency Traceable: TRUE
PTP Timescale: TRUE
Time Source: Internal Oscillator
```

Boundary Clock

Use the **show ptp clock dataset current** command to display the sample output.

```
Router# show ptp clock dataset current
CLOCK [Boundary Clock, domain 0]
  Steps Removed: 0
  Offset From Master: 0ns
```

Use the **show ptp clock dataset default** command to display the sample output.

```
Router# show ptp clock dataset default
CLOCK [Boundary Clock, domain 0]
  Two Step Flag: No
  Clock Identity: 0x0:0:0:FF:FE:0:23:45
  Number Of Ports: 1
  Priority1: 128
  Priority2: 128
  Domain Number: 0
  Slave Only: Yes
  Clock Quality:
    Class: 248
    Accuracy: Within 25us
```

```
    Offset (log variance): 22272
```

Use the **show ptp clock dataset parent domain** command to display the sample output.

```
Router# show ptp clock dataset parent domain 0
CLOCK [Boundary Clock, domain 0]
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 0
  Grandmaster Clock:
    Identity: 0x0:0:0:FF:FE:0:23:45
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 248
      Accuracy: Within 25us
      Offset (log variance): 22272
```

Use the **show ptp clock dataset time-properties domain** command to display the sample output.

```
Router# show ptp clock dataset time-properties domain 0
CLOCK [Boundary Clock, domain 0]
  Current UTC Offset Valid: FALSE
  Current UTC Offset: 34
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: FALSE
  Frequency Traceable: FALSE
  PTP Timescale: FALSE
  Time Source: Internal Oscillator
```

Use the **show ptp port running detail** command to display the details of PTP boundary clock such as primary clock sources added, clock class, and variance.

```
Router#show ptp port running detail

PORT [SLAVE] CURRENT PTP MASTER PORT

PORT [SLAVE] PREVIOUS PTP MASTER PORT

PORT [SLAVE] LIST OF PTP MASTER PORTS

LOCAL PRIORITY 1
  Protocol Address: 22.22.22.22
  Clock Identity:  0x40:55:39:FF:FE:89:6F:40
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 58
  Accuracy: Within 25us
  Offset (log variance): 22272
  Steps Removed: 0

LOCAL PRIORITY 2
  Protocol Address: 66.66.66.66
  Clock Identity:  0x4C:0:82:FF:FE:C7:6F:1C
  PTSF Status:
  Alarm In Stream:
```

```
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 58
  Accuracy: Within 25us
  Offset (log variance): 22272
  Steps Removed: 0

LOCAL PRIORITY 3
  Protocol Address: 77.77.77.77
  Clock Identity:  0x0:0:0:0:0:0:0:0
  PTSF Status: PTSF_SIGNAL_FAIL
  Alarm In Stream: ALARM_ANNOUNCE_FAIL
  Clock Stream Id: 0
  Priority1: 0
  Priority2: 0
  Class: 0
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0
```

Use the **show ptp clock running domain** command to display the sample output.

```
Router#show ptp clock running doman 0

                      PTP Boundary Clock [Domain 0]

         State          Ports          Pkts sent      Pkts rcvd     Redundancy Model

         PHASE_ALIGNED  2              324215         1257513       Hot standby

                               PORT SUMMARY
                                                                                PTP
Master
Name                Tx Mode      Role         Transport    State         Sessions      Port
Addr

SLAVE              unicast      slave        To3/0/2      -             1            9.9.9.1
MASTER              unicast      master       To3/0/2      -             2
```

Verifying PTP Configuration on the 1588V2 subordinate in Unicast Mode

The following examples help you verify the PTP configuration on the1588V2 subordinate.

Note The loopback interface assigned to PTP does not respond to ICMP pings. To check route availability, either do it before assigning the interface to PTP, or remove PTP from the interface and then perform ICMP ping. For removing PTP, use**no transport ipv4 unicast interface loopback** *interface*command. For PTP over VLAN, ping will work even when interface is assigned to PTP.

Note The bridge state indicates the extension of previously known state which can be ignored or considered to be normal. The clock state can get into holdover from bridge state when the packet delay variation is high on the received PTP packets or the PTP connection is lost. This holdover state indicates that the clock cannot be recovered from PTP packets as the quality is poor.

Example 1

```
Router# show ptp clock runn dom 0
                      PTP Ordinary Clock [Domain 0]
         State          Ports          Pkts sent      Pkts rcvd
         ACQUIRING      1              5308           27185
                               PORT SUMMARY
Name               Tx Mode      Role          Transport    State         Sessions
SUBORDINATE              unicast      slave         Lo10         -             1
                             SESSION INFORMATION
SUBORDINATE [L010] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 3.3.3.3            27185      5308       0          0
```

Example 2

```
Router# show platform ptp state
flag = 2
  FLL State                     : 2 (Fast Loop)
  FLL Status Duration           : 7049 (sec)
  Forward Flow Weight           : 0.0
  Forward Flow Transient-Free   : 900 (900 sec Window)
  Forward Flow Transient-Free   : 3600 (3600 sec Window)
  Forward Flow Transactions Used: 23.0 (%)
  Forward Flow Oper. Min TDEV   : 4254.0 (nsec)
  Forward Mafie                 : 38.0
  Forward Flow Min Cluster Width: 7550.0 (nsec)
  Forward Flow Mode Width       : 21400.0 (nsec)
  Reverse Flow Weight           : 100.0
  Reverse Flow Transient-Free   : 900 (900 sec Window)
  Reverse Flow Transient-Free   : 3600 (3600 sec Window)
  Reverse Flow Transactions Used: 200.0 (%)
  Reverse Flow Oper. Min TDEV   : 487.0 (nsec)
  Reverse Mafie                 : 36.0
  Reverse Flow Min Cluster Width: 225.0 (nsec)
  Reverse Flow Mode Width       : 450.0 (nsec)
  Frequency Correction          : 257.0 (ppb)
  Phase Correction              : 0.0 (ppb)
  Output TDEV Estimate          : 1057.0 (nsec)
  Output MDEV Estimate          : 1.0 (ppb)
  Residual Phase Error          : 0.0 (nsec)
  Min. Roundtrip Delay          : 45.0 (nsec)
  Sync Packet Rate              : 65 (pkts/sec)
  Delay Packet Rate             : 65 (pkts/sec)
  Forward IPDV % Below Threshold: 0.0
  Forward Maximum IPDV          : 0.0 (usec)
  Forward Interpacket Jitter    : 0.0 (usec)
  Reverse IPDV % Below Threshold: 0.0
  Reverse Maximum IPDV          : 0.0 (usec)
  Reverse Interpacket Jitter    : 0.0 (usec)
```

Verifying PTP Configuration on the 1588V2 Subordinate in Multicast Mode

A typical configuration on a 1588V2 subordinate in the multicast mode is:

Note For a OC-Subordinate configured in PTP over ethernet in the multicast mode, clock source details cannot be specified. The **show ptp port running detail** command shows all the four primary clock details. However, the details of those primary clocks that are having a session with the subordinate clock will be constantly updated. In the following example two OC-PRIMARY clocks are having session with a OC-SUBORDINATE.

```
Router# show run | sec ptp
ptp clock ordinary domain 0
 1pps-out 0 1 ns
 clock-port SUBORDINATE slave
  transport ethernet multicast bridge-domain 77

Router# show ptp port running detail

PORT [SUBORDINATE] CURRENT PTP PRIMARY PORT
  Protocol Address: 4055.3989.728b
  Clock Identity: 0x40:55:39:FF:FE:89:72:88

PORT [SUBORDINATE] PREVIOUS PTP PRIMARY PORT
  Protocol Address: 0000.0000.0000
  Clock Identity: 0x0:0:0:0:0:0:0:0
  Reason:

PORT [SUBORDINATE] LIST OF PTP PRIMARY PORTS

LOCAL PRIORITY 0
  Protocol Address: 4055.3989.78a3
  Clock Identity:  0x40:55:39:FF:FE:89:78:A0
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 248
  Accuracy: Within 25us
  Offset (log variance): 22272
  Steps Removed: 0

LOCAL PRIORITY 1
  Protocol Address: 4055.3989.728b
  Clock Identity:  0x40:55:39:FF:FE:89:72:88
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 58
  Accuracy: Within 25us
  Offset (log variance): 22272
  Steps Removed: 0

LOCAL PRIORITY 2
  Protocol Address: UNKNOWN
  Clock Identity:  0x0:0:0:0:0:0:0:0
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 0
  Priority2: 0
  Class: 0
```

```
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0

LOCAL PRIORITY 3
  Protocol Address: UNKNOWN
  Clock Identity:  0x0:0:0:0:0:0:0:0
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 0
  Priority2: 0
  Class: 0
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0


Router# show run int gigabitEthernet 0/0
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet0/0
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 33
  rewrite ingress tag pop 1 symmetric
  bridge-domain 77
 !
end

Router# show run int gigabitEthernet 0/3
Building configuration...

Current configuration : 297 bytes
!
interface GigabitEthernet0/3
 no ip address
 negotiation auto
 synchronous mode
 synce state slave
 service instance 2 ethernet
  encapsulation dot1q 33
  rewrite ingress tag pop 1 symmetric
  bridge-domain 77
 !
 service instance 17 ethernet
  encapsulation untagged
  bridge-domain 17
 !
end

Router# show platform ptp stats detailed
Statistics for PTP clock 0
###############################
Number of ports : 1
Pkts Sent       : 4793
Pkts Rcvd       : 26531
Pkts Discarded  : 0

LAST FLL STATE
###################
```

```
Normal loop : Number of Transitions = 0 and Last transition at : 00:00:00.000 UTC Mon Jan
1 1900
Bridge state: Number of Transitions = 0 and Last transition at : 00:00:00.000 UTC Mon Jan
1 1900
Holdover state : Number of Transitions = 1 and Last transition at : 12:08:38.774 UTC Thu
Jun 19 2014

        Statistics for PTP clock port 1
        ##################################
        Pkts Sent        : 4793
        Pkts Rcvd        : 26531
        Pkts Discarded   : 0
        Signals Rejected : 0
        Statistics for L2 Multicast packets
        ###################################
        Multicast address : 011b.1900.0000
        Announces Sent    : 0
        Syncs Sent        : 0
        Follow Ups Sent   : 0
        Delay Reqs Sent   : 4793
        Delay Resps Sent  : 0
        Signals Sent      : 0
        Packets Discarded : 0

                Statistics for peer 1
                ########################
                L2 address        : 4055.3989.728b
                Announces Sent    : 0
                Announces Rcvd    : 37
                Syncs Sent        : 0
                Syncs Rcvd        : 4752
                Follow Ups Sent   : 0
                Follow Ups Rcvd   : 4752
                Delay Reqs Sent   : 0
                Delay Reqs Rcvd   : 0
                Delay Resps Sent  : 0
                Delay Resps Rcvd  : 4753
                Mgmts Sent Rcvd   : 0
                Mgmts Rcvd        : 0
                Signals Sent      : 0
                Signals Rcvd      : 0
                Packets Discarded : 0

                Statistics for peer 2
                ########################
                L2 address        : 4055.3989.78a3
                Announces Sent    : 0
                Announces Rcvd    : 31
                Syncs Sent        : 0
                Syncs Rcvd        : 4069
                Follow Ups Sent   : 0
                Follow Ups Rcvd   : 4069
                Delay Reqs Sent   : 0
                Delay Reqs Rcvd   : 0
                Delay Resps Sent  : 0
                Delay Resps Rcvd  : 4068
                Mgmts Sent Rcvd   : 0
                Mgmts Rcvd        : 0
                Signals Sent      : 0
                Signals Rcvd      : 0
                Packets Discarded : 0
```

Verifying PTP Configuration on the 1588V2 Primary in Unicast Mode

A typical configuration on a 1588V2 primary is:

```
ptp clock ordinary domain 0
tod 0/0 cisco
input 1pps 0/0
clock-port PRIMARY master
transport ipv4 unicast interface Lo20 negotiation
```

Use the **show ptp clock running domain** command to display the PTP clock configuration:

```
Router# show ptp clock running domain 0
      PTP Ordinary Clock [Domain 0]
    State          Ports          Pkts sent      Pkts rcvd
    FREQ_LOCKED     1     1757273    599954
      PORT SUMMARY
Name      Tx Mode      Role         Transport    State        Sessions
o       unicast      master       Lo20         Master        5
      SESSION INFORMATION
o [Lo20] [Sessions 5]
Peer addr    Pkts in    Pkts out    In Errs    Out Errs
9.9.9.14    120208    344732    0    0
9.9.9.13    120159    344608    0    0
9.9.9.11    120148    343955    0    0
9.9.9.12    119699    342863    0    0
9.9.9.10    119511    342033    0    0
```

Use the **show platform ptp stats** command to display the PTP statistics:

```
Statistics for PTP clock 0
###############################
Number of ports : 1
Pkts Sent : 1811997
Pkts Rcvd : 619038
Pkts Discarded : 0
Statistics for PTP clock port 1
##################################
Pkts Sent : 1811997
Pkts Rcvd : 619038
Pkts Discarded : 0
Signals Rejected : 0
Statistics for peer 1
########################
IP addr : 9.9.9.14
Pkts Sent : 355660
Pkts Rcvd : 124008
Statistics for peer 2
########################
IP addr : 9.9.9.13
Pkts Sent : 355550
Pkts Rcvd : 123973
Statistics for peer 3
########################
IP addr : 9.9.9.11
Pkts Sent : 354904
Pkts Rcvd : 123972
Statistics for peer 4
########################
IP addr : 9.9.9.12
Pkts Sent : 353815
Pkts Rcvd : 123525
```

```
Statistics for peer 5
########################
IP addr : 9.9.9.10
Pkts Sent : 352973
Pkts Rcvd : 123326
```

Verifying PTP Configuration on the 1588V2 Primary in Multicast Mode

A typical configuration on a 1588V2 primary is:

```
ptp clock boundary domain 0
 clock-port SUBORDINATE slave
  transport ipv4 unicast interface Lo45 negotiation
  clock source 40.40.40.1
clock-port PRIMARY master
    transport ethernet multicast bridge-domain 1
```

Use the **show ptp clock running domain** command to display the PTP clock configuration:

```
Router# show ptp clock running domain 0

                      PTP Boundary Clock [Domain 0]

         State           Ports          Pkts sent      Pkts rcvd      Redundancy Mode

         PHASE_ALIGNED  2              242559956      189887918      Track all

                               PORT SUMMARY
                                                                         PTP Master
Name   Tx Mode      Role         Transport    State        Sessions     Port Addr

SUBORDINATE  unicast      slave        Lo45         Slave        1            40.40.40.1
PRIMARY mcast        master       Ethernet     Master       1            -


                             SESSION INFORMATION

SUBORDINATE [Lo45] [Sessions 1]

Peer addr          Pkts in    Pkts out   In Errs    Out Errs

40.40.40.1         132729502  44138439   0          0

PRIMARY [Ethernet] [Sessions 1]

Peer addr                          Pkts in    Pkts out   In Errs    Out Errs

4c00.8287.1d33     [BD 1         ] 960676     960676     0          0
```

Use the **show platform ptp state** command to display the PTP servo state:

```
         FLL State                     : 3 (Normal Loop)
         FLL Status Duration           : 687618 (sec)

         Forward Flow Weight           : 47.0
         Forward Flow Transient-Free   : 900 (900 sec Window)
         Forward Flow Transient-Free   : 3600 (3600 sec Window)
         Forward Flow Transactions Used: 200.0 (%)
         Forward Flow Oper. Min TDEV   : 5.0 (nsec)
```

```
Forward Mafie                 : 0.0
Forward Flow Min Cluster Width: 15000.0 (nsec)
Forward Flow Mode Width       : 100.0 (nsec)

Reverse Flow Weight           : 52.0
Reverse Flow Transient-Free   : 900 (900 sec Window)
Reverse Flow Transient-Free   : 3600 (3600 sec Window)
Reverse Flow Transactions Used: 200.0 (%)
Reverse Flow Oper. Min TDEV   : 6.0 (nsec)
Reverse Mafie                 : 0.0
Reverse Flow Min Cluster Width: 7500.0 (nsec)
Reverse Flow Mode Width       : 100.0 (nsec)

Frequency Correction          : 54.836 (ppb)
Phase Correction              : 0.0 (ppb)

Output TDEV Estimate          : 6.0 (nsec)
Output MDEV Estimate          : 0.0 (ppb)

Residual Phase Error          : 3.206 (nsec)
Min. Roundtrip Delay          : 14.0 (nsec)

Sync Packet Rate*             : 64 (pkts/sec)
Delay Packet Rate*            : 64 (pkts/sec)

Forward IPDV % Below Threshold: 0.0
Forward Maximum IPDV          : 0.0 (usec)
Forward Interpacket Jitter    : 0.0 (usec)

Reverse IPDV % Below Threshold: 0.0
Reverse Maximum IPDV          : 0.0 (usec)
Reverse Interpacket Jitter    : 0.0 (usec)
Note: The maximum rates for Sync and Delay packets will be approximately 64 pps.
```

Use the **show platform ptp stats detailed** command to display the PTP statistics:

```
Router#sh platform ptp stats detailed
Statistics for PTP clock 0
###############################
Number of ports : 2
Pkts Sent       : 242525543
Pkts Rcvd       : 189865083
Pkts Discarded  : 0

LAST FLL STATE
###################
Normal loop : Number of Transitions = 1 and Last transition at : 15:51:16.155 UTC Mon Apr
21 2014
Bridge state: Number of Transitions = 0 and Last transition at : 00:00:00.000 UTC Mon Jan
1 1900
Holdover state : Number of Transitions = 0 and Last transition at : 00:00:00.000 UTC Mon
Jan 1 1900

        Statistics for PTP clock port 1
        ##################################
        Pkts Sent        : 44132739
        Pkts Rcvd        : 132712363
        Pkts Discarded   : 0
        Signals Rejected : 0
                Statistics for peer 1
                ########################
                IP address        : 40.40.40.1
                Announces Sent    : 0
                Announces Rcvd    : 344686
                Syncs Sent        : 0
```

```
          Syncs Rcvd        : 44119383
          Follow Ups Sent   : 0
          Follow Ups Rcvd   : 44119383
          Delay Reqs Sent   : 44119179
          Delay Reqs Rcvd   : 0
          Delay Resps Sent  : 0
          Delay Resps Rcvd  : 44115351
          Mgmts Sent Rcvd   : 0
          Mgmts Rcvd        : 0
          Signals Sent      : 13560
          Signals Rcvd      : 13560
          Packets Discarded : 0

Statistics for PTP clock port 2
##################################
Pkts Sent        : 198392804
Pkts Rcvd        : 57152720
Pkts Discarded   : 0
Signals Rejected : 0
Statistics for L2 Multicast packets
###################################
Multicast address : 011b.1900.0000
Announces Sent    : 343722
Syncs Sent        : 83733919
Follow Ups Sent   : 83733919
Delay Reqs Sent   : 0
Delay Resps Sent  : 0
Signals Sent      : 0
Packets Discarded : 0

          Statistics for peer 2
          ########################
          L2 address        : 4c00.8287.1d33
          Announces Sent    : 0
          Announces Rcvd    : 0
          Syncs Sent        : 0
          Syncs Rcvd        : 0
          Follow Ups Sent   : 0
          Follow Ups Rcvd   : 0
          Delay Reqs Sent   : 0
          Delay Reqs Rcvd   : 954979
          Delay Resps Sent  : 954979
          Delay Resps Rcvd  : 0
          Mgmts Sent Rcvd   : 0
          Mgmts Rcvd        : 0
          Signals Sent      : 0
          Signals Rcvd      : 0
          Packets Discarded : 0
```

Note In primary node, the Delay Resps packet sent to a specific peer is a response to the Delay Reqs packet. Hence, the **sh platform ptp stats detailed** command displays the details of both the sent and received packets.

PTP Hybrid Clock

To improve the clock quality, you can either improve the oscillator class or reduce the number of hops between the primary and the subordinate. In PTP hybrid mode, the oscillator class is improved by using a physical layer clock (sourced from a stratum-1 clock) instead of the available internal oscillator. The PTP hybrid mode is supported for ordinary clock (in subordinate mode only) and boundary clock.

Configuring a Hybrid Ordinary Clock

Complete the following steps to configure a hybrid clocking in ordinary subordinate clock mode:

Before you begin

When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same primary clock.

Note

- Hybrid mode is not supported when PTP ordinary clock is in the primary mode.
- Hybrid clock is not supported with ToP as network-clock. It needs a valid physical clock source, for example, Sync-E/BITS/10M/TDM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain* **hybrid** **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock as an ordinary clock and enters clock configuration mode. • *domain*—The PTP clocking domain number. Valid values are from 0 to 127. • **hybrid**—(Optional) Enables the PTP boundary clock to work in hybrid mode. Enables the hybrid clock such that the output of the clock is transmitted to the remote slaves.
Step 4	**clock-port** *port-name* **slave** **Example:** `Router(config-ptp-clk)# clock-port subordinate slave`	Sets the clock port to PTP subordinate mode and enters clock port configuration mode. In subordinate mode, the port exchanges timing packets with a PTP primary clock.
Step 5	Do one of the following: • **transport ipv4 unicast interface** *interface-type interface-number*	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. • *interface-type*—The type of the interface.

	Command or Action	Purpose

	• **transport ethernet multicast bridge-domain** *bridge-id*
	Example:
	`Router(config-ptp-port)# transport ipv4`
	`unicast interface loopback 0`
		• *interface-number*—The number of the interface.
		Configures a bridge domain.
		• *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094.
		Note
		Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported.

Step 6	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 5.5.5.5`	Specifies the address of a PTP primary clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0, the highest priority. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2. • 3—Assigns a priority value of 3. Repeat this step for each additional primary clock. You can configure up to four primary clocks. **Note** Priority is used as an index for the configured clock sources and is not a criteria for the BMCA.
Step 7	**clock source** *source-address* **Example:** `Router(config-ptp-port)# clock source 8.8.8.1`	Specifies the address of a PTP primary clock.
Step 8	**announce timeout** *value* **Example:** `Router(config-ptp-port)# announce timeout 8`	(Optional) Specifies the number of PTP announcement intervals before the session times out. • *value*—The range is from 1 to 10. The default is 3.
Step 9	**delay-req interval** *interval* **Example:** `Router(config-ptp-port)# delay-req interval 1`	(Optional) Configures the minimum interval allowed between PTP delay request messages. The intervals are set using log base 2 values, as follows: • 5—1 packet every 32 seconds • 4—1 packet every 16 seconds

	Command or Action	Purpose
		• 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second. The default is -6.
Step 10	**sync interval** *interval* **Example:** `Router(config-ptp-port)# sync interval -5`	(Optional) Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values. The Cisco ASR 901 router supports the following values: • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. The default is -6.
Step 11	**end** **Example:** `Router(config-ptp-port)# end`	Exits clock port configuration mode and enters privileged EXEC mode.

Configuring a Hybrid Boundary Clock

Complete the following steps to configure a hybrid clocking in PTP boundary clock mode.

Before you begin

When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same primary clock.

Note Hybrid clock is not supported with ToP as network-clock. It needs a valid physical clock source, for example, Sync-E/BITS/10M/TDM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock boundary domain** *domain* **hybrid** **Example:** `Router(config)# ptp clock boundary domain 0 hybrid`	Configures the PTP boundary clock and enters clock configuration mode. • *domain*—The PTP clocking domain number. Valid values are from 0 to 127. • **hybrid**—(Optional) Enables the PTP boundary clock to work in hybrid mode. Enables the hybrid clock such that the output of the clock is transmitted to the remote slaves.
Step 4	**clock-port** *port-name* **slave** **Example:** `Router(config-ptp-clk)# clock-port subordinate slave`	Sets the clock port to PTP subordinate mode and enters the clock port configuration mode. In subordinate mode, the port exchanges timing packets with a PTP primary clock.
Step 5	Do one of the following: • **transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**] • **transport ethernet multicast bridge-domain** *bridge-id* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation`	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. • *interface-type*—The type of the interface. • *interface-number*—The number of the interface. • **negotiation**—(Optional) Enables dynamic discovery of subordinate devices and their preferred format for sync interval and announce interval messages. Configures a bridge domain. • *bridge-id*—Identifier for the bridge domain instance. The range is from 1 to 4094.

	Command or Action	Purpose
		Note Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported.
Step 6	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 5.5.5.5`	Specifies the address of a PTP primary clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0, the highest priority. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2. • 3—Assigns a priority value of 3. Repeat this step for each additional primary clock. You can configure up to four primary clocks. **Note** Priority is used as an index for the configured clock sources and is not a criteria for the BMCA.
Step 7	**clock source** *source-address* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133`	Specifies the address of a PTP primary clock.
Step 8	**clock-port** *port-name* **primary** **Example:** `Router(config-ptp-port)# clock-port primary master`	Sets the clock port to PTP primary mode. In primary mode, the port exchanges timing packets with PTP subordinate devices. **Note** The primary clock-port does not establish a clocking session until the subordinate clock-port is phase aligned.
Step 9	**transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**] **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation`	Sets port transport parameters. • *interface-type*—The type of the interface. • *interface-number*—The number of the interface. • **negotiation**—(Optional) Enables dynamic discovery of subordinate devices and their preferred format for sync interval and announce interval messages. **Note** Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported. The

	Command or Action	Purpose
		option of using dynamic IP for PTP over VLAN is generally meant for a subordinate interface. Though the implementation supports dynamic IP assignment on the PTP primary, you must configure the dynamically assigned IP in **“clock source**” command on the PTP subordinate.
Step 10	**exit** **Example:** `Router(config-ptp-port)# exit`	Exits clock port configuration mode. **Note** The hybrid clocking in PTP boundary clock mode will work as a PTP ordinary clock when frequency source is not selected. **Note** The hybrid clock (HC) relies on an external clock source for frequency recovery while phase is recovered through PTP. Once the HC reaches the normal or phase aligned state, and if the external frequency channel is active and traceable to PRC, then the HC moves into the phase aligned state even when the PTP link is down.

Verifying Hybrid modes

Use the show running-config | section ptp command to display the sample output.

```
Router# show running-config | section ptp
ptp clock ordinary domain 20 hybrid
 time-properties gps timeScaleTRUE currentUtcOffsetValidTRUE leap59FALSE leap61FALSE 35
 clock-port subordinate slave
  transport ipv4 unicast interface Lo17
  clock source 17.17.1.1
```

Use the show ptp clock running domain command to display the sample output.

```
Router# show ptp clock running domain
                      PTP Ordinary Clock [Domain 20] [Hybrid]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              27132197       81606642       Track all
                               PORT SUMMARY
                                                                       PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
Subordinate unicast      slave        Lo17         Slave        1            17.17.1.1
```

Use the show platform ptp channel_status command to display the sample output after PTP is in normal state.

```
Router#show platform ptp channel_status
Configured channels : 2
channel[0]: type=0, source=0, frequency=0, tod_index=0, freq_prio=5
            time_enabled=y, freq_enabled=y, time_prio=1 freq_assumed_QL=0
            time_assumed_ql=0, assumed_ql_enabled=n
```

```
channel[1]: type=6, source=17, frequency=0, tod_index=0, freq_prio=2
            time_enabled=n, freq_enabled=y, time_prio=0 freq_assumed_QL=0
            time_assumed_ql=0, assumed_ql_enabled=n
  Channel 0:    Frequency       Time
---------------------------------------
       Status  OK           OK
       Weight     0               100
       QL         9               9
---------------------------------------
   QL is not read externally.   Fault status: 00000000
  Channel 1:    Frequency       Time
---------------------------------------
       Status  OK           Disabled
       Weight     100             0
       QL         9               9
---------------------------------------
   QL is not read externally.   Fault status: 00000000
```

Configuration Examples for BMCA

This section provides the following configuration examples:

- Example: Configuring a Subordinate Ordinary Clock in BMCA, on page 352
- Example: Configuring a Subordinate Ordinary Clock in BMCA, on page 352

Example: Configuring a Subordinate Ordinary Clock in BMCA

The following is a sample configuration of a subordinate ordinary clock in BMCA:

```
!
  ptp clock ordinary domain 0
  clock-port subordinate slave
  transport ipv4 unicast interface Lo30 negotiation
  clock source 22.22.22.1
  clock source 66.66.66.1 1
  clock source 33.33.33.1 2
  clock source 44.44.44.1 3
!
```

Example: Configuring a Boundary Clock in BMCA

The following is a sample configuration of a boundary clock in BMCA:

```
!
  ptp clock boundary domain 0
  clock-port SLAVE slave
  transport ipv4 unicast interface Lo30 negotiation
  clock source 22.22.22.1
  clock source 66.66.66.1 1
  clock source 33.33.33.1 2
  clock source 44.44.44.1 3
  clock-port MASTER master
  transport ipv4 unicast interface Lo50 negotiation
!
```

Note The ordinary clock and boundary clock configurations remain the same for both hybrid clock and hybrid boundary clock. Change the PTP domain configuration to ptp clock ordinary domain 0 hybrid for a hybrid clock and ptp clock boundary domain 0 hybrid for a hybrid boundary clock. An appropriate frequency source (SyncE) will be enabled for the hybrid mode.

SSM and PTP Interaction

PTP carries clock quality in its datasets in the structure defined by the IEEE 1588 specification. The Ordinary Clock (OC) master carries the Grand Master (GM) clock quality in its default dataset which is sent to the downstream OC slaves and Boundary Clocks (BC). The OC slaves and BCs keep the GM clock quality in their parent datasets.

If the T0 clock in Cisco ASR 901 is driven by the clock recovered from the OC Slave (if ToP0/12 is selected as clock-source), then the clock quality in the PTP parent dataset represents the quality of the ToP0/12 input clock. This should be informed to the netsync process for proper clock selection. This is done by translating clockClass data field in clock quality to QL-values expected by netsync.

On the other hand, if Cisco ASR 901 serves as the OC Master, then the GM clock is the clock providing T0 clock to Cisco ASR 901 router. Hence, the T0 clock quality should be used by OC master to fill up clockClass in the clock quality field, in its default dataset. For this, the T0 output QL-value should be mapped to the clockClass value according to ITU-T Telecom Profile, and set in the default dataset of the OC Master. This QL-value is then transmitted to the PTP slaves and BC downstream.

ClockClass Mapping

The Cisco ASR 901 router supports two methods of mapping PTP ClockClass to SSM/QL-value:

- Telecom Profile based on ITU-T G.8265.1/Y.1365.1 PTP (Telecom) Profile for Frequency Synchronization [2]
- Default method of calculating clockClass based on IEEE 1588v2 PTP specification.

Telecom Profiles

The Telecom Profile specifies an alternative algorithm for selecting between different master clocks, based on the quality level (QL) of master clocks and on a local priority given to each master clock. Release 3.11 introduces support for telecom profiles using a new configuration method, which allow you to configure a clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes.

PTP Redundancy

PTP redundancy is an implementation on different clock nodes by which the PTP slave clock node achieves the following:

- Interact with multiple master ports such as grand master, boundary clock nodes, and so on.
- Open PTP sessions.
- Select the best master from the existing list of masters (referred to as the primary PTP master port or primary clock source).

- Switch to the next best master available in case the primary master fails, or the connectivity to the primary master fails.

> **Note** The Cisco ASR 901 Series Router supports unicast-based timing as specified in the 1588-2008 standard. Hybrid mode is not supported with PTP 1588 redundancy.

Configuring Telecom Profile in Slave Ordinary Clock

Complete the following steps to configure the telecom profile in slave ordinary clock.

Before you begin

- When configuring the Telecom profile, ensure that the master and slave nodes have the same network option configured.
- Negotiation should be enabled for master and slave modes.
- Cisco ASR 901 router must be enabled using the network-clock synchronization mode QL-enabled command for both master and slave modes.

> **Note**
> - Telecom profile is not applicable for boundary clocks. It is only applicable for ordinary clocks.
> - Hybrid mode with OC-MASTER is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain-name* **Example:** `Router(config)# ptp clock ordinary domain 4`	Configures the PTP ordinary clock and enters clock configuration mode. • *domain*—The PTP clocking domain number. Valid values are from 4 to 23.
Step 4	**clock-port** *port-name* {**master** | **slave**} **profile g8265.1** **Example:**	Sets the clock port to PTP slave mode and enters clock port configuration mode. In slave mode, the port exchanges timing packets with a PTP master clock.

	Command or Action	Purpose
	`Router(config-ptp-clk)# clock-port Slave slave`	The profile keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.

Step 5	**transport ipv4 unicast interface** *interface-type interface-number*
	Example:
	`Router(config-ptp-port)# transport ipv4`
	`unicast interface loopback 0`
		Sets port transport parameters.
		• *interface-type*—The type of the interface.
		• *interface-number*—The number of the interface.
		Note
		Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported.

Step 6	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 8.8.8.1`	Specifies the address of a PTP master clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0, the highest priority. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2.
Step 7	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 8.8.8.2 1`	Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to four master clocks.
Step 8	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 8.8.8.3 2`	Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to four master clocks.
Step 9	**clock source** *source-address priority* **Example:** `Router(config-ptp-port)# clock source 8.8.8.4 3`	Specifies the address of an additional PTP master clock; repeat this step for each additional master clock. You can configure up to four master clocks.
Step 10	**end** **Example:** `Router(config-ptp-port)# end`	Exits clock port configuration mode and enters privileged EXEC mode.

Configuring Telecom Profile in Master Ordinary Clock

Complete the following steps to configure the telecom profile in the master ordinary clock.

Before you begin

- When configuring the telecom profile, ensure that the master and slave nodes have the same network option configured.
- Negotiation should be enabled for master and slave modes.
- Cisco ASR 901 router must be enabled using the network-clock synchronization mode QL-enabled command for both master and slave modes.

Note

- Telecom profile is not applicable for boundary clocks. It is only applicable for ordinary clocks.
- Hybrid mode with OC-MASTER is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain-name* **Example:** `Router(config)# ptp clock ordinary domain 4`	Configures the PTP ordinary clock and enters clock configuration mode. • *domain*—The PTP clocking domain number. Valid values are from 4 to 23.
Step 4	**clock-port** *port-name* {**master** | **slave**} **profile g8265.1** **Example:** `Router(config-ptp-clk)# clock-port Master master profile g8265.1`	Sets the clock port to PTP master and enters clock port configuration mode. In master mode, the port exchanges timing packets with a PTP slave devices. The profile keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best master clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.

	Command or Action	Purpose
Step 5	**transport ipv4 unicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0`	Sets port transport parameters. • *interface-type*—The type of the interface. • *interface-number*—The number of the interface. **Note** Effective with Cisco IOS Release 15.5(2)S onwards, VLAN interface (with DHCP assigned IP or static IP) is supported. The option of using dynamic IP for PTP over VLAN is generally meant for a Slave interface. Though the implementation supports dynamic IP assignment on the PTP master, you must configure the dynamically assigned IP in **"clock source**" command on the PTP Slave.
Step 6	**end** **Example:** `Router(config-ptp-port)# end`	Exits clock port configuration mode and enters privileged EXEC mode.

Verifying Telecom profile

Use the show ptp port running detail command to display the details of PTP masters configured for a Telecom profile slave. The PTSF and Alarm fields indicate the alarm experienced by the SLAVE clock for the MASTER clock.

```
Router#show ptp port running detail
PORT [slave] CURRENT PTP MASTER PORT
  Protocol Address: 208.1.1.3
  Clock Identity: 0xE4:D3:F1:FF:FE:FF:BC:E4
PORT [slave] PREVIOUS PTP MASTER PORT
  Protocol Address: 208.1.1.1
  Clock Identity: 0xE4:D3:F1:FF:FE:22:F2:C8
  Reason:
PORT [slave] LIST OF PTP MASTER PORTS
LOCAL PRIORITY 0
  Protocol Address: 208.1.1.1
Clock Identity: 0xE4:D3:F1:FF:FE:22:F2:C8
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 102
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0
LOCAL PRIORITY 1
  Protocol Address: 208.1.1.3
  Clock Identity:  0xE4:D3:F1:FF:FE:FF:BC:E4
  PTSF Status:
  Alarm In Stream:
```

```
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 100
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0
LOCAL PRIORITY 2
  Protocol Address: 208.1.1.4
  Clock Identity:  0x40:55:39:FF:FE:89:44:48
  PTSF Status:
  Alarm In Stream:
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Class: 102
  Accuracy: Unknown
  Offset (log variance): 0
  Steps Removed: 0
```

Use the show ptp clock running domain command to display the sample output.

```
Router#show ptp clock running domain 10
                      PTP Ordinary Clock [Domain 10]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              22459694       67364835       Track all
                               PORT SUMMARY
                                                                       PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
SLAVE unicast      slave        Lo40         Slave        1            4.4.4.3
                             SESSION INFORMATION
SLAVE [Lo40] [Sessions 1]
Peer addr          Pkts in    Pkts out   In Errs    Out Errs
4.4.4.3            60023902   20011138   0          0
```

Setting the TimeProperties

The timeProperties dataset members (except timeTraceable and frequencyTraceable) can be individually set by using the time-properties command.

Caution The time-properties command does not perform any input validation; use this command with caution.

The following is an example of the time-properties command:

```
Router(config-ptp-clk)# time-properties atomic-clock timeScaleTRUE currentUtcOffsetValidTRUE
 leap59TRUE leap61FALSE 34
slave#show ptp clock dataset time-properties
CLOCK [Ordinary Clock, domain 0]
 Current UTC Offset Valid: TRUE
 Current UTC Offset: 34
 Leap 59: TRUE
 Leap 61: FALSE
 Time Traceable: TRUE
 Frequency Traceable: TRUE
 PTP Timescale: TRUE
 Time Source: Atomic
```

The values of *Time Traceable* and *Frequency Traceable* are determined dynamically.

ASR 901 Negotiation Mechanism

The Cisco ASR 901 router supports a maximum of 36 slaves, when configured as a negotiated 1588V2 master. For a slave to successfully negotiate with the Cisco ASR 901 master, it should request sync and announce packet rates that are not greater than the sync and announce rate that are currently set in the master.

For example, if the sync interval on the master is -5 (32 packets/second), and if the slave tries to negotiate a value of sync interval value of -6 (64 packets/second), the negotiation fails.

Static Unicast Mode

A clock destination can be added when the master is configured in the static unicast mode (by configuring the transport without the negotiation flag). The master does not communicate with any other slave, in this configuration.

```
Router(config-ptp-port)#clock destination
 9.9.9.10
```

VRF-Aware Precision Time Protocol

Effective from Cisco IOS Release 15.4(3)S, the Cisco ASR 901 Router supports VRF-aware PTP. PTP support over virtual routing and forwarding (VRF) instance-enabled interfaces allows the PTP loopback interface to be part of VRF rather than maintaining the loopback addresses in the global routing table. This enables the service providers to reuse the same IP address for multiple loopback interfaces by configuring PTP loopback under VRF. This enables you to use PTP over VRF lite and PTP over VRF with MPLS network. You can configure a loopback interface as part of a VRF instance or a global routing table depending on the requirement.

Configuring VRF-Aware Precision Time Protocol

To configure VRF-aware PTP, perform the following tasks:

Restrictions

- Bridge domains used internally by PTP are not available to user. To view the list of such internally used bridge domains, use the **show vlan internal usage** command.
- VRF-aware PTP feature is supported only on loopback interfaces with or without VRFs.
- The PTP with route leaks is *not* supported when the master is in global routing table and the slave is in vrf table.

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf green`	Creates a VPN routing and forwarding (VRF) instance. • *vrf-name*—Name assigned to the VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Specifies a route distinguisher (RD) for a VRF instance. • *route-distinguisher* —An autonomous system number (ASN) and an arbitrary number (for example, 101:1), or an IP address and an arbitrary number (for example, 192.168.122.15:1).
Step 5	**route-target export** *route-target-ext-community* **Example:** `Router(config-vrf)# route-target export 100:1`	Creates lists of export route-target extended communities for the specified VRF. • *route-target-ext-community* —An autonomous system number (ASN) and an arbitrary number (for example, 100:1) or an IP address and an arbitrary number (for example, 192.168.122.15:1). Enter the route-distinguisher value specified in 4.
Step 6	**route-target import** *route-target-ext-community* **Example:** `Router(config-vrf)# route-target import 100:1`	Creates lists of import route-target-extended communities for the specified VRF. • *route-target-ext-community* —An autonomous system number (ASN) and an arbitrary number (for example, 100:1), or an IP address and an arbitrary number (for example, 192.168.122.15:1). Enter the route-distinguisher value specified in 4.
Step 7	**exit** **Example:** `Router(config-vrf)# exit`	Exits VRF configuration mode.
Step 8	**interface vlan***vlan-id* **Example:** `Router(config)# interface vlan 4`	Configures a VLAN interface and enters interface configuration mode. • *vlan-id* —VLAN identifier. VLAN range is from 1 to 4093.
Step 9	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding green`	Associates a VRF with an interface or subinterface. • *vrf-name* —Name assigned to the VRF. Enter the value specified in Step 3.

	Command or Action	Purpose
Step 10	**ip address** *address mask* **Example:** `Router(config-if)# ip address 4.4.4.2 255.255.255.0`	Sets a primary or secondary IP address for the interface. By default, sets the primary IP address. • *address* —IP address • *mask* —Subnet mask
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 12	**router ospf** *process-id* [**vrf** *vrf-name*] **Example:** `Router(config)# router ospf 2 vrf green`	Configures an OSPF routing process and enters router configuration mode. • *process-id* —Internally-used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. • *vrf-name* —Name assigned to the VRF. Enter the value specified in 3.
Step 13	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# router ospf 2 vrf green`	Configures the interfaces on which OSPF runs and defines the area ID for those interfaces. • *ip-address* —IP address • *wildcard-mask*—IP-address-type mask that includes optional bits. • *area-id*—Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument. **Note** Repeat this step to configure different interfaces on which OSPF runs, and to define the area ID for those interfaces.
Step 14	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode.

Examples

The following is a sample configuration of VRF-aware PTP:

```
!
ip vrf green
rd 100:1
route-target export 100:1
route-target import 100:1
!
!
interface Vlan4
ip vrf forwarding green
ip address 4.4.4.2 255.255.255.0
mpls ip
!
interface Loopback4
ip vrf forwarding green
ip address 50.50.50.50 255.255.255.255
!
router ospf 2 vrf green
network 4.4.4.0 0.0.0.255 area 2
network 50.50.50.50 0.0.0.0 area 2
!
!
end

 ptp clock ordinary domain 0
 Clock-port slave slave
 Transport ipv4 unicast interface loopback 4 negotiation
 Clock source 5.5.5.5
!
```

Configuring ToD on 1588V2 Slave

Use the following commands configure ToD on the 1588V2 slave:

Command	Purpose
tod {slot|subslot} {cisco/ntp|ubx|nmea}	Configures ToD on 1588V2.
1pps-out *1 PPS offset in ns pulse width pulse width unit*	Configures 1 PPS output parameters.

This example shows the ToD configuration on the 1588V2 slave:

```
Router# config terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# tod 0/0 cisco
Router(config-ptp-clk)# 1pps-out 0 2250 ns
Router(config-ptp-clk)# clock-port SLAVE slave
Router(config-ptp-port)# transport ipv4 unicast interface Lo10 negotiation
Router(config-ptp-port)# clock source 1.1.1.1
Router(config-ptp-port)# end
```

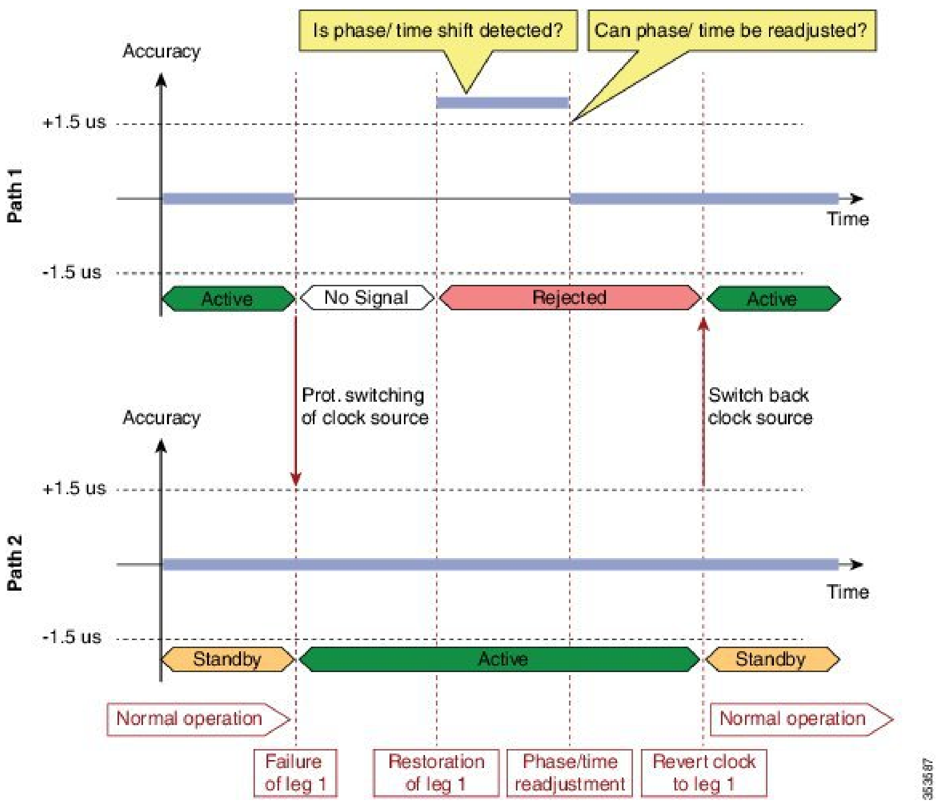
1588v2 Phase Asymmetry Correction

In Optical Transport Network (OTN) network based deployments, though the PDV produced by the network is within the G.8261 limits and asymmetry created by traffic is also less, the OTN elements may add a fixed asymmetry (about 4-5usec) when the OTN element is reboots or optical link related event occurs. The asymmetry detection is tied to the BMCA clock switchover and correction is supported from Cisco IOS

Release 15.5(1)S on the Cisco ASR 901 Series Routers. This mechanism is enabled on both ordinary clock (OC) slave and boundary clock (BC) slave.

The following diagram indicates the design statement of asymmetry correction at a high level.

Figure 22: 1588v2 Phase Asymmetry Correction



When the BMCA algorithm selects a new master, the previous recovered servo-reported phase offset is saved as fixed-phase-offset and a flag is set to indicate to use this value instead of the servo-reported phase offset. This results in phase holdover from the previous master until the path to new master is available. The BMCA master and the servo events portray a path to the new master by comparing the fixed-phase-offset value to the servo-reported phase offset from the new master. The delta phase is computed and applied to servo, which enables the servo to come out of phase holdover.

For certain failures over one path, the delay asymmetry could differ by up to 4 usec after restoration, which would shift the phase or time by up to 2 usec. The valid path continues to provide an accurate phase or time. The root cause for this behavior is the underlying optical network that causes the asymmetry variation and forces the system to do an internal allocation during a disruption. When a link goes down, the underlying optical network fails to allow the same buffer, causing the variation.

In the following scenarios, the asymmetry is corrected after an optical link disruption, based on the persistent PTP link:

Initially, the symmetry is corrected based on measurements and manual adjustment on the router. For that:

- Time Link 1 is marked as ACTIVE.
- Time Link 2 is marked as STANDBY.

Note The initial path asymmetry is compensated by using an external measurement device and compensates the 1pps offset.

In Scenario 1, the optical link 1 goes down and comes back after a while. Here:

- Time is persistent on Link 2 and is used as ACTIVE.
- When Link 1 comes back; time from this link is marked as suspicious.
- Asymmetry is adjusted based on Link 2, enabling it to be in sync with Link 1.
- Link 1 is marked as ACTIVE.
- Link 2 is marked as STANDBY.

In Scenario 2, the optical link 2 goes down and comes back after a while. Here:

- Time is persistent on Link 2 and is used as ACTIVE.
- When Link 2 comes back; time from this link is marked as suspicious.
- Asymmetry is adjusted based on Link 1, enabling it to be in sync with Link 2.
- Link 2 is marked as ACTIVE.
- Link 1 is marked as STANDBY.

Note Both the above scenarios requires use of *phase holdover* mode, which becomes active when there is a Master switch. After the old link is restored, the SERVO learns the new path and applies the correction.

- The PTP phase symmetry correction feature is supported only on IEEE1588v2 BMCA.
- Delay asymmetry value should be enabled on the available master clock source if reference master is removed.
- The delay asymmetry in the network should be measured exactly before its applied on the clock source.
- The Hybrid Slave clock always remains in Normal_loop during a PTP master switch and hence, the newly calculated asymmetry is compensated after 10 minutes of the master switch.
- If the selected PTP master before-reload is not the same after-reload, then the asymmetry table in flash is cleared to avoid using stale values for the new master.
- Phase asymmetry is not supported in Telecom profile and PTP over Ethernet.
- Phase asymmetry (phase correction and path asymmetry) is supported only in Ordinary Slave clock, Boundary Clock slave, Hybrid Slave clock, and Hybrid Boundary Slave clock.
- Exact delay asymmetry value should be measured from the network path to the master source before its applied on clock source.
- The clock sources should be enabled with delay-asymmetry value configuration measured from the network path.

- The router supports phase asymmetry correction feature for a maximum of four BMCA clock sources.
- A syslog message is generated for every phase correction change applied by phase correction feature.

Configuring Asymmetry Correction

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ptp clock ordinary domain** *domain* **Example:** `Router(config)# ptp clock ordinary domain 0`	Creates a Precision Time Protocol (PTP) clock and specifies the clock mode.
Step 4	**asymmetry-compensation** **Example:** `Router(config-ptp-clk)# asymmetry-compensation`	Enables inter-path asymmetry compensation.
Step 5	**clock-port** *name* **slave** **Example:** `Router(config-ptp-clk)# clock-port SLAVE slave`	Specifies the clocking mode of a PTP clock port and enters clock port configuration mode.

Step 6	**transport ipv4 unicast interface** *interface-type* **negotiation**
	Example:
	`Router(config-ptp-port)# transport ipv4`
	`unicast interface Lo1 negotiation`
		Specifies the IP version, transmission mode, and interface that a PTP clock port uses to exchange timing packets.

Step 7	**clock source** *source-address local-priority* **delay-asymmetry** *asymmetry-delay* **nanoseconds** **Example:** `Router(config-ptp-port)# clock source 100.100.100.100 1 delay-asymmetry 73000 nanoseconds`	Configures a connection to a PTP master device, and sets the asymmetry delay.

	Command or Action	Purpose
Step 8	**clock source** *source-address local-priority* **delay-asymmetry** *asymmetry-delay* **nanoseconds** **Example:** `Router(config-ptp-port)# clock source 9.9.9.9 2 delay-asymmetry 56000 nanoseconds`	Configures a connection to a PTP master device, and sets the asymmetry delay.
Step 9	**clock source** *source-address local-priority* **delay-asymmetry** *asymmetry-delay* **nanoseconds** **Example:** `Router(config-ptp-port)# clock source 5.5.5.1 3 delay-asymmetry 89000 nanoseconds`	Configures a connection to a PTP master device, and sets the asymmetry delay.

Verifying 1588v2 Phase Asymmetry Correction

To verify the 1588v2 phase asymmetry correction configuration, use the **show** command as shown in the example below:

```
Router# show platform ptp phase_correction_details

Last Phase Correction applied : 36500 nanoseconds
```

Example: Configuring 1588v2 Phase Asymmetry Correction

```
ptp clock ordinary domain 0
 asymmetry-compensation
 clock-port SLAVE slave
 transport ipv4 unicast interface Lo1 negotiation
 clock source 100.100.100.100 1 delay-asymmetry 73000 nanoseconds
 clock source 9.9.9.9 2 delay-asymmetry 56000 nanoseconds
 clock source 5.5.5.1 3 delay-asymmetry 89000 nanoseconds
```

Troubleshooting Tips

Use the following debug commands to troubleshoot the PTP configuration on the Cisco ASR 901 router:

Danger We suggest you do not use these debug commands without TAC supervision.

Command	Purpose
[no] debug platform ptp error	**Enables debugging of internal errors.** **The no form of the command disables debugging internal errors.**

Command	Purpose
[no] debug platform ptp event	Displays event messages. **The no form of the command disables displaying event messages.**
[no] debug platform ptp verbose	Displays verbose output. **The no form of the command disables displaying verbose output.**
[no] debug platform ptp all	Debugs for error, event and verbose. **The no form of the command disables all debugging.**

CHAPTER 22

G.8275.1 Telecom Profile

Precision Time Protocol (PTP) is a protocol for distributing precise time and frequency over packet networks. PTP is defined in the IEEE Standard 1588. It defines an exchange of timed messages

PTP allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

This recommendation allows for proper network operation for phase and time synchronization distribution when network equipment embedding a telecom boundary clock (T-BC) and a telecom time slave clock (T-TSC) is timed from another T-BC or a telecom grandmaster clock (T-GM). This recommendation addresses only the distribution of phase and time synchronization with the full timing support architecture as defined in ITU-T G.8275.

Effective from Cisco IOS Release 3.18.1SP, the Cisco ASR 901 Router supports G.8275.1 telecom profile.

Why G.8275.1?

The G.8275.1 profile is used in mobile cellular systems that require accurate synchronization of time and phase. For example, the fourth generation (4G) of mobile telecommunications technology.

The G.8275.1 profile is also used in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol.

Because a boundary clock is used at every node in the chain between PTP Grandmaster and PTP Subordinate, there is reduction in time error accumulation through the network.

More About G.8275.1

The G.8275.1 must meet the following requirements:

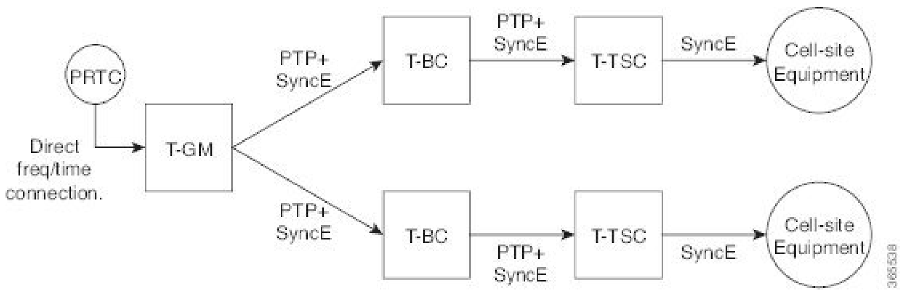
- Non-participant devices, that is, devices that only forward PTP packets, and PTP transparent clocks are not allowed.
- The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock

(PRTC). T-GM in locked mode must have phase and frequency sources that are traceable to PRTC. T-GM in locked mode must always have QL-PRC/PRS frequency. T-GM can be in holdover when losing phase. In such case, its default clock class is defined based on the available frequency source quality.

- The telecom time subordinate clock (T-TSC) synchronizes its local clock to another PTP clock (in most cases, the T-BC), and does not provide synchronization through PTP to any other device.
- The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an upstream T-BC, and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster.

The following figure describes a sample G.8275.1 topology.

Figure 23: A Sample G.8275.1 Topology



PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol.

A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

The allowed domain numbers of PTP domains within a G.8275.1 network are between 24 and 43 (both inclusive).

PTP Messages and Transport

The following PTP transport parameters are defined:

- For transmitting PTP packets, either the forwardable multicast MAC address (01-1B-19-00-00-00) or the non-forwardable multicast MAC address (01-80-C2-00-00-0E) must be used as the destination MAC address. The MAC address in use is selected on a per-port basis through the configuration. However, the non-forwardable multicast MAC address (01-80-C2-00-00-0E) will be used if no destination MAC is configured.

The source MAC address is the interface MAC address.

- For receiving PTP packets, both multicast MAC addresses (01-80-C2-00-00-0E and 01-1B-19-00-00-00) are supported.
- The packet rate for Announce messages is 8 packets-per-second. For Sync, Delay-Req, and Delay-Resp messages, the rate is 16 packets-per-second.
- Signaling and management messages are not used.

PTP Modes

Two-Way Operation

To transport phase and time synchronization and to measure propagation delay, PTP operation must be two-way in this profile. Therefore, only two-way operation is allowed in this profile.

PTP Clocks

Two types of ordinary clocks and boundary clocks are used in this profile:

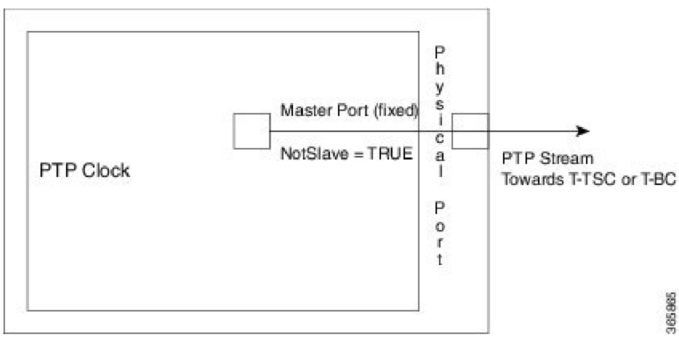
Ordinary Clock (OC)

- OC that can only be a grandmaster clock (T-GM). In this case, one port will be used as master port.

The T-GM uses the frequency, 1PPS, and ToD input from an upstream grandmaster clock.

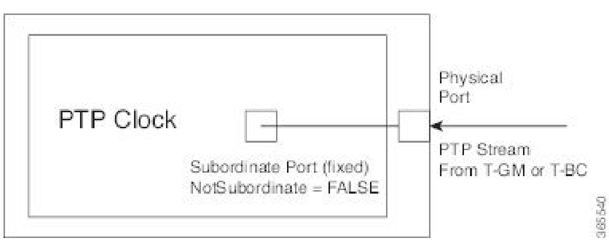
Note The T-GM master port is a fixed master port.

Figure 24: Ordinary Clock As T-GM



- OC that can only be a slave clock (T-TSC). In this case, only one PTP port is used for T-TSC, which in turn will have only one PTP master associated with it.

Figure 25: Ordinary Clock As Slave Clock (T-TSC)

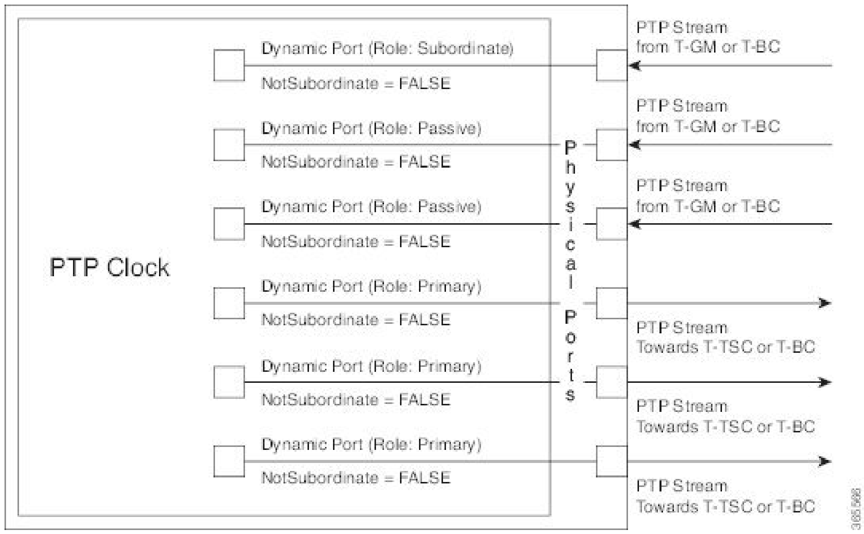


Boundary Clock (T-BC)

1. T-GM in boundary clock is not supported.
2. T-BC that can become a master clock and can also be a slave clock to another PTP clock.

If the BMCA selects a port on the T-BC to be a slave port, all other ports are moved into the master role or a passive state.

Figure 26: Boundary Clock



PTP Ports

A port can be configured to perform either fixed master or slave role or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a master, passive, or slave role based on the BMCA.

A master port provides the clock to its downstream peers.

A slave port receives clock from an upstream peer.

A dynamic port can work either as a master or a slave based on the BMCA decision.

In Cisco's implementation of the G.8275.1:

- OC clocks can support only fixed master or slave port.
- One PTP port can communicate with only one PTP peer.
- The maximum number of clock-ports on a T-BC is limited to the number of 1GE and 10GE interfaces.

Alternate BMCA

The BMCA implementation in G.8275.1 is different from that in the default PTP profile. The G.8275.1 implementation is called the Alternate BMCA. Each device uses the alternate BMCA to select a clock to synchronize to, and to decide the port states of its local ports.

Benefits

With upcoming technologies like LTE-TDD, LTE-A CoMP, LTE-MBSFN and Location-based services, eNodeBs (base station devices) are required to be accurately synchronized in phase and time. Having GNSS systems at each node is not only expensive, but also introduces vulnerabilities. The G.8275.1 profile meets the synchronization requirements of these new technologies.

Prerequisites for Using the G.8275.1 Profile

- PTP over Multicast Ethernet must be used.
- Cisco ASR 901 Router must be enabled using **network-clock synchronization mode QL-enabled** command on T-GM and T-BC.
- Every node in the network must be PTP aware.
- It is mandatory to have a stable physical layer frequency whilst using PTP to define the phase.
- Multiple active grandmasters are recommended for redundancy.

Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.
- SyncE is not compliant with G.8262 when G.8275.1 is enabled.
- Virtual Port is not supported.

Configuring the G.8275.1 Profile

Note To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List.

Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM section in the Clocking and Timing chapter of this book.

Creating a Master-Only Ordinary Clock

```
ptp clock ordinary domain 24
clock-port master master profile g8275.1
transport ethernet multicast interface Gig 0/0
```

Creating an Ordinary Slave

```
ptp clock ordinary domain 24 hybrid
```

```
clock-port slave-port slave profile g8275.1
transport ethernet multicast interface Gig 0/0
```

Creating Dynamic Ports

Note Dynamic ports can be created when you do not specify whether a port is master or slave. In such cases, the BMCA dynamically chooses the role of the port.

```
ptp clock boundary domain 24 hybrid
clock-port bc-port-1 profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0
clock-port bc-port-2 profile g8275.1 local-priority 2
transport ethernet multicast interface Gig 0/1
```

Verifying the Local Priority of the PTP Clock

```
Router# show ptp clock dataset default
CLOCK [Boundary Clock, domain 24]
  Two Step Flag: No
  Clock Identity: 0x2A:0:0:0:58:67:F3:4
  Number Of Ports: 1
  Priority1: 128
  Priority2: 90
  Local Priority: 200
  Domain Number: 24
  Slave Only: No
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

Verifying the Port Parameters

```
Router# show ptp port dataset port
PORT [SERVER]
  Clock Identity: 0x49:BD:D1:0:0:0:0:0
  Port Number: 0
  Port State: Unknown
  Min Delay Req Interval (log base 2): 42
  Peer Mean Path Delay: 648518346341351424
  Announce interval (log base 2): 0
  Announce Receipt Timeout: 2
  Sync Interval (log base 2): 0
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): 0
  PTP version: 2
  Local Priority: 1
  Not-slave: True
```

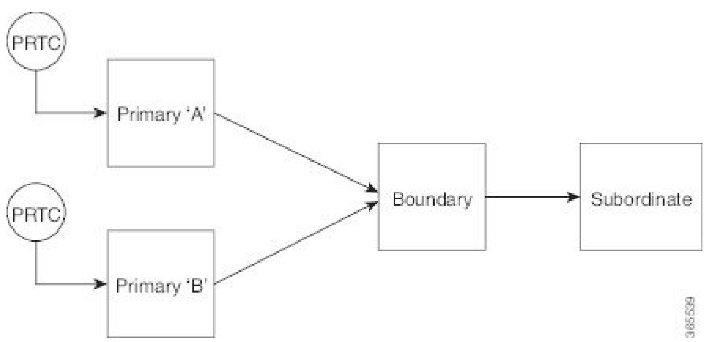
Verifying the Foreign Master Information

```
Router# show ptp clock dataset parent
CLOCK [Boundary Clock, domain 24]

  Parent Clock Identity: 0x3C:8:F6:FF:FE:79:3A:14
  Parent Port Number: 1
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
    Identity: 0x3C:8:F6:FF:FE:79:3A:14
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 58
      Accuracy: Within 25us
      Offset (log variance): 22272
```

G.8275.1 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.1 network with two masters, a boundary clock and a slave. Let's assume that master A is the primary master and B is the backup master.

Figure 27: Topology for a Configuration Example



The configuration on master clock A is:

```
ptp clock ordinary domain 24
  clock-port master master profile g8275.1
    transport ethernet multicast interface GigabitEthernet 0/0
```

The configuration on master clock B is:

```
ptp clock ordinary domain 24
  clock-port master master profile g8275.1
   transport ethernet multicast interface GigabitEthernet 0/1
```

The configuration on the boundary clock is:

```
ptp clock boundary domain 24 hybrid
  local-priority 3
  clock-port slave-port-a profile g8275.1 local-priority 1
```

```
    transport ethernet multicast interface Gig 0/0
  clock-port slave-port-b profile g8275.1 local-priority 2
    transport ethernet multicast interface Gig 0/1
  clock-port master-port profile g8275.1
    transport Ethernet multicast interface Gig 0/2
```

The configuration on the slave clock is:

```
ptp clock ordinary domain 24 hybrid
  clock-port slave-port slave profile g8275.1
    transport Ethernet multicast interface Gig 0/0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Interface and Hardware Component commands	Cisco IOS Interface and Hardware Component Command Reference
Clocking and Timing	Clocking and Timing

Standards

Standard	Title
G.8275.1/Y.1369.1 (07/14)	SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS Packet over Transport aspects – Synchronization, quality and availability targets

MIBs

MIB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
—	There are no new RFCs for this feature.

CHAPTER 23

Cisco IOS IP SLA

The Cisco IOS IP Service Level Agreements (SLAs) is a core part of the Cisco IOS software portfolio, which allows Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages.

The Cisco IOS IP SLAs uses active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. Using Cisco IOS IP SLA, service provider customers can measure and provide SLAs, and enterprise customers can verify service levels, verify out sourced SLAs, and understand network performance.

The Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting.

The Cisco IOS IP SLAs can be accessed using the Cisco IOS CLI or Simple Network Management Protocol (SNMP) through the Cisco Round-Trip Time Monitor (RTTMON) and syslog Management Information Bases (MIBs).

For detailed information on Cisco IOS IP SLA features, see IP SLAs Configuration Guide, Cisco IOS Release 15.1S.

Note Cisco IOS IP SLA for VoIP, ICMP Jitter, Gatekeeper and Data Link Switching Plus (DLSw+) features are not supported in Cisco ASR 901 router.

Configuring IPSLA Path Discovery

The LSP path discovery (LPD) feature allows the IP SLA MPLS LSP to automatically discover all the active paths to the forwarding equivalence class (FEC), and configure LSP ping and traceroute operations across various paths between the provide edge (PE) devices.

Complete the following steps to configure IPSLA path discovery in a typical VPN setup for MPLS LPD operation:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls discoveryvpnnext-hop** **Example:** `Router(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `Router(config)# mpls discovery vpn interval 120`	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the next hop neighbor discovery database of an MPLS VPN.
Step 5	**auto ip slampls-lsp-monitor** *operation-number* **Example:** `Router(config)# auto ip sla mpls-lsp-monitor 1`	Begins configuration for an LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
Step 6	**type echo ipsla-vrf-all** **Example:** `Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`	Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.

What to do next

Configuration Parameters

```
Router(config)#auto ip sla mpls-lsp-monitor 1

Router(config-auto-ip-sla-mpls)#?
Auto IP SLAs MPLS LSP Monitor entry configuration commands:
 exit  Exit IP SLAs MPLSLM configuration
 type  Type of entry
Router(config-auto-ip-sla-mpls)#type ?
 echo      Perform MPLS LSP Ping operation
```

```
 pathEcho  Perform MPLS LSP Trace operation
Router(config-auto-ip-sla-mpls)#type pathEcho ?
 ipsla-vrf-all  Configure IP SLAs MPLS LSP Monitor for all VPNs
 vrf            vrf Name
```

Following parameters can be configured in the **auto-ip-sla-mpls-params** mode:

```
Router(config-auto-ip-sla-mpls)#type echo ipsla-vrf-all
Router(config-auto-ip-sla-mpls-params)#?
IP SLAs MPLSLM entry parameters configuration commands:
 access-list          Apply Access-List
 default              Set a command to its defaults
 delete-scan-factor   Scan Factor for automatic deletion
 exit                 Exit IP SLAs MPLSLM configuration
 exp                  EXP value
 force-explicit-null  force an explicit null label to be added
 lsp-selector         LocalHost address used to select the LSP
 no                   Negate a command or set its defaults
 path-discover        IP SLAs LSP path discover configuration
 reply-dscp-bits      DSCP bits in reply IP header
 reply-mode           Reply for LSP echo request
 request-data-size    Request data size
 scan-interval        Scan Interval for automatic discovery in minutes
 secondary-frequency  Frequency to be used if there is any violation condition
                      happens
 tag                  User defined tag
 threshold            Operation threshold in milliseconds
 timeout              Timeout of an operation
 ttl                  Time to live
```

Following parameters can be configured in the **auto-ip-sla-mpls-lpd-params** mode:

```
Router(config-auto-ip-sla-mpls-params)#path-discover
Router(config-auto-ip-sla-mpls-lpd-params)#?
IP SLAs MPLS LSP Monitor LPD configuration commands:
 default                   Set a command to its defaults
 exit                      Exit IP SLAs MPLS LSP Monitor path discover
                           configuration
 force-explicit-null       Force an explicit null label to be added
 hours-of-statistics-kept  Maximum number of statistics hour groups to capture
 interval                  Send interval between requests in msec
 lsp-selector-base         Base 127/8 address to start the tree trace
 maximum-sessions          Number of concurrent active tree trace requests
                           which can be submit at one time
 no                        Negate a command or set its defaults
 scan-period               Time period for finishing tree trace discovery in
                           minutes
 session-timeout           Timeout value for the tree trace request in seconds
 timeout                   Timeout for an MPLS Echo Request in seconds
```

Example for IPSLA Path Discovery

```
auto ip sla mpls-lsp-monitor 1
type echo ipsla-vrf-all
path-discover
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 1 frequency 10 start-time now
```

This example shows the LPD parameter values configured:

```
auto ip sla mpls-lsp-monitor 2
```

```
type echo vrf vpn1
path-discover
force-explicit-null
hours-of-statistics-kept 1
scan-period 30
lsp-selector-base 127.0.0.7
session-timeout 20
timeout 100
interval 1000
auto ip sla mpls-lsp-monitor schedule 2 schedule-period 1 frequency 10 start-time now
Router#show
 ip sla mpls-lsp-monitor summary

Index                    -  MPLS LSP Monitor probe index
Destination              -  Target IP address of the BGP next hop
Status                   -  LPD group status
LPD Group ID             -  Unique index to identify the LPD group
Last Operation Time      -  Last time an operation was attempted by
                            a particular probe in the LPD Group
Index  Destination     Status     LPD Group ID    Last Operation Time
1      2.2.2.2         up         100004          *20:08:01.481 UTC Tue Nov 14 2000
Router#show
 ip sla mpls-lsp-monitor neighbors

IP SLA MPLS LSP Monitor Database : 1
BGP Next hop 2.2.2.2 (Prefix: 2.2.2.2/32)  OK Paths: 2
  ProbeID: 100004 (pavan_1)
Router# show ip sla mpls-lsp-monitor lpd operational-state
Entry number: 100004
MPLSLM Entry Number: 1
Target FEC Type: LDP IPv4 prefix
Target Address: 2.2.2.2
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *18:00:57.817 UTC Sat Nov 11 2000
Traps Type: 1
Latest Path Discovery Mode: initial complete
Latest Path Discovery Start Time: *20:04:26.473 UTC Tue Nov 14 2000
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 40
Number of Paths Discovered: 2
Path Information :
Path   Outgoing   Lsp             Link  Conn  Adj             NextHop         Downstream
Index  Interface  Selector        Type  Id    Addr            Addr            Label Stack
    Status
1      Vl22       127.0.0.0       90    0     22.1.1.1        22.1.1.1        29
    OK
2      Vl26       127.0.0.0       90    0     26.1.1.2        26.1.1.2        21
    OK
Router# show ip sla mpls-lsp-monitor configuration

Entry Number : 1
Modification time   : *20:19:08.233 UTC Tue Nov 14 2000
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 5000
Threshold(ms)       : 5000
Frequency(sec)      : 10
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100006
Schedule Period(sec): 1
Request size        : 100
```

```
Start Time           : Start Time already passed
SNMP RowStatus       : Active
TTL value            : 255
Reply Mode           : ipv4
Reply Dscp Bits      :
Path Discover        : Enable
    Maximum sessions          : 1
    Session Timeout(seconds)  : 120
    Base LSP Selector         : 127.0.0.0
    Echo Timeout(seconds)     : 5
    Send Interval(msec)       : 1000
    Label Shimming Mode       :
    Number of Stats Hours     : 2
    Scan Period(minutes)      : 1
[Wrap text]  [Edit this enclosure]
Unit-test_IPSLA: Added 12/02/2011 00:05:01 by pacv
[Unwrap text]  [Edit this enclosure]
Unit-test_IPSLA: Added 12/02/2011 00:05:01 by pacv
```

Two-Way Active Measurement Protocol

Two-Way Active Measurement Protocol (TWAMP) consists of two related protocols. Use the TWAMP-Control protocol to start performance measurement sessions. You can deploy TWAMP in a simplified network architecture, with the control-client and the session-sender on one device and the server and the session-reflector on another device.

The Cisco IOS software TWAMP implementation supports a basic configuration. Figure 28: TWAMP Deployment, on page 381 shows a sample deployment.

Figure 29: TWAMP Architecture, on page 382 shows the four logical entities that comprise the TWAMP architecture.

Figure 28: TWAMP Deployment

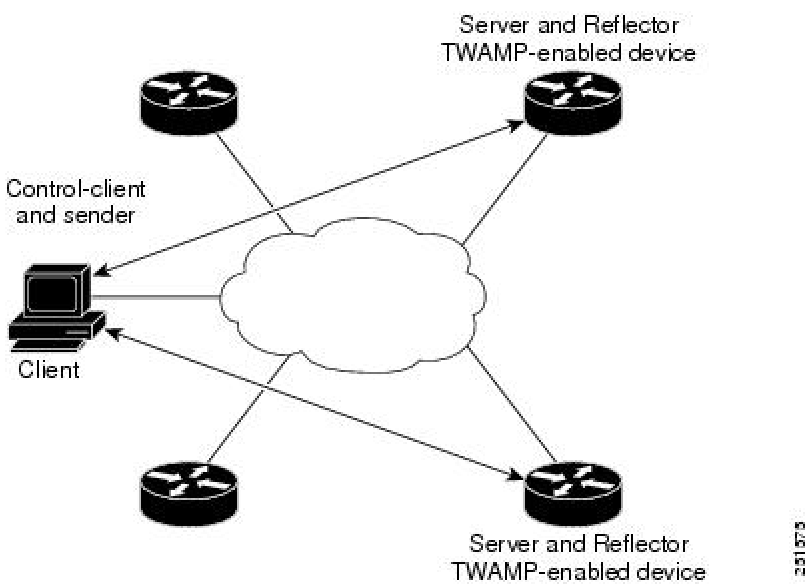
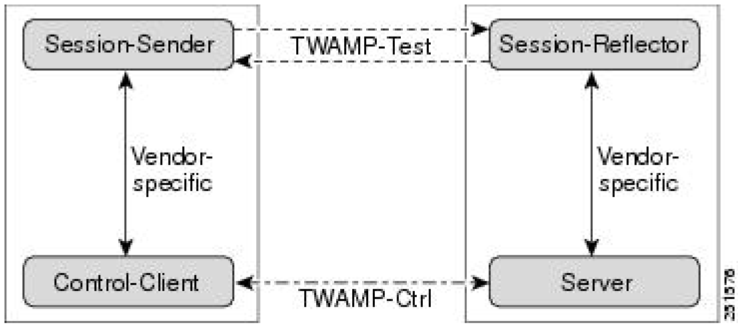


Figure 29: TWAMP Architecture



Although each entity is separate, the protocol allows for logical merging of the roles on a single device.

Configuring TWAMP

The TWAMP server and reflector functionality are configured on the same device. This section contains the following topics:

Configuring the TWAMP Server

Complete the following steps to configure the TWAMP server:

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla server twamp** **Example:** `Router(config)# ip sla server twamp`	Configures the Cisco ASR 901 router as a TWAMP server, and enters TWAMP configuration mode.
Step 4	**port port-number** **Example:** `Router(config-twamp-srvr)# port 9000`	(Optional) Specifies the port number to be used by the TWAMP server to listen for connection and control requests. The same port negotiates for the port to which performance probes are sent. The configured port should not be an IANA port or any port used by other applications. The default is port 862.

	Command or Action	Purpose
Step 5	**timer inactivity seconds** **Example:** `Router(config-twamp-srvr)# timer inactivity 300`	(Optional) Sets the maximum time, in seconds. The session can be inactive before the session ends. The range is between 1 to 6000 seconds. The default is 900 seconds.
Step 6	**end** **Example:** `Router(config-twamp-srvr)# end`	Return to privileged EXEC mode.

Configuring the TWAMP Reflector

To disable the IP SLA TWAMP server, enter the **no ip sla server twamp** global configuration command.

Configuring the TWAMP Reflector

The TWAMP server and reflector functionality are both configured on the same device.

Complete the following steps to configure the TWAMP reflector:

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla server twamp** **Example:** `Router(config)# ip sla server twamp`	Configures the switch as a TWAMP responder, and enter TWAMP configuration mode.
Step 4	**timer inactivity seconds** **Example:** `Router(config-twamp-srvr)# timer inactivity 300`	(Optional) Sets the maximum time, in seconds. The session can be inactive before the session ends. The range is between 1 to 604800 seconds. The default is 900 seconds.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-twamp-srvr)# end`	Return to privileged EXEC mode.

Configuration Examples for TWAMP

This section provides the following configuration examples:

- Example: Configuring the Router as an IP SLA TWAMP server, on page 384
- Example: Configuring the Router as an IP SLA TWAMP Reflector, on page 384

Example: Configuring the Router as an IP SLA TWAMP server

```
Router(config)# ip sla server
twamp
Router(config-twamp-srvr)# port 9000
```

Router(config-twamp-srvr)# **timer inactivity 300**

Example: Configuring the Router as an IP SLA TWAMP Reflector

```
Router(config)# ip sla responder
twamp
```

Router(config-twamp-srvr)# **timeout 300**

CHAPTER 24

Configuring QoS

This chapter describes how to configure quality of service (QoS) by using the modular QoS CLI (MQC) on the Cisco ASR 901 router. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. When QoS is not configured, the router offers the best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput. MQC provides a comprehensive hierarchical configuration framework for prioritizing or limiting specific streams of traffic.

> **Note** IPv6 QoS is supported only from Cisco IOS Release 15.2(2)SNG onwards.

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 Configuring QoS, on page 487.

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.

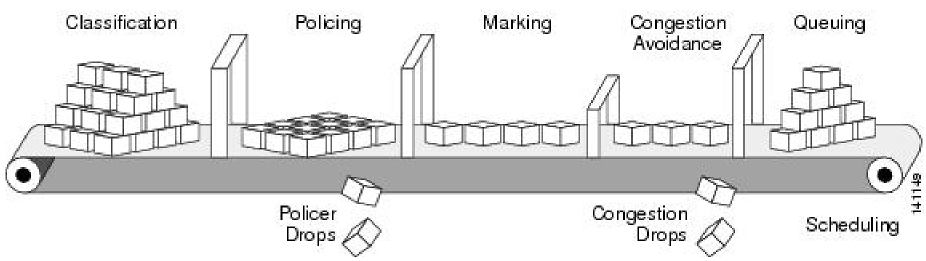
Understanding QoS

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use traffic-management techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

Figure 30: Modular QoS CLI Model, on page 386 shows the MQC QoS CLI model.

Figure 30: Modular QoS CLI Model



Basic QoS includes these actions:

Default QoS for Traffic from External Ethernet Ports

The Cisco ASR 901 router allows complete configuration of QoS via policy maps for the external ethernet ports. However, the default case when no policy map is configured is described below:

By default, the qos-group (internal-priority) applied to every packet from an External port is zero.

In cases where Cisco ASR 901 Router configuration causes those fields that were not present on the incoming packet, (to be generated, for example, if a VLAN tag or an MPLS label that was not present on the incoming packet is added by Cisco ASR 901 Router), the router uses the following default procedures to propagate the priority from the received frame as described below:

In the absence of a policy map, when adding an 802.1Q VLAN outer tag (service tag) when a service tag is not present, the priority value in the outer tag is zero. The priority value of the inner tag (if present) is not modified from its original value.

When adding an 802.1Q VLAN inner tag (customer tag), the default priority value for the inner tag is zero.

The default QoS-group used for internal prioritization, output queuing and shaping, and for propagating QoS information to MPLS EXP, is zero.

For tunneling technologies, such as EoMPLS pseudowires and L3VPN, additional defaults are in place to propagate QoS. These are described below:

- For MPLS-based L3 VPN and for the EoMPLS (both VPWS and VPLS), upon imposition of the first (bottom of stack) MPLS label, ingress policy-map needs to be configured which matches based on COS for EoMPLS & matched based on DSCP for L3VPN and using "set action" of internal QoS group setting (internal priority), MPLS EXP values are set.
- Using table-map on egress port, you can remark the EXP value if required.

Default QoS for Traffic from Internal Ports

The Cisco ASR 901 Router does not allow policy maps to be applied to internal ports, such as the Ethernet or PCI ports to the CPU, or the Ethernet ports to the timing CPU or the Winpath.

The Cisco ASR 901 Router generally treats these internal ports as trusted. The Cisco ASR 901 Router defaults to propagate the priority from the received frame, as described below:

By default, the QoS-group (internal-priority) applied to every packet from an internal port is equal to the priority received in the 802.1Q VLAN tag received on that packet.

If a packet is received on one of the internal interfaces that do not have a VLAN tag attached, a VLAN tag is added internally, with the priority value copied from the ip-precedence field (in case of IP packets), and zero (in case on non-IP packets).

The default QoS-group (internal priority) for internal queue assignment and for propagating QoS information to MPLS EXP, is set equal to the priority of the outer VLAN tag (either the original or the default value) on the received frame.

For tunneling technologies, such as EoMPLS pseudowires and L3VPN, additional defaults are in place to propagate QoS as follows:

- For MPLS-based L3 VPN and for the EoMPLS (both VPWS and VPLS), upon imposition of the first (bottom of stack) MPLS label, MPLS EXP values are equal to the value is specified in the internal QoS group setting (internal priority).
- When adding additional MPLS labels to an existing stack, the default MPLS EXP values are set to the match QoS group value.

This section contains the following topics:

Modular QoS CLI

Modular QoS CLI (MQC) allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. Use a traffic class to classify traffic, and the QoS features in the traffic policy determine how to treat the classified traffic.

Complete the following steps to configure Modular QoS CLI:

Procedure

Step 1 Define a traffic class.

Use the **class-map** [**match-all** | **match-any**] *type number* global configuration command to define a traffic class and to enter class-map configuration mode. A traffic class contains three elements: a name, an instruction on how to evaluate the configured **match** commands (if more than one match command is configured in the class map), and a series of **match** commands

- Name the traffic class in the **class-map** command line to enter class-map configuration mode.
- You can optionally include keywords to evaluate these match commands by entering **class-map match-any** or **class-map match-all**. If you specify **match-any**, the traffic being evaluated must match *type number*of the specified criteria. If you specify **match-all**, the traffic being evaluated must match *type number*of the specified criteria. A **match-all** class map can contain only one match statement, but a **match-any** class map can contain multiple match statements.

Note

If you do not enter **match-all** or **match-any**, the default is to match all.

- Use the **policy-map** class-map configuration commands to specify criteria for classifying packets. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Step 2 Create a traffic policy to associate the traffic class with one or more QoS features.

Use the **policy-map***type number* global configuration command to create a traffic policy and to enter policy-map configuration mode. A traffic policy defines the QoS features to associate with the specified traffic class. A traffic policy contains three elements: a name, a traffic class (specified with the **class** policy-map configuration command), and the QoS policies configured in the class.

- Name the traffic policy in the **policy-map** command line to enter policy-map configuration mode.
- In policy-map configuration mode, enter the name of the traffic class used to classify traffic to the specified policy, and enter policy-map class configuration mode.
- In policy-map class configuration mode, you can enter the QoS features to apply to the classified traffic. These include using the **set**, **police**, or **police aggregate** commands for input policy maps or the **bandwidth**, **priority**, or **shape average** commands for output policy maps.

Note
A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy is used. To configure more than one match criterion for packets, you can associate multiple traffic classes with a single traffic policy.

Step 3 Attach the traffic policy to an interface.

Use the **service-policy** interface configuration command to attach the policy map to an interface for packets entering or leaving the interface. You must specify whether the traffic policy characteristics should be applied to incoming or outgoing packets. For example, entering the **service-policy output class1** interface configuration command attaches all the characteristics of the traffic policy named *type number* to the specified interface. All packets leaving the specified interface are evaluated according to the criteria specified in the traffic policy named *type number*.

Note
If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. For example: Warning: Detaching Policy test1 from Interface GigabitEthernet0/1 The policy map is then detached and deleted.

Input and Output Policies

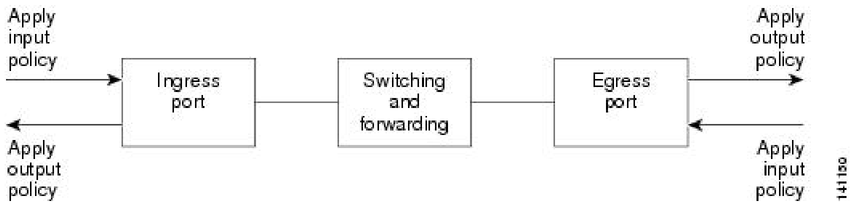
Policy maps are either input policy maps or output policy maps, attached to packets as they enter or leave the router by service policies applied to interfaces. Input policy maps perform policing and marking on the received traffic. Policed packets can be dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps perform scheduling and queuing of traffic as it leaves the router.

Input policies and output policies have the same basic structure; the difference is in the characteristics that they regulate. Figure 31: Input and Output Policy Relationship, on page 389 shows the relationship of input and output policies.

You can configure a maximum of 32 policy maps.

You can apply one input policy map and one output policy map to an interface.

Figure 31: Input and Output Policy Relationship



Input Policy Maps

Input policy map classification criteria include matching a CoS, a DSCP, or an IP precedence value or VLAN ID (for per-port and per-VLAN QoS). Input policy maps can perform any of these actions:

- Setting or marking a CoS, a DSCP, an IP precedence, or QoS group value
- Individual policing
- Aggregate policing

Only input policies provide matching on VLAN IDs, and only output policies provide matching on QoS groups. You can assign a QoS group number in an input policy and match it in the output policy. The **class-default** class is used in a policy map for any traffic that does not explicitly match any other class in the policy map. Input policy maps do not support queuing and scheduling keywords, such as **bandwidth**, **priority**, and **shape average**.

An input policy map can have a maximum of 64 classes plus **class-default**. You can configure a maximum of 64 classes in an input policy.

Output Policy Maps

Output policy map classification criteria include matching a CoS, a DSCP, an IP precedence, or a QoS group value. Output policy maps support scheduling of **bandwidth**, **priority**, and **shape average**.

Output policy maps do not support matching of access groups. You can use QoS groups as an alternative by matching the appropriate access groups in the input policy map and setting a QoS group. In the output policy map, you can then match the QoS group. For more information, see the Classification Based on QoS Groups, on page 394.

Output policies do not support policing, except in the case of priority with policing.

The **class-default** class is used in a policy map for any traffic that does not explicitly match any other class in the policy map.

An output policy map attached to an egress port can match only the packets that have already been matched by an input policy map attached to the ingress port for the packets. You can attach an output policy map to any or all the ports on the router. The router supports configuration and attachment of a unique output policy map for each port. There are no limitations on the configurations of bandwidth, priority, or shaping.

Access Control Lists

Cisco IOS Release 15.2(2)SNH1 introduces support for access control list-based QoS on the Cisco ASR 901 Router. This feature provides classification based on source and destination IP. The current implementation of this feature supports only the named ACLs. Effective from Cisco IOS Release 15.4 (2) S, the Cisco ASR 901 Router supports IPv6 addresses in ACLs.

ACLs are an ordered set of filter rules. Each rule is a permit or a deny statement known as access control entry (ACE). These ACEs filter network traffic by forwarding or blocking routed packets at the interface of the router. The router examines each packet to determine whether to forward or drop the packets based on the criteria specified within the access list.

The permit and deny statements are not applicable when ACLs are used as part of ACL-based QoS. ACLs are used only for traffic classification purposes as part of QoS.

Restrictions

- The Loopback feature should not be enabled when Layer 2 Control Protocol Forwarding is enabled.
- The following Cisco IOS Keywords are not supported on the Cisco ASR 901 Router—**match-any**, **ip-options**, **logging**, **icmp-type/code**, **igmp type**, **dynamic**, **reflective**, **evaluate**. The **icmp-type/code** keyword is supported from Cisco IOS Release 15.5(2)S, as part of the support for ICMP based ACL feature.
- Ingress PACL and RACL support TCP/UDP port range; egress ACLs are not supported.
- Sharing access lists across interfaces is not supported.
- ACLs are not supported on management port (Fast Ethernet) and serial interfaces.
- Devices in the management network (network connected to the Fast Ethernet port) cannot be accessed from any other port. If the default route is configured on the Cisco ASR 901 to fast ethernet interface (Fa0/0), all the routed packets will be dropped. However, this configuration could keep the CPU busy and affect overall convergence.
- Compiled ACLs are not supported in Cisco ASR 901 Router.
- ACLs are not supported on EVC interfaces.
- ACLs are not supported on interface loopback interfaces.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the router examines the header and identifies all the key packet fields. A packet can be classified based on the DSCP, the CoS, or the IP precedence value in the packet, or by the VLAN ID. Figure 32: QoS Classification Layers in Frames and Packets, on page 391 shows the classification information carried in a Layer 2 or a Layer 3 IP packet header, using six bits from the deprecated IP type of service (ToS) field to carry the classification information.

The classification information carried in a Layer 2 or Layer 3 IP packet is as follows:

- On ports configured as Layer 2 IEEE 802.1Q trunks, all the traffic is in 802.1Q frames except for traffic in the native VLAN. Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value, called the User Priority bits, in the three most-significant bits, and the VLAN ID value in the 12 least-significant bits. Other frame types cannot carry Layer 2 CoS values.

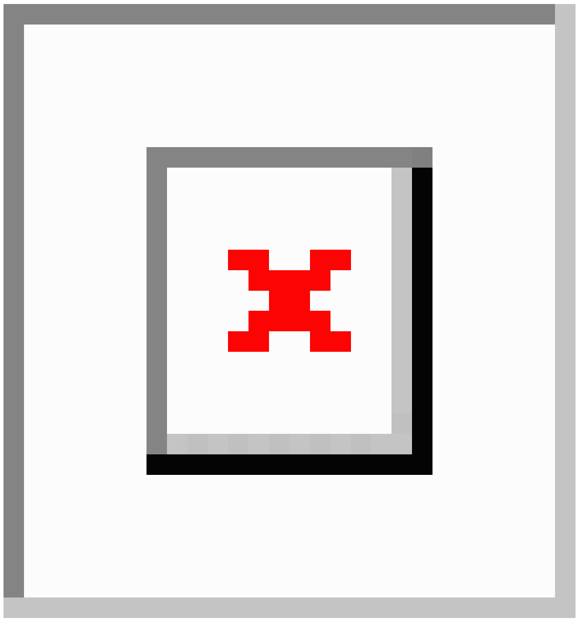
Layer 2 CoS values range from 0 to 7.

- Layer 3 IP packets can carry either an IP precedence value or a DSCP value. QoS supports the use of either value because DSCP values are backward compatible with IP precedence values.

IP precedence values range from 0 to 7. DSCP values range from 0 to 63.

- Output re-marking is based on the Layer 2 or Layer 3 marking type, marking value, and packet type.

Figure 32: QoS Classification Layers in Frames and Packets



These sections contain additional information about classification:

Class Maps

Use an MQC class map to name a specific traffic flow (or class) and to isolate it from all other traffic. A class map defines the criteria used to match against a specific traffic flow to further classify it. If you wish to classify more than one type of traffic, you can create another class map and use a different name. When you use the **class-map** command with a class-map name, the router enters the class-map configuration mode. In this mode, you define the match criteria for the traffic by using the **match class-map** configuration command. After a packet is matched against the class-map criteria, it is acted on by the associated action specified in a policy map.

You can match more than one criterion for classification. You can also create a class map that requires that all the matching criteria in the class map be in the packet header by using the **class map match-all** *class-map name* global configuration command and enter class map configuration mode.

Note You can configure only one match entry in the **match-all** class map.

You can use the **class map match-any** *class-map name* global configuration command to define a classification with any of the listed criteria.

Note If you do not enter **match-all** or **match-any** , the default is to match all. A match-all class map cannot have more than one classification criterion (match statement). A class map with no match condition has a default of match all.

The match Command

To configure the type of content used to classify packets, use the **match** class-map configuration command to specify the classification criteria. If a packet matches the configured criteria, it belongs to a specific class and is forwarded according to the specified policy. For example, you can use the **match** class-map command with CoS, IP DSCP, and IP precedence values. These values are referred to as *markings* on a packet.

- For an input policy map, you cannot configure an IP classification (**match ip dscp**, **match ip precedence**, **match ip acl**) and a non-IP classification (**match cos** or **match mac acl**) in the same policy map or class map.
- In an output policy map, no two class maps can have the same classification criteria, that is, the same match qualifiers and values.

This example shows how to create a class map *example* to define a class that matches any of the listed criteria. In this example, if a packet is received with the DSCP equal to 32 or a 40, the packet is identified (classified) by the class map.

```
Router(config)# class-map match-any example
Router(config-cmap)# match ip dscp 32
Router(config-cmap)# match ip dscp 40
Router(config-cmap)# exit
```

Classification Based on Layer 2 CoS

You can use the **match** command to classify Layer 2 traffic based on the CoS value, which ranges from 0 to 7.

Note A match cos command is supported only on Layer 2 802.1Q trunk ports.

This example shows how to create a class map to match a CoS value of 5:

```
Router(config)# class-map premium
Router(config-cmap)# match cos 5
Router(config-cmap)# exit
```

Classification Based on IP Precedence

You can classify IPv4 traffic based on the packet IP precedence values, which range from 0 to 7.

This example shows how to create a class map to match an IP precedence value of 4:

```
Router(config)# class-map sample
Router(config-cmap)# match ip precedence 4
Router(config-cmap)# exit
```

Classification Based on IP DSCP

When you classify IPv4 traffic based on the IP DSCP value, and enter the **match ip dscp** class-map configuration command, you have several classification options to choose from:

- Entering a specific DSCP value (0 to 63).
- Using the Default service, that corresponds to an IP precedence and DSCP value of 0. The default per-hop behavior (PHB) is usually best-effort service.

- Using Assured Forwarding (AF) by entering the binary representation of the DSCP value. AF sets the relative probability that a specific class of packets is forwarded when congestion occurs and the traffic does not exceed the maximum permitted rate. AF *per-hop behavior* provides delivery of IP packets in four different AF classes: AF11-13 (the highest), AF21-23, AF31-33, and AF41-43 (the lowest). Each AF class can be allocated a specific amount of buffer space and drop probabilities, specified by the binary form of the DSCP number. When congestion occurs, the drop precedence of a packet determines the relative importance of the packet within the class. An AF41 provides the best probability of a packet being forwarded from one end of the network to the other.
- Entering Class Selector (CS) service values of 1 to 7, corresponding to the IP precedence bits in the ToS field of the packet.
- Using Expedited Forwarding (EF) to specify a low-latency path. This corresponds to a DSCP value of 46. EF services use priority queuing to preempt lower-priority traffic classes.

This example shows the available classification options:

```
Router(config-cmap)# match ip dscp ?
  <0-63>    Differentiated services codepoint value
  af11      Match packets with AF11 dscp (001010)
  af12      Match packets with AF12 dscp (001100)
  af13      Match packets with AF13 dscp (001110)
  af21      Match packets with AF21 dscp (010010)
  af22      Match packets with AF22 dscp (010100)
  af23      Match packets with AF23 dscp (010110)
  af31      Match packets with AF31 dscp (011010)
  af32      Match packets with AF32 dscp (011100)
  af33      Match packets with AF33 dscp (011110)
  af41      Match packets with AF41 dscp (100010)
  af42      Match packets with AF42 dscp (100100)
  af43      Match packets with AF43 dscp (100110)
  cs1       Match packets with CS1(precedence 1) dscp (001000)
  cs2       Match packets with CS2(precedence 2) dscp (010000)
  cs3       Match packets with CS3(precedence 3) dscp (011000)
  cs4       Match packets with CS4(precedence 4) dscp (100000)
  cs5       Match packets with CS5(precedence 5) dscp (101000)
  cs6       Match packets with CS6(precedence 6) dscp (110000)
  cs7       Match packets with CS7(precedence 7) dscp (111000)
  default   Match packets with default dscp (000000)
  ef        Match packets with EF dscp (101110)
```

Note For more information on DSCP prioritization, see RFC-2597 (AF per-hop behavior), RFC-2598 (EF), or RFC-2475 (DSCP).

Classification Comparisons

Table 20: Typical Traffic Types , on page 393 shows the recommended IP DSCP, IP precedence, and CoS values for typical traffic types.

Table 20: Typical Traffic Types

Traffic Type	DSCP Per-Hop	DSCP (Decimal)	IP Precedence	CoS
Voice-bearer—Traffic in a priority queue or the queue with the highest service weight and lowest drop priority.	EF	46	5	5

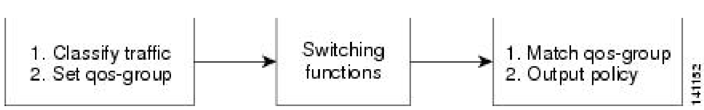
Traffic Type	DSCP Per-Hop	DSCP (Decimal)	IP Precedence	CoS
Voice control—Signalling traffic related to call setup from a voice gateway or a voice application server.	AF31	26	3	3
Video conferencing—In most networks, video conferencing over IP has similar loss, delay, and delay variation requirements as Voice over IP traffic.	AF41	34	4	4
Streaming video—Relatively high bandwidth applications with a high tolerance for loss, delay, and delay variation. Usually considered more important than regular background applications such as e-mail and web browsing.	AF13	14	1	1
Mission-critical date (gold data)—Delay-sensitive applications critical to the operation of an enterprise, classified as: • Level 1 • Level 2 • Level 3	AF21 AF22 AF23	18 20 22	2 2 2	2 2 2
Less critical data (silver data)—Noncritical, but relatively important data, classified as: • Level 1 • Level 2 • Level 3	AF11 AF12 AF13	10 12 14	1 1 1	1 1 1
Best-effort data (bronze data)—Other traffic, including all the noninteractive traffic, regardless of importance.	Default	0	0	0
Less-than-best-effort data—Noncritical, bandwidth-intensive data traffic given the least preference. This is the first traffic type to be dropped, and includes these levels: • Level 1 • Level 2 • Level 3	—	2 4 6	0 0 0	0 0 0

Classification Based on QoS Groups

A QoS group is an internal label used by the router to identify packets as a members of a specific class. The label is not a part of the packet header, and is restricted to the router that sets the label. QoS groups provide a way to tag a packet for subsequent QoS action without explicitly marking (changing) the packet.

A QoS group is identified at ingress and used at egress; it is assigned in an input policy to identify packets in an output policy (see Classification Based on QoS Groups, on page 394). The QoS groups help aggregate different classes of input traffic for a specific action in an output policy.

Figure 33: QoS Groups



You can use QoS groups to aggregate multiple input streams across input classes and policy maps for the same QoS treatment on the egress port. Assign the same QoS group number in the input policy map to all the streams that require the same egress treatment, and match the QoS group number in the output policy map to specify the required queuing and scheduling actions.

You can also use QoS groups to identify traffic entering a particular interface if the traffic has to be treated differently at the output based on the input interface.

You can use QoS groups to configure per-port, per-VLAN QoS output policies on the egress interface for bridged traffic on the VLAN. Assign a QoS group number to a VLAN on the ingress interface by configuring a per-port, per-VLAN input policy. Then use the same QoS-group number for classification at the egress. Because the VLAN of the bridged traffic does not change during forwarding through the router, the QoS-group number assigned to the ingress VLAN can be used on the egress interface to identify the same VLAN.

You can independently assign QoS-group numbers at the ingress to any combination of interfaces, VLANs, traffic flows, and aggregated traffic. To assign QoS-group numbers, configure a QoS group marking in an input policy map, along with any other marking or policing actions required in the input policy map for the same service class. This allows the input marking and policing functions to be decoupled from the egress classification function if necessary because only the QoS group must be used for egress classification.

This example identifies specific packets as part of QoS group 1 for later processing in an output policy:

```
Router(config)# policy-map in-gold-policy
Router(config-pmap)# class in-class1
Router(config-pmap-c)# set qos-group 1
Router(config-cmap-c)# exit
Router(config-cmap)# exit
```

Use the **set qos-group** command only in an input policy. The assigned QoS group identification is subsequently used in an output policy with no mark or change to the packet. Use the **match qos-group** in the output policy.

Note You cannot configure **match qos-group** for an input policy map.

This example shows how to create an output policy to match the QoS group created in the input policy map *in-gold-policy* . Traffic that is internally tagged as *qos-group 1* is identified and processed by the output policy.

```
Router(config)# class-map out-class1
Router(config-cmap)# match qos-group 1
Router(config-cmap)# exit
```

Classification Based on VLAN IDs

With classification based on VLAN IDs, you can apply QoS policies to frames carried on a user-specified VLAN for a given interface. Per-VLAN classification is not required on access ports because access ports carry traffic for a single VLAN.

The router supports two policy levels: a *parent* level and a *child* level. With the QoS parent-child structure, you can reference a child policy in a parent policy to provide additional control of a specific traffic type. For per-port, per-VLAN QoS, the parent-level matches the VLAN; match criteria is defined by the service instance encapsulation. You cannot configure multiple service classes at the parent level to match different combinations of VLANs.

Note A per-port, per-VLAN parent-level class map supports only the **class-default** class; you should configure with a single rate policer. A flat policy can have multiple classes with match VALN and any action.

Note You can configure only class default in the parent level of a per-port, per-VLAN hierarchical policy map.

In this example, the class maps in the child-level policy map specify the matching criteria for voice, data, and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Router(config)# class-map match-any dscp-1 data
Router(config-cmap)# match ip dscp 1
Router(config-cmap)# exit
Router(config)# class-map match-any dscp-23 video
Router(config-cmap)# match ip dscp 23
Router(config-cmap)# exit
Router(config)# class-map match-any dscp-63 voice
Router(config-cmap)# match ip dscp-63
Router(config-cmap)# exit
Router(config)# policy-map customer-1-ingress
Router(config-pmap)# class class-default
Router(config-pmap-c)# service-policy child_policy-1
```

Note You can also enter the match criteria as **match vlan 100 200 300** in the child-level policy map.

```
Router(config)# policy-map child policy-1
Router(config-pmap)# class dscp-63 voice
Router(config-pmap-c)# police cir 10000000 bc 50000
Router(config-pmap-c)# conform-action set-cos-transmit 5
Router(config-pmap-c)# exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# class dscp-1 data
Router(config-pmap-c)# set cos 0
Router(config-pmap-c)# exit
Router(config-pmap)# class dscp-23 video
Router(config-pmap-c)# set cos 4
Router(config-pmap-c)# set ip precedence 4
Router(config-pmap-c)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service instance 100 ethernet
Router(config-if)# encapsulation dot1q 100
Router(config-if)# service-policy input customer-1-ingress
Router(config-if)# rewrite ingress tag pop 1 symmetric
Router(config-if)# bridge-domain 100
```

Classification Based on ACL

Effective with Cisco IOS Release 15.4 (2) S, the Cisco ASR 901 Router supports ACL-based QoS on Layer 4. This feature allows you to configure the Layer 3 or Layer 4 options while configuring the ACL for QoS on ingress only. Layer 3 or Layer 4 options such as ToS, source port, and destination port are supported.

The following example shows a sample configuration for ACL-based QoS on Layer 4:

```
ip access-list extended test
permit tcp any any
permit udp any any
class-map test
match access-group name test
policy-map test
class test
set dscp af11
interface gig 0/3
ip access-group test in
```

Restrictions

- Only named ACLs are supported in Layer 4 ACL-based QoS.
- The not operation is not supported in Layer 4 ACL-based QoS.
- Layer 4 ACL-based QoS is not supported on a multilink interface and BCPoMLPPP.

Table Maps

You can use table maps to manage a large number of traffic flows with a single command. You can specify table maps in the **set** commands and use them as mark-down mapping for the policers. You can also use table maps to map an incoming QoS marking to a replacement marking without having to configure a large number of explicit matches and sets. Table maps are used only in input policy maps.

Table maps can be used to:

- Correlate specific CoS, DSCP, or IP precedence values to specific CoS, DSCP, or IP precedence values
- Mark down a CoS, DSCP, or IP precedence value
- Assign defaults for unmapped values

This example shows how to create a table to map specific CoS values to DSCP values. The unspecified values are all mapped to a to-value (0).

```
Router(config)# table-map cos-dscp-tablemap
Router(config-tablemap)# map from 5 to 46
Router(config-tablemap)# map from 6 to 56
Router(config-tablemap)# map from 7 to 57
Router(config-tablemap)# exit
```

The Cisco ASR 901 Router supports a maximum of 32 unique table maps. You can enter up to 64 different **map from–to** entries in a table map. These table maps are supported on the router:

- Cos to QoS-group
- QoS-group to mpls experimental topmost

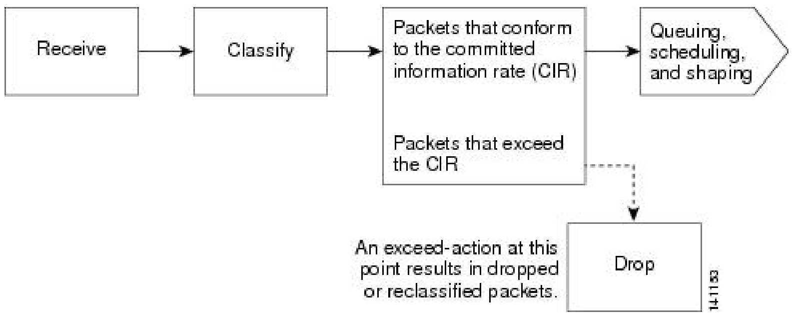
Table maps modify only one parameter (CoS, IP precedence, or DSCP, whichever is configured) and are only effective when configured with a **set** command in a policy map.

Policing

After a packet is classified, you can use policing, as shown in Figure 34: Policing of Classified Packets, on page 398 to regulate the class of traffic. The policing function limits the amount of bandwidth available to a specific traffic flow or prevents a traffic type from using excessive bandwidth and system resources. A policer identifies a packet as being in or out of profile by comparing the rate of the inbound traffic to the configuration profile of the policer and traffic class. Packets that exceed the permitted average rate or burst rate are *out of profile* or *nonconforming* . These packets are dropped or modified (marked for further processing), depending on the policer configuration.

Policing is used primarily on the receiving interfaces. You can attach a policy map to a policer only in an input service policy. The only policing allowed in an output policy map is in priority classes (see the Unconditional Priority Policing, on page 400).

Figure 34: Policing of Classified Packets



This section contains the following topics:

Individual Policing

Individual policing applies only to input policy maps. In the policy-map configuration mode, use the **class** command followed by the class map name, and enter the policy-map class configuration mode. Effective Cisco IOS Release 15.3(3)S, the Cisco ASR 901 Router supports policing ingress traffic over the cross-connect EVC, similar to the bridge domain service policy.

Use the **police** policy-map class configuration command to define the policer, the committed rate limitations of the traffic, committed burst size limitations of the traffic, and the action to take for a class of traffic that is below the limits (**conform-action**) and above the limits (**exceed-action**). If you do not specify burst size (bc), the system calculates an appropriate burst size value. The calculated value is appropriate for most applications.

To make the policy map effective, attach it to a physical port by using the **service-policy input** interface configuration command. Policing is done only on received traffic, so you can only attach a policer to an input service policy.

Note The QoS group precedes the CoS value that is matched in the class map, when the set qos-group command is used along with MPLS experimental imposition.

Restrictions

- Only byte counters are supported.
- Only drop and pass counters are supported.
- If an ingress cross-connect policer is attached to a physical interface, an ingress cross-connect policer cannot be attached to EVCs under the specific physical port.

- Applying or removing a policy-map on a cross-connect interface requires **shutdown** or **no shutdown** on the interface.
- User class-based MPLS experimental imposition is supported only for user classes based on CoS match.
- Only policy maps on 254 ingress cross-connect interfaces are supported.
- Dynamic modification of policy maps (modifying a policy map or a class map while it is attached to an interface) is not supported for the policy maps applied on cross-connect.
- The match cos inner is not supported.

Configuration Examples

The following is a sample configuration of basic policing for all the traffic received with a CoS of 4. The first value following the **police** command limits the average traffic rate to 10, 000,000 bits per second (bps); the second value represents the additional burst size (10 kilobytes). The policy is assigned to Gigabit Ethernet port 1.

```
Router(config)# class-map video-class
Router(config-cmap)# match cos 4
Router(config-cmap)# exit
Router(config)# policy-map video-policy
Router(config-pmap)# class video-class
Router(config-pmap-c)# police 10000000 10000
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input video-policy
Router(config-if)# exit
```

The following is a sample configuration that shows the policing of traffic over cross-connect EVC:

```
Router(config)# interface GigabitEthernet0/3
Router(config-if)# service instance 22 ethernet
Router(config-if-svr)# encapsulation dot1q 22
Router(config-if-svr)# rewrite ingress tag pop 1 symmetric
Router(config-if-svr)# xconnect 1.1.1.1 100 encapsulation mpls
Router(config-if-svr)# service-policy input policy1
```

Router(config-if-svr)# exit

You can use the **conform-action** and **exceed-action** policy-map class configuration commands or the **conform-action** and **exceed-action** policy-map class police configuration commands to specify the action to be taken when a packet conforms to or exceeds the specified traffic rate.

Conform actions involve sending the corresponding packet without modifications, setting a new CoS, DSCP, or IP precedence value, or setting up a QoS group value for classification at the egress. Exceed actions involve dropping the packet, sending the packet without modification, setting a new CoS, DSCP, or IP precedence to a value, or setting a QoS group value for classification at the egress.

You can configure each marking action by using explicit values, table maps, or a combination of both. Table maps list specific traffic attributes and map (or convert) them to other attributes.

You can configure multiple conform and exceed actions simultaneously for each service class.

After you create a table map, configure a policy-map policer to use the table map.

Note In Cisco ASR 901 router, the **from**–type action in the table map must be **cos**.

To configure multiple actions in a class, you can enter multiple conform or exceed action entries in the policy-map class police configuration mode, as in this example:

```
Router(config)# policy-map map1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 100000 500000
Router(config-pmap-c-police)# conform-action set-cos-transmit 4
Router(config-pmap-c-police)# conform-action set-qos-transmit 4
Router(config-pmap-c-police)# exceed-action set-cos-transmit 2
Router(config-pmap-c-police)# exceed-action set-qos-transmit 2
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Unconditional Priority Policing

Priority policing applies only to output policy maps. You can use the **priority** policy-map class configuration command in an output policy map to designate a low-latency path or class-based priority queuing for a specific traffic class. With strict priority queuing, the packets in the priority queue are scheduled and sent until the queue is empty, at the expense of other queues. Excessive use of high-priority queuing may create congestion for lower-priority traffic.

To eliminate this congestion, you can use priority with implicit policer (priority policing) to reduce the bandwidth used by the priority queue, and allocate traffic rates on other queues. Priority with police is the only form of policing supported in output policy maps.

Note You cannot configure a policer-committed burst size for an unconditional priority policer because any configured burst size is ignored.

This example shows how to use the **priority percent** command to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20,000,000 bps so that the priority queue never uses more than that. Traffic above that rate is dropped. This allows other traffic queues to receive some port bandwidth, in this case, a minimum bandwidth guarantee of 50 percent and 20 percent. The **class-default** class queue gets the remaining port bandwidth.

```
Router(config)# policy-map policy1
Router(config-pmap)# class out-class1
Router(config-pmap-c)# priority percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class2
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class3
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

Egress Policing

Egress policing can be classified based on QoS groups, DSCP, and IP precedence value. For QoS groups to work at egress, you should map the traffic at ingress to a specific QoS group value.

Marking

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. After network traffic is organized into classes, you use marking to identify certain traffic types for unique handling. For example, you can change the CoS value in a class or set IP DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated. You can also use marking to assign traffic to a QoS group within the router.

Traffic marking is typically performed on a specific traffic type at the ingress port. The marking action can cause the CoS, DSCP, or precedence bits to be rewritten or left unchanged, depending on the configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet. The marking function can use information from the policing function or directly from the classification function.

You can specify and mark traffic by using the **set** commands in a policy map for all supported QoS markings (CoS, IP DSCP, IP precedence, and QoS groups). A **set** command unconditionally *marks* the packets that match a specific class. You then attach the policy map to an interface as an input policy map.

You can also mark traffic by using the **set** command with table maps. Table maps list specific traffic attributes and maps (or converts) them to another attribute. A table map establishes a to-from relationship for the attribute and defines the change to be made.

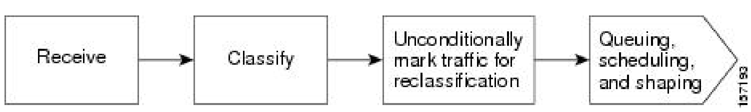
You can simultaneously configure actions to modify DSCP, precedence, and COS markings in the packet for the same service along with QoS group marking actions. You can use the QoS group number defined in the marking action for egress classification.

Note When you use a table map in an input policy map, the protocol type of the **from**-type action in the table map must be the same as the protocol type of the associated classification. If the class map represents a non-IP classification, the **from**-type action in the table map must be **cos**.

Note Cisco ASR 901 transparently preserves the ECN bits while marking DSCP.

After you create a table map, configure a policy map to use the table map. See the Congestion Management and Scheduling, on page 402. Figure 35: Marking of Classified Traffic , on page 401 shows the steps for marking traffic.

Figure 35: Marking of Classified Traffic



This example uses a policy map to remark a packet. The first marking (the **set** command) applies to the QoS default class map that matches all traffic not matched by class *AF31-AF33* and sets all traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

```
Router(config)# policy-map Example
Router(config-pmap)# class class-default
Router(config-pmap-c)# set ip dscp 1
Router(config-pmap-c)# exit
Router(config-pmap)# class AF31-AF33
Router(config-pmap-c)# set ip dscp 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy input Example
Router(config-if)# exit
```

Congestion Management and Scheduling

Cisco Modular QoS CLI (MQC) provides several related mechanisms to control outgoing traffic flow. They are implemented in output policy maps to control output traffic queues. The scheduling stage holds packets until the appropriate time to send them to one of the four traffic queues. Queuing assigns a packet to a particular queue based on the packet class. You can use different scheduling mechanisms to provide a guaranteed bandwidth to a particular class of traffic while also serving other traffic in a fair way. You can limit the maximum bandwidth that can be consumed by a particular class of traffic and ensure that delay-sensitive traffic in a low-latency queue is sent before traffic in other queues.

The Cisco ASR 901 Router supports these scheduling mechanisms:

- Traffic shaping

Use the **shape average** policy-map class configuration command to specify that a class of traffic should have a maximum permitted average rate. Specify the maximum rate in bits per second.

- Class-based weighted fair queuing (CBWFQ)

Use the **bandwidth** policy-map class configuration command to control the bandwidth allocated to a specific class. The minimum bandwidth can be specified as percentage.

- Priority queuing or class-based priority queuing

Use the **priority** policy-map class configuration command to specify the priority of a type of traffic over other types of traffic. You can specify strict priority for high-priority traffic and allocate excess bandwidth, if any, to other traffic queues, or specify priority with unconditional policing of high-priority traffic, and allocate the known remaining bandwidth among the other traffic queues.

- To configure strict priority, use only the **priority** policy-map class configuration command to configure the priority queue. Use the **bandwidth remaining percent** policy-map class configuration command for the other traffic classes to allocate the excess bandwidth in the desired ratios.
- To configure priority with unconditional policing, configure the priority queue by using the **priority** policy-map class configuration command and the **police** policy-map class configuration command to unconditionally rate-limit the priority queue. In this case, you can configure the other traffic classes with the **bandwidth** command or the **shape average** command, depending on your requirements

These sections contain additional information about scheduling:

Traffic Shaping

Traffic shaping is a traffic-control mechanism similar to traffic policing. While traffic policing is used in input policy maps, traffic shaping occurs as traffic leaves an interface. The router can apply class-based shaping to classes of traffic leaving an interface, and port shaping to all the traffic leaving an interface. Configuring a queue for traffic shaping sets the maximum bandwidth or peak information rate (PIR) of the queue.

Note Effective Cisco IOS Release 15.2(2)SNI, the lower limit of the committed burst size (bc) is 1 ms.

Class-Based Shaping

Class-based shaping uses the **shape average** policy-map class configuration command to limit the rate of data transmission as the number of bits per second to be used for the committed information rate for a class of traffic. The router supports separate queues for three classes of traffic. The fourth queue is always the default queue for the **class-default** class, unclassified traffic.

Note In the Cisco ASR 901 Router, configuring traffic shaping automatically sets the minimum bandwidth guarantee or committed information rate (CIR) of the queue to the same value as the PIR.

This example shows how to configure traffic shaping for outgoing traffic on a Gigabit Ethernet port so that *outclass1* , *outclass2* , and *outclass3* get a maximum of 50, 20, and 10 Mbps, respectively, of the available port bandwidth. The**class-default** class gets the remaining bandwidth.

```
Router(config)# policy-map out-policy
Router(config-pmap)# class classout1
Router(config-pmap-c)# shape average 50000000
Router(config-pmap-c)# exit
Router(config-pmap)# class classout2
Router(config-pmap-c)# shape average 20000000
Router(config-pmap-c)# exit
Router(config-pmap)# class classout3
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service-policy output out-policy
Router(config-if)# exit
```

Port Shaping

To configure port shaping (a transmit port shaper), create a policy map that contains only a default class, and use the **shape average** command to specify the maximum bandwidth for a port.

This example shows how to configure a policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example. The **service-policy** policy map class command is used to create a child policy to the parent:

```
Router(config)# policy-map out-policy-parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 90000000
Router(config-pmap-c)# service-policy out-policy
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output out-policy-parent
Router(config-if)# exit
```

Parent-Child Hierarchy

The router also supports *parent* policy levels and *child* policy levels for traffic shaping. The QoS parent-child structure is used for specific purposes, where a child policy is referenced in a parent policy to provide additional control of a specific traffic type.

The first policy level, the parent level, is used for port shaping. You can specific only one class of type **class-default** within the policy. This is an example of a parent-level policy map:

```
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 50000000
Router(config-pmap-c)# exit
```

The second policy level, the *child* level, is used to control a specific traffic stream or class, as shown in this example:

```
Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# priority
Router(config-pmap-c)# exit
```

Note The total of the minimum bandwidth guarantees (CIR) for each queue of the child policy cannot exceed the total port-shape rate.

This is an example of a parent-child configuration:

```
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 50000000
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# service-policy output parent
Router(config-if)# exit
```

Class-Based Weighted Fair Queuing

You can configure CBWFQ to set the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. Use the **bandwidth** policy-map class configuration command to set the output bandwidth for a class of traffic as a percentage of total bandwidth, or a percentage of remaining bandwidth.

Note When you configure bandwidth in a policy map, you must configure all the rates in the same format. The total of the minimum bandwidth guarantees (CIR) for each queue of the policy cannot exceed the total speed of the parent.

When you use the **bandwidth** policy-map class configuration command to configure a class of traffic as a percentage of total bandwidth, it represents the minimum bandwidth guarantee (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth indicated by the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio in which the CIR rates are configured.

Note You cannot configure bandwidth as a percentage of total bandwidth when strict priority (priority without police) is configured for another class in the output policy.

When you use the **bandwidth** policy-map class configuration command to configure a class of traffic as a percentage of total bandwidth, it represents the portion of the excess bandwidth of the port that is allocated to the class. This means that the class is allocated bandwidth only if there is excess bandwidth on the port, and if there is no minimum bandwidth guarantee for this traffic class.

Note You can configure bandwidth as a percentage of remaining the bandwidth only when strict priority (priority without police) is configured for another class in the output policy map.

Note You cannot configure bandwidth and traffic shaping (**shape average**) or priority queuing (**priority**) for the same class in an output policy map.

This example shows how the classes *outclass1* , *outclass2* ,*outclass3* , and *class-default* get a minimum of 40 percent, 20 percent, 10 percent, and 10 percent of the total bandwidth, respectively. Any excess bandwidth is divided among the classes in the same proportion as rated in the CIR.

```
Router(config)# policy-map out-policy
Router(config-pmap)# class outclass1
Router(config-pmap-c)# bandwidth percent 40
Router(config-pmap-c)# exit
Router(config-pmap)# class outclass2
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class outclass3
Router(config-pmap-c)# bandwidth percent 10
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth percent 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service-policy output out-policy
Router(config-if)# exit
```

Note When you configure CIR bandwidth for a class as a percentage of the total bandwidth, any excess bandwidth remaining after servicing the CIR of all the classes in the policy map is divided among the classes in the same proportion as the CIR rates. If the CIR rate of a class is configured as 0, that class is also not eligible for any excess bandwidth, and as a result, receives no bandwidth.

This example shows how to allocate the excess bandwidth among queues by configuring bandwidth for a traffic class as a percentage of remaining bandwidth. The class *outclass1* is given priority queue treatment. The other classes are configured to get percentages of the excess bandwidth if any, after servicing the priority queue; *outclass2* is configured to get 20 percent, *outclass3* to get 30 percent, and the *class-default* class to get the remaining 50 percent.

```
Router(config)# policy-map out-policy
Router(config-pmap)# class outclass1
Router(config-pmap-c)# priority
Router(config-pmap-c)# exit
Router(config-pmap)# class outclass2
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class outclass3
Router(config-pmap-c)# bandwidth remaining percent 30
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service-policy output out-policy
Router(config-if)# exit
```

Priority Queuing

You can use the **priority** policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced. All the packets in the queue are scheduled and sent until the queue is empty. Priority queuing allows traffic for the associated class to be sent before the packets in the other queues are sent.

Caution Be careful when using the **priority** command. Excessive use of strict priority queuing might cause congestion in other queues.

The router supports strict priority queuing or **priority percent** policy-map command.

- *Strict priority queuing* (priority without police) assigns a traffic class to a low-latency queue to ensure that the packets in this class have the lowest possible latency. When this is configured, the priority queue is continually serviced until it is empty, possibly at the expense of packets in other queues.

Note You cannot configure priority without policing for a traffic class when traffic shaping or CBWFQ are configured for another class in the same output policy map.

- Use the **priority percent** policy-map command, or *unconditional priority policing* , to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue, and you can use the **bandwidth** and **shape average** policy-map commands for other classes to allocate traffic rates on other queues. Effective Cisco IOS Release 15.3(2)S, Cisco ASR 901 Router allows configuration of multiple classes to serve based on priority.

Note When priority is configured in an output policy map *without* the **priority** command, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map command to allocate excess bandwidth.

Restrictions

- You can associate the **priority** command with a single unique class for all the attached output polices on the router. Efective Cisco IOS Release 15.3(2)S, Cisco ASR 901 Router allows the configuration of multiple classes with *priority percent*.
- You cannot configure priority and other scheduling action (**shape average** or **bandwidth**) in the same class.
- You cannot configure priority queuing for the class-default of an output policy map.

This example shows how to configure the class *out-class1* as a strict priority queue so that all the packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The *class-default* class receives the remaining 30 percent with no guarantees.

```
Router(config)# policy-map policy1
Router(config-pmap)# class out-class1
Router(config-pmap-c)# priority
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class2
Router(config-pmap-c)# bandwidth remaining percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class3
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

This example shows how to use the **priority** keyword with the **percent** command to configure *out-class1* as the priority queue, with the traffic going to the queue limited to 20,000,000 bps so that the priority queue will never use more than that. Traffic above that rate is dropped. The other traffic queues are configured to use 50 percent and 20 percent of the bandwidth that is left, as shown in the previous example.

```
Router(config)# policy-map policy1
Router(config-pmap)# class out-class1
Router(config-pmap-c)# priority percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class2
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class out-class3
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet 0/1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

The following example shows how to use the **priority** keyword with the **percent** command to configure multiple traffic classes:

```
Router(config)# policy-map pmap_bckbone
Router(config-pmap)# class VOICE_GRP
Router(config-pmap-c)# priority percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class CTRL_GRP
Router(config-pmap-c)# priority percent 5
Router(config-pmap-c)# exit
Router(config-pmap)# class E1_GRP
Router(config-pmap-c)# priority percent 55
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth percent 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Ingress and Egress QoS Functions

This section lists the supported and unsupported QoS functions for ingress and egress on the Cisco ASR 901 Router.

Ingress QoS Functions

In Cisco ASR 901 router:

- Interfaces support ingress classification.
- Ethernet interfaces support ingress policing.
- Ethernet interfaces support ingress marking.
- Ethernet interfaces do not support Low-Latency Queuing (LLQ). Ingress Priority is not supported on ingress.
- Ethernet interfaces do not support queuing, shaping, and scheduling on ingress.
- Classification based on QoS group is not supported.

Egress QoS Functions

In Cisco ASR 901 router:

- Gigabit Ethernet interfaces support egress classification.
- Gigabit Ethernet interfaces support egress marking.
- Gigabit Ethernet interfaces support egress scheduling.
- Interfaces support per interface and per QoS group shaping on egress ports.
- Interfaces support LLQ and weighted random early detection on egress.

Configuring QoS

The following sections describe how to configure the QoS features supported by the Cisco ASR 901 Router:

QoS Limitations

The Cisco ASR 901 Router offers different QoS support according to the physical interface and traffic type. The following sections describe the limitations for each QoS capability on the Cisco ASR 901 Router.

General QoS Limitations

The following general QoS limitations apply to the Cisco ASR 901 Router:

- You can create a maximum of 256 class maps, including the class-default class map.
- You can create a maximum of 32 policy maps.
- Input policy-map is not supported on SVI.
- Output policy-map is not supported on service instance.
- The CoS marking is supported only on normal interfaces.
- EXP to COS marking is not supported on Port channel.
- Policy-map having class-map with mpls experimental topmost must be applied only on MPLS enabled interface. Usage of policy-map on non-mpls interface can result in other packets matching this criteria.
- The match cos inner is not supported.
- Egress Queue on POCH is supported only on POCH interface and uses replication model.

The following limitations apply to the QoS policies on HDLC, PPP, PPP interfaces:

- Input PPP interfaces support only QoS marking policies.
- Only a maximum of eight **match** statements can be created within a class map in a service policy applied to a PPP interface.
- Only a maximum of eight classes can be created within a policy map that is applied to a PPP interface. This number includes the default-class.
- Only one priority class can be used within a policy map applied to a PPP interface.
- The **match-all** keyword of the **class-map** command is not supported.
- The following actions are not supported for egress policy:
    - Bandwidth value
    - Priority value
    - Set of qos-group (VLAN priority)—This is relevant only for Layer 2 Transport over MLPPP interface.
- Requires explicit configuration of class-default with bandwidth percent.
- DSCP marking is not supported for the class-default queue.

All the above restrictions are applicable to MPLS over MLPPP and IP over MLPPP, in addition to the following specific restrictions that apply to QoS policies on MPLS and IP over MLPPP interfaces:

- The Cisco ASR 901 Router supports the DSCP marking priority, eight bandwidth queues, link fragmentation, interleave, and queue limits features for MLPPP egress.
- Input policy is not supported.
- EXP marking is not supported for the class-default queue.

The following limitations apply to Gigabit Ethernet interfaces:

- You can apply only a maximum of two different service policies to the Gigabit Ethernet interfaces.
- You can only use the class-default class for HQoS parent service policies applied to egress Gigabit Ethernet interfaces.

Statistics Limitations

The following statistical QoS limitations apply to the Cisco ASR 901 Router:

- Input service policies on the Gigabit Ethernet interface support statistics only in bytes.
- PPP and MLPPP interfaces support QoS statistics only in packets.
- Output service policies on the Gigabit Ethernet interface support statistics only in bytes.
- The 2R3C policer provides exceed-and-violate counters as a single counter.
- Marking statistics will not be displayed for any class.

Propagation Limitations

The Cisco ASR 901 Router has the following limitations when propagating QoS values between interfaces:

- The following limitation is applicable when traffic ingresses through a GigabitEthernet interface and egresses through a GigabitEthernet interface:
  - When traffic is switched at Layer 2, the QoS group is propagated through the router.
- The following limitations are applicable when traffic ingresses through any other interface type (host-generated and PPP) and egresses through the GigabitEthernet interface.
  - The Precedence bit value is propagated to the CoS bit (for host-generated interface only).
  - The CoS bit value is mapped 1:1 to the QoS group value.

See the Sample QoS Configuration, on page 417 section for a sample QoS configuration that accounts for propagation limitations on the Cisco ASR 901 Router.

Classification Limitations

The following table summarizes the values that you can use to classify traffic based on interface type. The values are parameters that you can use with the **match** command.

Table 21: QoS Classification Limitations by Interface

	Gigabit Ethernet		**PPP**	
Value	Ingress	Egress	Ingress	Egress
access-group	X	—	—	—
all	X	X	—	—
any	X	X	X	X
class-map	—	—	—	—
cos	X	X	—	—
destination-address	—	—	—	—
discard-class	—	—	—	—
dscp	X	X	X	X
flow pdp	—	—	—	—

frde	—	—	—	—
frdlci	—	—	—	—
ip dscp	X	X	X	X
ip precedence	X	X	—	—
ip rtp	—	—	—	—
mpls experimental	X	—	—	—
not	—	—	—	—
packet length	—	—	—	—
precedence	X	X	—	—
protocol	—	—	—	—
qos-group	—	X	—	—
source-address	—	—	—	—
vlan	X	X	—	—

The following limitations are also applicable when configuring classification on the Cisco ASR 901 Router:

- The **set qos-group cos** command used for trusting CoS is supported only under class-default, as a stand-alone class in the policy-map. No other user class is supported on the same policy-map. Counters are not supported for the policy-map.
- The following limitations apply to the input Gigabit Ethernet interface QoS policies:
  - You can use the **match vlan** command with a maximum of four VLANs. The **match vlan** command is supported only for port, EVC, and pseudowire.
  - You can use the **match dcsp** command with a maximum of four DSCP values.
  - The Cisco ASR 901 Router first looks for IP DSCP and then the MPLS experimental imposition for the MPLS packets.
- The following limitations apply to the output Gigabit Ethernet interface QoS policies:
  - Class maps with queuing action only support matching based on QoS group. This limitation does not apply to the class-default class map.
  - You cannot create two matching class maps based on the same QoS group value.
  - Class-default on the egress supports matching only on qos-group 0.
- The following limitation applies to input PPP interfaces:
  - You can create only up to eight matches in a class map, using DSCP or MPLS Exp values.

> **Note** The **show policy-map interface counters** command does not display cumulative queue statistics for priority classes. It shows only queue statistics for individual priority classes. Similarly, output or marking counters are not supported.

Marking Limitations

The following table summarizes the values that you can use to mark traffic, based on interface type. The values are parameters that you can use with the **set** command.

	Gigabit Ethernet		**PPP**	
Value	Ingress	Egress	Ingress	Egress
atm-clp	—	—	—	—
cos	—	—	—	—
discard-class	X	—	—	—
dscp	X	—	—	—
dscp-transmit	X	—	—	—
ip dscp	X	X	X	—
ip precedence	X	X	—	—
mpls experimental	—	—	—	—
mpls experimental imposition	X	—	X	—
mpls experimental topmost qos-group	—	X	—	—
precedence	X	—	—	—
prec-transmit	X	—	—	—
qos-group	X	—	X	—

Congestion Management Limitations

The congestion management limitations for the Cisco ASR 901 Router are described in the following sections:

Queuing Limitations

The Cisco ASR 901 Router uses Class-Based Weighted Fair Queuing (CBWFQ) for congestion management. The following table summarizes the queuing commands that you can apply when using CBWFQ according to interface type.

Table 22: QoS Queuing Limitations by Interface

	Gigabit Ethernet		PPP	
Value	Ingress	Egress	Ingress	Egress
bandwidth (kbps)	—	—	—	—
bandwidth percent	—	X	—	X
bandwidth remaining percent	—	X	—	X
compression header ip	—	—	—	—
drop	—	—	—	—
fair-queue	—	—	—	—
priority	—	X	—	X
priority (kbps)	—	—	—	—
priority (without queue-limit)	—	—	—	—
priority percent	—	X	—	X
queue-limit (cells)	—	—	—	
queue-limit (packets)	—	—	—	X
random-detect discard-class-based	—	X	—	—

Rate-Limiting Limitations

You can use rate limiting for congestion management on the Cisco ASR 901 Router. The following table summarizes the rate-limiting parameters that you can use with the **police** command, according to interface type. The table uses the following terms:

- Rate—A speed of network traffic, such as a committed information rate (CIR) or peak information rate (PIR).
- Actions—A defined action when traffic exceeds a rate, such as conform-action, exceed-action, or violate-action.

Table 23: QoS Rate Limiting Limitations by Interface

	Gigabit Ethernet		PPP	
Policing With	Ingress	Egress	Ingress	Egress
One rate	—	—	—	—

One rate and two actions	X	—	—	—
Two rates and two actions	—	—	—	—
Two rates and three actions	X	—	—	—

Shaping Limitations

The following table summarizes the values that you can use to mark traffic based on interface type. The values are parameters that you can use with the **shape** command.

Table 24: QoS Shaping Limitations by Interface

	Gigabit Ethernet		**MLPPP**	
Value	Ingress	Egress	Ingress	Egress
adaptive	—	—	—	—
average	—	X	—	X
fecn-adapt	—	—	—	—
max-buffers	—	—	—	—
peak	—	—	—	—

The following limitations also apply to QoS shaping on the Cisco ASR 901 Router:

- The following limitations apply to the input Gigabit Ethernet interfaces:
  - You cannot apply shaping to the class-default class unless you are using hierarchical policy maps and applying shaping to the parent policy map.
  - If you are using hierarchical policy maps, you can only apply the class-default class to the parent policy map.
- The following limitations apply to Egress Shaping on the MLPPP interfaces:
  - Only shape average is supported.
  - Hierarchical shaping is not supported.
  - More than one shape in the same policy-map is not allowed.
  - Shape and bandwidth in the same class is not allowed.
  - Shape command in default class is not allowed.

ACL-based QoS Restrictions

In addition to all the limitations applicable to a current QoS configuration, the following restrictions are applicable for ACL-based QoS:

- IPv6 ACL-based QoS is not supported.
- ACL-based QoS is limited to source and destination IP addresses. Extended ACLs with extended options such as DSCP, fragments, option, precedence, time-range, ToS, and TTL are not supported.
- MAC ACLs are not supported. Only IP ACLs are supported.
- You can configure only named access lists in QoS; other ACL types are not supported.
- Only source and destination IPv4 addresses are supported in the access-list definition.
- You can add only a maximum of 128 ACL match filters (including default deny ace) as part of class or classes.

Improving Feature Scalability

Effective Cisco IOS Release 15.3(2)S, Ternary content-addressable memory (TCAM) is allocated and deallocated dynamically based on system configuration. This improves both feature scalability and efficiency of TCAM usage. 25 percent of this memory is reserved for Layer 2 and Layer 3 control protocols and the remaining 75 percent is allocated dynamically based on the requirements. Layer 2 and Layer 3 forwarding tables are independent of TCAM.

TCAM with QoS

The scalability of QoS changes depending on the features configured on the Cisco ASR 901 Router, as shown in the following examples:

- You can create a maximum of 768 TCAM rules.
- You can create a maximum of 640 TCAM rules with remote loopback in Ethernet OAM (802.3ah), Ethernet loopback, and DelayMeasurement configured.
- You can create a maximum of 512 TCAM rules with remote loopback in Ethernet OAM (802.3ah), Ethernet loopback, DelayMeasurement, and Router ACL configured.

For more information on troubleshooting scalability, see Troubleshooting Tips, on page 481.

QoS for MPLS over MLPPP and IP over MLPPP

Effective Cisco IOS Release 15.4(1)S, the extended QoS functionality is supported on the MLPPP interface. The egress policy supports classification on the MLPS EXP bits.

The following actions are supported:

- Bandwidth percent
- Priority percent
- Setting the MPLS EXP bits
- Setting the queue limit
- Egress shaping

QoS for CPU-Generated Traffic

Effective Cisco IOS Release 15.4(1)S, QoS is provided for CPU-generated traffic. The classification is based on DSCP (for packets going over IP adjacency) or EXP (for packets going over TAG adjacency).

QoS treatment is available for the following CPU generated traffic:

- Open Shortest Path First (OSPF) Packets

- Internet Control Message Protocol (ICMP) Packets
- Border Gateway Protocol (BGP) Packets
- Label Distribution Protocol (LDP) Packets
- Intermediate System to Intermediate System (IS-IS) Frames

The QoS configuration for CPU-generated traffic is the same as that of QoS for MPLS over MLPPP. However, you should use **class-map** to match the DSCP or EXP values of the CPU-generated traffic.

For example:

- If the OSPF packets use DSCP CS6, the policy map should use the class map to match DSCP CS6.
- BGP and LDP packets use either IP adjacency or TAG adjacency (depending on the type of packets)
    - Packets going over IP adjacency use DSCP CS6
    - Packets going over TAG adjacency use EXP 6
- For ICMP packets (PING traffic), the default DSCP value is 0; you can specify TOS value while sending the ping traffic.
- If IS-IS packets do not have either DSCP or EXP; they are treated with the policy configuration of DSCP CS6.

Note The **show policy-map interface multilink** *bundle-number* command shows the combined counters of the CPU-generated traffic and data traffic if both the data traffic and CPU-generated traffic flow in the same class.

Egress Shaping on the MLPPP Interfaces

Traffic shaping allows you to control the speed of traffic that is leaving an interface to match the intake capacity of the receiving interface. Cisco IOS Release 15.5(1)S introduces support for Egress shaping over MLPPP interfaces. This feature allows you to shape all MLPPP interfaces using a port policy with a class-default shaper configuration.

You should complete the following steps to configure Egress Shaping over MLPPP:

1. Configure a Class-map
2. Configure the policy-map with shaping and bandwidth
3. Attach the policy-map on the MLPPP interface

QoS Configuration Guidelines

- You can configure QoS on physical ports and EFPs (only in ingress).
- QoS can likely be configured on port channel.
- Only table-map configuration is allowed on Switch Virtual Interface (SVI) interfaces.
- On a port configured for QoS, all the traffic received through the port is classified, policed, and marked according to the input policy map attached to the port. On an EFP configured for QoS, traffic in all the VLANs received through the port is classified, policed, and marked according to the policy map attached to the port. If a per-port, per-VLAN policy map is attached, traffic on the trunk port is classified, policed, and marked for the VLANs specified in the class filter.

- If you have EtherChannel ports configured on your router, you must configure QoS classification, policing, mapping, and queuing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all the ports in the EtherChannel.
- Control traffic (such as Spanning-tree Bridge Protocol Data Units [BPDUs] and routing update packets) received by the router are subject to all ingress QoS processing.
- You might lose data when you change queue settings. Therefore, try to make changes when traffic is at a minimum.
- When you try to attach a new policy to an interface and this brings the number of policer *instances* to more than 255, you receive an error message, and the configuration fails.
- When you try to attach a new policy to an interface and this brings the number of policer *profiles* to more than 254, you receive an error message, and the configuration fails. A profile is a combination of commit rate, peak rate, commit burst, and peak burst. You can attach one profile to multiple instances, but if one of these characteristics differs, the policer is considered to have a new profile.
- On all Cisco ASR 901 Routers, you can specify 128 unique VLAN classification criteria within a per-port, per-VLAN policy map, across all the ports on the router. Any policy attachment or change that causes this limit to be exceeded fails with a `VLAN label resources exceeded` error message.
- On all Cisco ASR 901 Routers, you can attach per-port, per-VLAN policy-maps across all ports on the router until QoS classification resource limitations are reached. Any policy attachment or change that causes this limit to be exceeded fails with a `TCAM resources exceeded` error message.

Sample QoS Configuration

The following configuration demonstrates how to apply QoS given the hardware limitations. The Cisco ASR 901 Router processes traffic between interfaces as follows:

- For Layer 2 traffic passing between the Gigabit Ethernet 0/2 interface and the Gigabit Ethernet 0/0 interface, the output queue is determined by the QoS group assigned in the in-qos policy map.
- For Layer 3 traffic passing between Gigabit Ethernet 0/2 interface and the Gigabit Ethernet 0/0 interface, the output queue is determined based on the CoS value assigned in the in-qos policy map. (the CoS value is mapped 1:1 to the QoS group value.)
- For traffic passing between other interfaces, the output queue is determined based on the CS fields (top three bits) of the IP DSCP bits; these bits are copied to the CoS bits, which are mapped 1:1 to the QoS group value.

The following is a sample configuration for QoS:

Note The sample configuration is a partial configuration intended to demonstrate the QoS feature.

```
!
class-map match-all q0
 match qos-group 0
class-map match-all q1
 match qos-group 1
class-map match-all q2
 match qos-group 2
class-map match-all q3
 match qos-group 3
class-map match-all q4
 match qos-group 4
class-map match-all q5
 match qos-group 5
```

```
class-map match-all q6
 match qos-group 6
class-map match-all q7
 match qos-group 7
class-map match-any Voice
 match dscp ef
class-map match-any Signaling
 match dscp af41
class-map match-any HSDPA
 match dscp af11 af12
class-map match-any TCAM1
!translates to 3 TCAM rules because each match in match-any uses one entry
match dscp af21
match cos 3
match mpls experimental topmost
class-map match-all TCAM2
!translates to 1 TCAM rules because all the match-all clauses together take only 1 entry
match dscp af21
match cos 3
match mpls experimental topmost 1
!
policy-map in-qos
 class Voice
  set cos 5
  set qos-group 5
 class control_plane
  set cos 4
  set qos-group 4
 class HSDPA
  set cos 1
  set qos-group 1
!
policy-map out-child
 class q5
    priority percent 20
 class q4
    bandwidth remaining percent 20
 class q1
    bandwidth remaining percent 59
!
!
policy-map out-parent
 class class-default
    shape average 100000000
  service-policy out-child
!
```

Configuring Classification

Classifying network traffic allows you to organize packets into traffic classes based on whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many QoS features on your network.

This section contains the following topics:

Creating a Class Map for Classifying Network Traffic

Class maps allow you to define classes of network traffic in order to apply QoS features to each class. Complete the following steps to create a class map:

Procedure

Step 1 Enter the enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 3 Enter global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Use the **class-map** command to define a new class map and enter class map configuration mode.

Example:

```
Router(config)# class-map class1
```

Step 5 Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

Example:

```
Router(config-cmap)# match qos-group 7
```

Note
The class-default queue matches packets with qos-group 0.

Example:

Step 6 Exit configuration mode.

Example:

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

Creating a Policy Map for Applying a QoS Feature to Network Traffic

A policy map allows you to apply a QoS feature to network traffic based on the traffic classification. Complete the following steps to create and configure a policy map that uses an existing class map.

Procedure

Step 1 Enter the enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 3 Enter the global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Use the **policy-map** command to define a new policy map and enter policy map configuration mode.

Example:

```
Router(config)# policy-map policy1
Router(config-pmap)#
```

Step 5 Use the **class** command to specify a traffic class to which the policy applies. This command enters policy-map class configuration mode, which allows you to define the treatment for the traffic class.

Example:

```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```

Use the **bandwidth** command to specify the bandwidth allocated for a traffic class attached to the policy map. You can define the amount of bandwidth in kbps, a percentage of bandwidth, or an absolute amount of bandwidth. This step is optional.

Note
GigabitEthernet interfaces only support bandwidth defined as a percentage or remaining percent.

Example:

```
Router(config-pmap-c)# bandwidth percent 50
```

Step 6 Exit the configuration mode.

Example:

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

Note

You can use the **show policy-map** command to verify your configuration.

Attaching the Policy Map to an Interface

After you create the policy map, you must attach it to an interface. Policy maps can be attached to either the input or output direction of the interface.

Complete these steps to attach the policy map to an interface:

Procedure

Step 1 Enter enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router, you have entered enable mode.

Step 3 Enter global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Specify the interface to which you want to apply the policy map.

Example:

```
Router(config)# interface gigabitEthernet0/1
```

Step 5 Use the **service-policy** command to attach the policy map to an interface. The **input** and **output** parameters specify the direction in which router applies the policy map.

Example:

```
Router(config-if)# service-policy output policy1
```

Step 6 Exit configuration mode.

Example:

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

Note
You can use the **show policy map** interface command to verify your configuration.

For more information about configuring classification, see the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR .

Attaching a Policy Map to a Cross-Connect EVC

After you create a policy map, you must attach it to a cross-connect EVC. Policy maps can be attached only to ingress.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/3`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**service instance** *instance-id* **ethernet** **Example:** `Router(config-if)# service instance 22 ethernet`	Creates a service instance on an interface and defines the matching criteria. • *instance-id* —Unique identifier of the instance.
Step 5	**encapsulation dot1q vlan-id** **Example:** `Router(config-if)# encapsulation dot1q 22`	Defines the matching criteria to be used to map 802.1Q frames ingress on an interface to the appropriate EFP. Enter a single VLAN ID for an exact match of the outermost tag. VLAN IDs are 1 to 4094. **Note** VLAN IDs 4093, 4094, and 4095 are reserved for internal use.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-svr)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation modification to occur on packets at ingress. • **pop 1**—the outermost tag. • **symmetric**—Configure the packet to undergo the reverse of the ingress action

	Command or Action	Purpose
		at egress. If a tag is removed at ingress, it is added at egress. Although the **symmetric** keyword appears to be optional, you must enter it for rewrite to function correctly.
Step 7	**xconnect** *peer-ip-address vc-id encapsulation mpls* **Example:** `Router(config-if-srv)# xconnect 1.1.1.1 100 encapsulation mpls`	Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers. • *encapsulation*—Specifies the tunneling method to encapsulate the data in the pseudowire. • *mpls*—Specifies MPLS as the tunneling method.
Step 8	**service policy** *input policy name* **Example:** `Router(config-if-srv)# service-policy input policy1`	Attaches the policy map to an interface. • *input*—Specifies the direction in which the router applies the policy map. • *policy name*—The name of the policy map.
Step 9	**exit**	Enters global configuration mode.

Configuring Marking

Marking network traffic allows you to set or modify the attributes for packets in a defined traffic class. You can use marking with traffic classification to configure a variety of QoS features for your network.

The Cisco ASR 901 Router marking allows you to modify the following packet attributes:

- Differentiated services code point (DSCP) value
- Class of service (CoS) value
- MPLS Exp bit value
- Qos group value (internal)

For instructions on how to configure marking for IP Precedence, DSCP, or CoS value, see the following sections:

- Creating a Class Map for Marking Network Traffic, on page 424
- Creating a Policy Map for Applying a QoS Feature to Network Traffic, on page 425
- Attaching the Policy Map to an Interface, on page 426

For instructions on how to configure MPLS Exp bit marking, see:

• Configuring MPLS Exp Bit Marking using a Pseudowire, on page 427.

Creating a Class Map for Marking Network Traffic

Class maps allow you to define classes of network traffic in order to apply QoS features to each class. Complete the following steps to define a traffic class to mark network traffic:

Procedure

Step 1 Enter the enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 3 Enter the global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Use the **class-map** command to define a new class map and enter class map configuration mode.

Example:

```
Router(config)# class-map class1
```

Step 5 Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

Example:

```
Router(config-cmap)# match qos-group 7
```

Step 6 Exit the configuration mode.

Example:

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

Creating a Policy Map for Applying a QoS Feature to Network Traffic

Policy maps allow you to apply the appropriate QoS feature to the network traffic based on the traffic classification. The following sections describe how to create and configure a policy map to use a class map or table map.

The following restrictions apply when applying a QoS feature to network traffic:

- A policy map containing the **set qos-group** command can only be attached as an intput traffic policy.
- A policy map containing the **set cos** command can only be attached as an input traffic policy.

Complete the following steps to create a policy map.

Procedure

Step 1 Enter the enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 3 Enter the global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Use the **policy-map** command to define a policy map and enter policy map configuration mode.

Example:

```
Router(config)# policy-map policy1
Router(config-pmap)#
```

Step 5 Use the **class** command to specify the traffic class for which you want to create a policy and enter policy map class configuration mode. You can also use the **class-default** parameter to define a default class.

Example:

```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```

Step 6 Use one of the **set** commands listed in Table 25: set Commands Summary, on page 426 to define a QoS treatment type.

Table 25: set Commands Summary

set Commands	Traffic Attributes	Network Layer	Protocol
set cos	Layer 2 CoS value of the outgoing traffic	Layer 2	802.1q
set dscp	DSCP value in the ToS byte	Layer 3	IP
set qos-group	QoS group ID	Layer 3	IP, MPLS

Step 7 Exit the configuration mode.

Example:

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

Note
You can use the **show policy-map** or **show policy-map** *policy-map* **class** *class-name* commands to verify your configuration.

Attaching the Policy Map to an Interface

Procedure

Step 1 Enter enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router, you have entered enable mode.

Step 3 Enter global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Specify the interface to which you want to apply the policy map.

Example:

```
Router(config)# interface gigabitEthernet0/1
```

Step 5 Use the **service-policy** command to attach the policy map to an interface. The **input** and **output** parameters specify the direction in which router applies the policy map.

Example:

```
Router(config-if)# service-policy input policy1
```

Step 6 Exit configuration mode.

Example:

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

Note
You can use the **show policy map** interface command to verify your configuration.

Configuring MPLS Exp Bit Marking using a Pseudowire

You can also configure MPLS Exp bit marking within an EoMPLS pseudowire interface using the **set mpls experimental imposition** command. MQC based policy configuration supersedes pseudowire-class mode of configuring QoS marking. The MQC policy shall contain only class-default with set action to achieve the same. Follow these steps to configure MPLS Exp bit marking using a pseudowire interface.

Note The policy-map configured with the **set mpls experimental imposition** command, is allowed only on the cross-connect EFP.

Complete the following steps to apply a marking policy to a pseudowire:

Procedure

Step 1 Enter the interface configuration mode.

Example:

```
Router(config)# interface gigabitethernet 0/0
Router(config-if)#
```

Step 2 Specify an EVC.

Example:

```
Router(config-if)# service instance 1 ethernet
Router(cfg-if-srv)#
```

Step 3 Specify an encapsulation type for the EVC.

Example:

```
Router(cfg-if-srv)# encapsulation dot1q 200
```

Step 4 Use the **xconnect** command with the service policy that uses the configuration defined in the pseudowire class.

Example:

```
Router(cfg-if-srv)# xconnect 10.10.10.1 121
Router(cfg-if-srv)# service-policy in <mark-policy>
```

For more information about configuring marking, see the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR.

Note
The Cisco ASR 901 does not support all of the commands described in the IOS Release 12.2SR documentation.

Configuration Example

This is a sample configuration example for applying a marking policy to a pseudowire.

```
policy-map cos-6
class cos-6
 police rate percent 5
  conform-action transmit
  exceed-action drop
set mpls experimental imposition 4
interface GigabitEthernet0/3
no ip address
load-interval 30
negotiation auto
service instance 22 ethernet
 encapsulation dot1q 22
 rewrite ingress tag pop 1 symmetric
 service-policy input cos-6
 xconnect 2.2.2.2 22 encapsulation mpls
```

Configuring Congestion Management

The following sections describe how to configure congestion management on the Cisco ASR 901.

- Configuring Low Latency Queueing, on page 428
- Configuring Multiple Priority Queueing, on page 430
- Configuring Class-Based Weighted Fair Queuing (CBFQ), on page 431
- Weighted Random Early Detection (WRED), on page 433

Configuring Low Latency Queueing

Low latency queuing allows you to define a percentage of bandwidth to allocate to an interface or PVC as a percentage. You can define a percentage for priority or nonpriority traffic classes.

Complete the following steps to configure LLQ.

Procedure

Step 1 Enter enable mode.

Example:

```
Router> enable
```

Step 2 Enter the password.

Example:

```
Password: password
```

When the prompt changes to Router , you have entered enable mode.

Step 3 Enter global configuration mode.

Example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 4 Use the **policy-map** command to define a policy map.

Example:

```
Router(config)# policy-map policy1
```

Step 5 Use the **class** command to reference the class map that defines the traffic to which the policy map applies.

Example:

```
Router(config-pmap)# class class1
```

Step 6 Use the **priority** command to specify the priority percentage allocated to the traffic class assigned to the policy map. You can use the **burst** parameter to configures the network to accommodate temporary bursts of traffic.

Example:

```
Router(config-pmap-c)# priority percent 10
```

Step 7 Use the bandwidth command to specify the bandwidth available to the traffic class within the policy map. You can specify the bandwidth in kbps or by a percentage of bandwidth.

Example:

```
Router(config-pmap-c)# bandwidth percent 30
```

Step 8 Exit configuration mode.

Example:

```
Router(config-pmap-c)# end
```

Note
You can use the **show policy-map**, **show policy-map policy-map class** *class-name, or* **show policy-map interface** *commands to verify your configuration.*

Configuring Multiple Priority Queueing

Multiple priority queuing allows you to configure more than one class with priority percentage. The queue-number decides the ordering. The QoS group is serviced in the descending order starting with the highest queue number. This guarantees each of the queues its allocated bandwidth. This configuration has a higher latency on the lower priority queue like voice, due to servicing multiple traffic types on priority.

Note There is no provision to configure the priority level for a traffic class.

Complete the following steps to configure multiple priority queueing.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode. Enter your password if prompted.
Step 2	**policy-map** **Example:** `Router(config)# policy-map policy1`	Defines a new policy map and enters policy map configuration mode.
Step 3	**class** *class-name* **Example:** `Router(config-pmap)# class class1`	Specifies a traffic class to which the policy applies. This command enters policy-map class configuration mode, which allows you to define the treatment for the traffic class.
Step 4	**priority percent** *percent* **Example:** `Router(config-pmap-c)# priority percent 10`	Specifies the priority percentage allocated to the traffic class assigned to the policy map.
Step 5	**bandwidth percent** *percent* **Example:** `Router(config-pmap-c)# bandwidth percent 50`	(Optional) Specifies the bandwidth allocated for a traffic class attached to the policy map. You can define the percentage of bandwidth, or an absolute amount of bandwidth.
Step 6	**exit**	Returns to global configuration mode.

Configuration Examples

This section shows sample configuration examples for multiple priority queuing on Cisco ASR 901 router:

```
policy-map pmap_bckbone
 class VOICE_GRP
  priority percent 50
```

```
class CTRL_GRP
 priority percent 5
class E1_GRP
 priority percent 35
class class-default
 bandwidth percent 10
```

Note You can use the **show policy-map**, **show policy-map policy-map class** *class-name, or* **show policy-map interface** *commands to verify your configuration.*

Configuring Class-Based Weighted Fair Queuing (CBFQ)

The Cisco ASR 901 supports Class-Based Weighted Fair Queuing (CBWFQ) for congestion management.

Complete the following steps to configure CBWFQ.

Procedure

Step 1 A class map contains match criteria against which a packet is checked to determine if it belongs to the class. You can use class maps to define criteria that are referenced in one or more policy maps. Use the **class-map** command to create a class map.

a) **class-map** *class-map name*

Example:

```
Router(config)# class-map class1
Router(config-cmap)#
```

b) Use the **match** command to specify the match criteria for the class map. You can define a variety of match criteria including CoS, DSCP, MPLS Exp, or QoS group value.

Example:

```
Router(config-cmap)# match qos-group 7
```

c) Use the **exit** command to exit class map configuration.

Example:

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

Step 2 Complete the following steps to configure a policy map and attach it to an interface.

Note
This router does not support **queue-limit** commands. Only **random-detect discard-class-based** is supported on GigabitEthernet Interfaces.

a) Use the **policy-map** command to define a policy map.

Example:

```
Router(config)# policy-map policy1
Router(config-pmap)#
```

b) Use the **class** command to reference the class map that defines the traffic to which the policy map applies.

Example:

```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```

c) Use the **bandwidth** command to specify the bandwidth allocated for the traffic class.

Example:

```
Router(config-pmap-c)# bandwidth percent 10
```

d) Use the **exit** command to exit the policy map class configuration.

Example:

```
Router(config-pmap-c)# exit
Router(config-pmap)#
```

e) Use the **exit** command to exit the policy map configuration.

Example:

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

f) Enter configuration for the interface to which you want to apply the policy map.

Example:

```
Router(config)# interface atm0/ima0
```

g) Use the **service-policy** command to apply the service policy to the interface.

Example:

```
Router(config-if)# service-policy output policy1
```

Modifying CPU Queue Limits

You can modify the rate-limit and burst of network packets that are received by the CPU queue on the Cisco ASR 901 platform by using the following command:

```
router(config)#platform cosq <cosq-number> rate-limit <rate-limit> [burst <burst-value>]
```

Table 26: Syntax Description

cosq	Enter the CPU queue number. The queue number ranges from 0 to 47.

rate-limit	Enter the number of packets that should be received by the CPU queue. The value ranges from 1 to 1000 packets.
burst	(Optional) Enter the number of packets that must be pushed above the configured bandwitdth limit. The value ranges from 1 to 100.

To disable the command, use the **no** form of this command.

```
router(config)#no platform cosq <cosq-number>
```

Upon execution of the above command, the rate limit and burst values of the specified queue are reset to their default values.

The following example shows how to modify the defualt rate-limit and burst values for a CPU queue:

```
router(config)#platform cosq 38 rate-limit 500 [burst 100]
```

Weighted Random Early Detection (WRED)

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of the congestion control mechanism of TCP. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. WRED drops packets selectively based on IP discard-class. Discard-class is assigned to packets at the ingress, as they enter the network. WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than at the edge. WRED uses discard-class to determine how it treats different types of traffic.

When a packet arrives, the following events occur:

1. The average queue size is calculated.
2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.

Note Cisco ASR 901 supports configuration of random-detect thresholds only in number-of-packets.

Complete the following steps to configure WRED:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter the global configuration mode
Step 2	**policy-map** **Example:** `Example`	Define a new policy map and enter policy map configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# policy-map policy1`	
Step 3	**class** **Example:** `Router(config-pmap)# class class1`	Specify a traffic class to which the policy applies. This command enters policy-map class configuration mode, which allows you to define the treatment for the traffic class.
Step 4	**bandwidth** **Example:** `Router(config-pmap-c)# bandwidth percent 50`	Specify the bandwidth allocated for a traffic class attached to the policy map. You can define the percentage of bandwidth, or an absolute amount of bandwidth. This step is optional.
Step 5	**[no] random-detect discard-class-based**	Base WRED on the discard class value of a packet. To disable this feature, use the **no** form of this command.
Step 6	**[no] random-detect discard-class** **Example:** `Router(config-pmap-c)# random-detect discard-class 2 100 200 10`	Configure WRED parameters for a discard-class value for a class policy in a policy map. • Discard class. Valid values are 0 to 2. **Note** WRED counters are not supported for discard class 0. • *min-threshold*— Minimum threshold in number of packets. Valid values are 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence. • *max-threshold*— Maximum threshold in number of packets. Valid values are 1 to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence. **Note** Max-threshold values configured above 1024 cannot be reached. • —Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid

	Command or Action	Purpose
		values are 1 to 65535. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold. To return the values to the default for the discard class, use the **no** form of this command.

Configuring Shaping

The Cisco ASR 901 supports class-based traffic shaping. Follow these steps to configure class-based traffic shaping.

Class-based traffic shaping is configured using a hierarchical policy map structure; you enable traffic shaping on a primary level (parent) policy map and other QoS features such as queuing and policing on a secondary level (child) policy map.

This section contains the following topics:

- Configuring Class-Based Traffic Shaping in a Primary-Level (Parent) Policy Map, on page 435
- Configuring the Secondary-Level (Child) Policy Map, on page 436

Configuring Class-Based Traffic Shaping in a Primary-Level (Parent) Policy Map

Follow these steps to configure a parent policy map for traffic shaping.

Procedure

Step 1 Use the **policy-map** command to specify the policy map for which you want to configure shaping and enter policy-map configuration mode.

Example:

```
Router(config)# policy-map output-policy
```

Step 2 Use the **class** command to specify the traffic class to which the policy map applies.

Example:

```
Router(config-pmap)# class class1
Router(config-pmap-c)#
```

Step 3 Use the **shape** command to define algorithm and rate used for traffic shaping.

Example:

```
Router(config-pmap-c)# shape average mean-rate burst-size
```

Step 4 Use the **service-policy** command to attach the policy map to the class map.

Example:

```
Router(config-pmap-c)# service-policy policy-map
```

Step 5 Exit configuration mode.

Example:

```
Router(config-pmap-c)# end
Router#
```

Note
You can use the **show policy-map** command to verify your configuration.

For more information about configuring shaping, see Regulating Packet Flow on a Per-Class Basis---Using Class-Based Traffic Shaping .

Note
This router does not support all of the commands described in the IOS Release 12.2SR documentation.

Configuring the Secondary-Level (Child) Policy Map

Follow these steps to create a child policy map for traffic shaping.

Procedure

Step 1 Use the **policy-map** command to specify the policy map for which you want to configure shaping and enter policy-map configuration mode.

Example:

```
Router(config)# policy-map output-policy
```

Step 2 Use the **class** command to specify the traffic class to which the policy map applies.

Example:

```
Router(config-pmap)# class class1
```

Step 3 Use the **bandwidth** command to specify the bandwidth allocated to the policy map. You can specify the bandwidth in kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth.

Example:

```
Router(config-pmap-c)# bandwidth percent 50
```

Step 4 Exit configuration mode.

Example:

```
Router(config-pmap-c)# end
```

For more information about configuring shaping, see Regulating Packet Flow on a Per-Class Basis---Using Class-Based Traffic Shaping .

Note

The Cisco ASR 901 does not support all of the commands described in the IOS Release 12.2SR documentation.

Configuring Ethernet Trusted Mode

The Cisco ASR 901 supports trusted and non-trusted mode for Gigabit ethernet ports. Gigabit ethernet ports are set in non-trusted mode by default. Trust mode is configured through table-maps. Use the **set qos-group cos** command to use default mapping.

Creating IP Extended ACLs

Complete the following steps to create an IP extended ACL for IP traffic:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**access-list** *access-list-number***permit***access-list-number access-list-number access-list-number* [**precedence** *access-list-number*] [**tos** *access-list-number*] [**dscp** *access-list-number*]	Create an IP extended ACL. Repeat the step as many times as necessary. • For *access-list-number* , enter the access list number. The range is 100 to 199 and 2000 to 2699. • For *access-list-number* , enter the name or number of an IP protocol. Use the question mark (?) to see a list of available protocols. To match any Internet protocol (including ICMP, TCP, and UDP), enter **ip**. • The *access-list-number* is the number of the network or host sending the packet. • The *access-list-number* applies wildcard bits to the source. • The *access-list-number* is the network or host number receiving the packet. • The *access-list-number* applies wildcard bits to the destination. You can specify source, destination, and wildcards as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** for 0.0.0.0 255.255.255.255 (any host). • The keyword **host** for a single host 0.0.0.0.

	Command or Action	Purpose
Step 3	**ip access-list extended***access-list-number*	Define an extended IPv4 access list using a name, and enter access-list configuration mode. The *name* can be a number from 100 to 199. In access-list configuration mode, enter **permit***protocol source source-wildcard destination destination-wildcard* } .
Step 4	**end**	Return to the privileged EXEC mode.
Step 5	**show access-lists**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To delete an access list, use the **no access-list***access-list-number* global configuration command.

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2:

```
Router(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2
```

Using Class Maps to Define a Traffic Class

You use the **class-map** global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. A class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as CoS value, DSCP value, IP precedence values, or QoS group values, or VLAN IDs. You define match criterion with one or more **match** statements entered in the class-map configuration mode.

Follow these guidelines when configuring class maps:

- A **match-all** class map cannot have more than one classification criterion (one match statement), but a **match-any** class map can contain multiple match statements.
- The match cos and **match vlan** commands are supported only on Layer 2 802.1Q trunk ports.
- You use a class map with the **match vlan** command in the parent policy in input hierarchical policy maps for per-port, per-VLAN QoS on trunk ports. A policy is considered a parent policy map when it has one or more of its classes associated with a child policy map. Each class within a parent policy map is called a parent class. You can configure only the **match vlan** command in parent classes. You cannot configure the **match vlan** command in classes within the child policy map.
- You cannot configure **match qos-group** for an input policy map.
- In an output policy map, no two class maps can have the same classification criteria; that is, the same match qualifiers and values.
- The maximum number of class maps supported on the Cisco ASR 901 router is 256.

Complete the following steps to create a class map and to define the match criterion to classify traffic:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**class-map** [**match-all** | **match-any**] **controller e1***slot/subslot*	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. • (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. • (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched. • For **controller e1***slot/subslot*, specify the name of the class map. If no matching statements are specified, the default is **match-all**. **Note** A **match-all** class map cannot have more than one classification criterion (match statement).
Step 3	**match** {**cos controller e1***slot/subslot* | **ip dscpcontroller e1***slot/subslot*| **ip precedencecontroller e1***slot/subslot* | **qos-groupcontroller e1***slot/subslot* | **vlancontroller e1***slot/subslot*	Define the match criterion to classify traffic. By default, no match criterion is defined. Only one match type per class map is supported. • For **cos controller e1***slot/subslot*, enter a list of up to four CoS values in a single line to match against incoming packets. Separate each value with a space. You can enter multiple **controller e1***slot/subslot* lines to match more than four CoS values. The range is 0 to 7. • For **ip dscpcontroller e1***slot/subslot*, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple **controller e1***slot/subslot* lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms. See the Classification Based on IP DSCP, on page 392. • For **ip precedencecontroller e1***slot/subslot*, enter a list of up to four IPv4 precedence values to match against

	Command or Action	Purpose
		incoming packets. Separate each value with a space. You can enter multiple **controller e1***slot/subslot* lines to match more than four precedence values. The range is 0 to 7. • For **vlancontroller e1***slot/subslot* specify a VLAN ID or a range of VLANs to be used in a parent policy map for per-port, per-VLAN QoS on a trunk port. The VLAN ID range is 1 to 4094. • For **qos-groupcontroller e1***slot/subslot* specify the QoS group number. The range is 0 to 7. Matching of QoS groups is supported only in output policy maps.
Step 4	**end**	Return to the privileged EXEC mode.
Step 5	**show class-map**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

This example shows how to create a class map called **controller e1***slot/subslot*, which matches incoming traffic with DSCP values of 10, 11, and 12.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match ip dscp 10 11 12
Router(config-cmap)# exit
```

Creating a Named Access List

To create a standard or extended named access list, perform the following tasks:

Note Extended ACLs with extended options like DSCP, fragments, option, precedence, time-range, ToS, and TTL are not supported. Only ACLs with source and destination IP addresses are supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	Do one of the following: • **ip access-list {standard | extended}** *name* **Example:** `Router(config)# ip access-list standard acl-std`	Define a standard or extended IP access list using a name. • **standard**—Specifies a standard IP access list. • **extended**—Specifies an extended IP access list. • *name*—Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
Step 4	*permit {source [source-wildcard] | any} log* **Example:** `Router(config-std-nacl)# permit 10.10.10.10 255.255.255.0`	Enters access-list configuration mode, and specifies one or more allowed or denied conditions. This determines whether the packet is passed or dropped. • *source*—Number of the network or host from which the packet is sent in a 32-bit quantity in four-part, dotted-decimal format. • *source-wildcard*—(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • **any**—Specifies any source or destination host as an abbreviation for the source-addr or destination-addr value and the source-wildcard, or destination-wildcard value of 0.0.0.0 255.255.255.255. • **log**—Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)
Step 5	**exit** **Example:** `Router(config-std-nacl)# exit`	Enters the global configuration mode.

	Command or Action	Purpose
Step 6	**class-map class-map-name** **Example:** `Router(config)# class-map class-acl-std`	Defines name for the class map and enters class-map config mode. • class-map-*name*—Name of the class map.

Step 7	**match access-group name access-group-name**
	Example:
	`Router(config-cmap)# match access-group`
	`name acl-std`
		Defines a named ACL for the match criteria.
		• access-group-name—Specifies a named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The name can be up to 40 alphanumeric characters.

What to do Next

After creating a standard access list using names, define a policy map and attach it to the interface. See Creating a Policy Map for Applying a QoS Feature to Network Traffic, on page 419 and Attaching the Policy Map to an Interface, on page 421 for more details.

TCAM with ACL

The scalability of ACLs will change depending on the features configured on the Cisco ASR 901 Router. With on-demand allocation, ACLs can be allocated up to a maximum of 1536 TCAM rules. For more information on troubleshooting scalability, see Troubleshooting Tips, on page 481.

Configuration Examples for ACL

The following is a sample output of the show ip access-lists tcam command.

```
Router# show ip access-lists tcam1
!consumes 1 TCAM entry per rule + a default rule.
!4 TCAM entries in this case]
Extended IP access list tcam1
    10 permit ip host 1.1.1.12 any
    20 deny ip host 2.2.2.11 any
    30 permit ip host 1.1.1.13 any
Router#
Router# show run int gig 0/1
Building configuration...
Current configuration : 221 bytes
!
interface GigabitEthernet0/1
 no ip address
 ip access-group tcam1 in
 negotiation auto
Router# show platform tcam detailed
Ingress     : 6/8 slices, 1536/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress      : 0/4 slices, 0/512 entries used
Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 29/256
Slice allocated to: Layer-2 Classify and Assign Group
```

```
Slice ID: 4
Stage: Pre-Ingress
Mode: Double
Entries used: 11/128
Slice allocated to: L2CP
Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 27/128
Slice allocated to: L2 Post-Switch Processing Group
Slice ID: 5
Stage: Ingress
Mode: Single
Entries used: 4/256
Slice allocated to: Port ACLs
Slice ID: 7
Stage: Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: OAM, Ethernet loopback, Y.1731 DMM
Slice ID: 3
Stage: Ingress
Mode: Double
Entries used: 15/128
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
Slice ID: 8
Stage: Ingress
Mode: Double
Entries used: 220/256
Slice allocated to: Quality Of Service
```

Verifying Named Access List

To verify the standard or extended access list configuration, use the show access-lists command as given below:

```
Router# show access-lists tes456
Extended IP access list tes456
    10 permit ip host 10.1.1.1 192.168.1.0 0.0.0.255
    20 permit ip host 10.1.1.1 192.168.2.0 0.0.0.255
    30 permit ip host 10.1.1.1 192.168.3.0 0.0.0.255
    40 permit ip host 10.1.1.1 192.168.4.0 0.0.0.255
    50 permit ip host 10.1.1.1 192.168.5.0 0.0.0.255
    60 permit ip host 10.1.1.1 192.168.6.0 0.0.0.255
    70 permit ip host 10.1.1.1 192.168.7.0 0.0.0.255
    80 permit ip host 10.1.1.1 192.168.8.0 0.0.0.255
    90 permit ip host 10.1.1.1 192.168.9.0 0.0.0.255
!
!
!
```

To verify the ACL-based QoS classification, use the show policy-map command as given below:

```
Router# show policy-map interface gigabitethernet 0/0
 GigabitEthernet0/0
  Service-policy input: test
    Class-map: test (match-any)
      0 packets, 244224 bytes
      5 minute offered rate 6000 bps, drop rate 0000 bps
      Match: access-group name test
      QoS Set
```

```
        dscp af32
          Packets marked 0
        No marking statistics available for this class
    Class-map: class-default (match-any)
      0 packets, 239168 bytes
      5 minute offered rate 6000 bps, drop rate 0000 bps
      Match: any
```

Configuration Example for Named Access List

The following is the sample configuration of a named access list on the Cisco ASR 901 router.

Note In the following configuration, both the ACL and ACL-based QoS are exclusive of each other and are not related to each other.

```
Router# show running-config
Building configuration...
Current configuration : 11906 bytes
!
! Last configuration change at 22:51:12 UTC Sun May 13 2001
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!card type command needed for slot/vwic-slot 0/0
enable password lab
!
no aaa new-model
ip cef
!
!
!
!
no ipv6 cef
!
!
mpls label protocol ldp
multilink bundle-name authenticated
!
table-map sach
 map from  0 to 0
 map from  1 to 1
 map from  2 to 2
 map from  3 to 3
 map from  4 to 3
 map from  5 to 5
 map from  6 to 6
 map from  7 to 7
 default copy
!
l3-over-l2 flush buffers
```

```
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
username lab password 0 lab
!
!
!
class-map match-any test
 match access-group name test123
class-map match-all test456
 match access-group name tes456
class-map match-any test1
 match access-group name test123
!
policy-map test
 class test456
 class class-default
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
!
interface Port-channel1
 no negotiation auto
!
interface Port-channel8
 no negotiation auto
 service-policy input test
 service instance 2000 ethernet
  encapsulation dot1q 2000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2000
 !
!
interface GigabitEthernet0/0
 no negotiation auto
 service-policy input test
!
interface GigabitEthernet0/1
 shutdown
 no negotiation auto
!
interface GigabitEthernet0/2
 negotiation auto
 channel-group 8 mode active
!
interface GigabitEthernet0/3
 no negotiation auto
!
interface GigabitEthernet0/4
 negotiation auto
 service instance 200 ethernet
  encapsulation untagged
  bridge-domain 200
```

```
 !
!
interface GigabitEthernet0/5
 negotiation auto
!
interface GigabitEthernet0/6
 no negotiation auto
!
interface GigabitEthernet0/7
 no negotiation auto
!
interface GigabitEthernet0/8
 negotiation auto
 channel-group 8 mode active
!
interface GigabitEthernet0/9
 no negotiation auto
!
interface GigabitEthernet0/10
 no negotiation auto
!
interface GigabitEthernet0/11
 no negotiation auto
!
interface FastEthernet0/0
 ip address 10.104.99.152 255.255.255.0
 full-duplex
!
interface Vlan1
 no ip address
!
interface Vlan108
 ip address 11.11.11.1 255.255.255.0
 mpls ip
!
interface Vlan200
 ip address 10.1.1.2 255.255.255.0
 mpls ip
!
interface Vlan2000
 ip address 200.1.1.1 255.255.255.0
!
router ospf 1
 router-id 10.10.10.1
 network 10.10.10.1 0.0.0.0 area 0
 network 200.1.1.0 0.0.0.255 area 0
!
router bgp 1
 bgp router-id 10.10.10.1
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 2
 neighbor 10.10.10.50 remote-as 1
 neighbor 10.10.10.50 update-source Loopback0
!
ip forward-protocol nd
!
!
no ip http server
ip route 0.0.0.0 0.0.0.0 10.104.99.1
!
ip access-list extended check
 deny   ip any any
ip access-list extended tes456
 permit ip host 10.1.1.1 192.168.1.0 0.0.0.255
```

```
permit ip host 10.1.1.1 192.168.2.0 0.0.0.255
permit ip host 10.1.1.1 192.168.3.0 0.0.0.255
permit ip host 10.1.1.1 192.168.4.0 0.0.0.255
permit ip host 10.1.1.1 192.168.5.0 0.0.0.255
permit ip host 10.1.1.1 192.168.6.0 0.0.0.255
permit ip host 10.1.1.1 192.168.7.0 0.0.0.255
permit ip host 10.1.1.1 192.168.8.0 0.0.0.255
permit ip host 10.1.1.1 192.168.9.0 0.0.0.255
permit ip host 10.1.1.1 192.168.10.0 0.0.0.255
permit ip host 10.1.1.1 192.168.11.0 0.0.0.255
permit ip host 10.1.1.1 192.168.12.0 0.0.0.255
permit ip host 10.1.1.1 192.168.13.0 0.0.0.255
permit ip host 10.1.1.1 192.168.14.0 0.0.0.255
permit ip host 10.1.1.1 192.168.15.0 0.0.0.255
permit ip host 10.1.1.1 192.168.16.0 0.0.0.255
permit ip host 10.1.1.1 192.168.17.0 0.0.0.255
permit ip host 10.1.1.1 192.168.18.0 0.0.0.255
permit ip host 10.1.1.1 192.168.19.0 0.0.0.255
permit ip host 10.1.1.1 192.168.20.0 0.0.0.255
permit ip host 10.1.1.1 192.168.21.0 0.0.0.255
permit ip host 10.1.1.1 192.168.22.0 0.0.0.255
permit ip host 10.1.1.1 192.168.23.0 0.0.0.255
permit ip host 10.1.1.1 192.168.24.0 0.0.0.255
permit ip host 10.1.1.1 192.168.25.0 0.0.0.255
permit ip host 10.1.1.1 192.168.26.0 0.0.0.255
permit ip host 10.1.1.1 192.168.27.0 0.0.0.255
permit ip host 10.1.1.1 192.168.28.0 0.0.0.255
permit ip host 10.1.1.1 192.168.29.0 0.0.0.255
permit ip host 10.1.1.1 192.168.30.0 0.0.0.255
permit ip host 10.1.1.1 192.168.31.0 0.0.0.255
permit ip host 10.1.1.1 192.168.32.0 0.0.0.255
permit ip host 10.1.1.1 192.168.33.0 0.0.0.255
permit ip host 10.1.1.1 192.168.34.0 0.0.0.255
permit ip host 10.1.1.1 192.168.35.0 0.0.0.255
permit ip host 10.1.1.1 192.168.36.0 0.0.0.255
permit ip host 10.1.1.1 192.168.37.0 0.0.0.255
permit ip host 10.1.1.1 192.168.38.0 0.0.0.255
permit ip host 10.1.1.1 192.168.40.0 0.0.0.255
permit ip host 10.1.1.1 192.168.41.0 0.0.0.255
permit ip host 10.1.1.1 192.168.42.0 0.0.0.255
permit ip host 10.1.1.1 192.168.43.0 0.0.0.255
permit ip host 10.1.1.1 192.168.44.0 0.0.0.255
permit ip host 10.1.1.1 192.168.45.0 0.0.0.255
permit ip host 10.1.1.1 192.168.46.0 0.0.0.255
permit ip host 10.1.1.1 192.168.47.0 0.0.0.255
permit ip host 10.1.1.1 192.168.48.0 0.0.0.255
permit ip host 10.1.1.1 192.168.49.0 0.0.0.255
permit ip host 10.1.1.1 192.168.50.0 0.0.0.255
permit ip host 10.1.1.1 192.168.51.0 0.0.0.255
permit ip host 10.1.1.1 192.168.52.0 0.0.0.255
permit ip host 10.1.1.1 192.168.53.0 0.0.0.255
permit ip host 10.1.1.1 192.168.54.0 0.0.0.255
permit ip host 10.1.1.1 192.168.55.0 0.0.0.255
permit ip host 10.1.1.1 192.168.56.0 0.0.0.255
permit ip host 10.1.1.1 192.168.57.0 0.0.0.255
permit ip host 10.1.1.1 192.168.58.0 0.0.0.255
permit ip host 10.1.1.1 192.168.59.0 0.0.0.255
permit ip host 10.1.1.1 192.168.60.0 0.0.0.255
permit ip host 10.1.1.1 192.168.61.0 0.0.0.255
permit ip host 10.1.1.1 192.168.62.0 0.0.0.255
permit ip host 10.1.1.1 192.168.63.0 0.0.0.255
permit ip host 10.1.1.1 192.168.64.0 0.0.0.255
permit ip host 10.1.1.1 192.168.65.0 0.0.0.255
permit ip host 10.1.1.1 192.168.66.0 0.0.0.255
```

```
 permit ip host 10.1.1.1 192.168.67.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.68.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.69.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.70.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.71.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.72.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.73.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.74.0 0.0.0.255
 permit ip host 10.1.1.1 192.168.75.0 0.0.0.255
ip access-list extended test123
 remark 1
 permit ip host 10.1.1.1 192.168.1.0 0.0.0.255
 remark 2
 permit ip host 10.1.1.1 192.168.2.0 0.0.0.255
 remark 3
 permit ip host 10.1.1.1 192.168.3.0 0.0.0.255
 remark 4
 permit ip host 10.1.1.1 192.168.4.0 0.0.0.255
 remark 5
 permit ip host 10.1.1.1 192.168.5.0 0.0.0.255
 remark 6
 permit ip host 10.1.1.1 192.168.6.0 0.0.0.255
 remark 7
 permit ip host 10.1.1.1 192.168.7.0 0.0.0.255
 remark 8
 permit ip host 10.1.1.1 192.168.8.0 0.0.0.255
 remark 9
 permit ip host 10.1.1.1 192.168.9.0 0.0.0.255
 remark 10
 permit ip host 10.1.1.1 192.168.10.0 0.0.0.255
 remark 11
 permit ip host 10.1.1.1 192.168.11.0 0.0.0.255
 remark 12
 permit ip host 10.1.1.1 192.168.12.0 0.0.0.255
 remark 13
 permit ip host 10.1.1.1 192.168.13.0 0.0.0.255
 remark 14
 permit ip host 10.1.1.1 192.168.14.0 0.0.0.255
 remark 15
 permit ip host 10.1.1.1 192.168.15.0 0.0.0.255
 remark 16
 permit ip host 10.1.1.1 192.168.16.0 0.0.0.255
 remark 17
 permit ip host 10.1.1.1 192.168.17.0 0.0.0.255
 remark 18
 permit ip host 10.1.1.1 192.168.18.0 0.0.0.255
 remark 19
 permit ip host 10.1.1.1 192.168.19.0 0.0.0.255
 remark 20
 permit ip host 10.1.1.1 192.168.20.0 0.0.0.255
 remark 21
 permit ip host 10.1.1.1 192.168.21.0 0.0.0.255
 remark 22
 permit ip host 10.1.1.1 192.168.22.0 0.0.0.255
 remark 23
 permit ip host 10.1.1.1 192.168.23.0 0.0.0.255
 remark 24
 permit ip host 10.1.1.1 192.168.24.0 0.0.0.255
 remark 25
 permit ip host 10.1.1.1 192.168.25.0 0.0.0.255
 remark 26
 permit ip host 10.1.1.1 192.168.26.0 0.0.0.255
 remark 27
 permit ip host 10.1.1.1 192.168.27.0 0.0.0.255
```

```
 remark 28
 permit ip host 10.1.1.1 192.168.28.0 0.0.0.255
 remark 29
 permit ip host 10.1.1.1 192.168.29.0 0.0.0.255
 remark 30
 permit ip host 10.1.1.1 192.168.30.0 0.0.0.255
 remark 31
 permit ip host 10.1.1.1 192.168.31.0 0.0.0.255
 remark 32
 permit ip host 10.1.1.1 192.168.32.0 0.0.0.255
 remark 33
 permit ip host 10.1.1.1 192.168.33.0 0.0.0.255
 remark 34
 permit ip host 10.1.1.1 192.168.34.0 0.0.0.255
 remark 35
 permit ip host 10.1.1.1 192.168.35.0 0.0.0.255
 remark 36
 permit ip host 10.1.1.1 192.168.36.0 0.0.0.255
 remark 37
 permit ip host 10.1.1.1 192.168.37.0 0.0.0.255
 remark 38
 permit ip host 10.1.1.1 192.168.38.0 0.0.0.255
 remark 39
 permit ip host 10.1.1.1 192.168.39.0 0.0.0.255
 remark 40
 permit ip host 10.1.1.1 192.168.40.0 0.0.0.255
 remark 41
 permit ip host 10.1.1.1 192.168.41.0 0.0.0.255
 remark 42
 permit ip host 10.1.1.1 192.168.42.0 0.0.0.255
 remark 43
 permit ip host 10.1.1.1 192.168.43.0 0.0.0.255
 remark 44
 permit ip host 10.1.1.1 192.168.44.0 0.0.0.255
 remark 45
 permit ip host 10.1.1.1 192.168.45.0 0.0.0.255
 remark 46
 permit ip host 10.1.1.1 192.168.46.0 0.0.0.255
 remark 47
 permit ip host 10.1.1.1 192.168.47.0 0.0.0.255
 remark 48
 permit ip host 10.1.1.1 192.168.48.0 0.0.0.255
 remark 49
 permit ip host 10.1.1.1 192.168.49.0 0.0.0.255
 remark 50
 permit ip host 10.1.1.1 192.168.50.0 0.0.0.255
!
access-list 2600 permit ip any any
!
mpls ldp router-id Loopback0
!
!
control-plane
!
environment monitor
!
line con 0
line aux 0
 transport preferred none
 transport output lat pad telnet rlogin udptn ssh
line vty 0 4
 exec-timeout 3 3
 password lab
 login
```

```
!
exception crashinfo buffersize 128
!
!
end
```

Access Control Lists for IPv6 Traffic Filtering

The standard ACL functionality in IPv6 is similar to standard ACLs in IPv4. Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses and inbound interface. Each access list has an implicit deny statement at the end. IPv6 ACLs are defined and their deny and permit conditions are set using the ipv6 access-list command with the deny and permit keywords in global configuration mode.

Creating and Configuring an IPv6 ACL for Traffic Filtering

Perform the following task to create and configure IPv6 ACL to filter traffic.

Restrictions

- Port based ACLs are not supported.
- Outbound ACLs are not supported due to hardware limitations.
- Only named ACLs are supported for IPv6 ACLs.
- Only standard IPv6 headers are supported in Layer 3 options. Extended IPv6 headers are not supported.
- Only layer 3 options such as dscp and flow-label are supported for IPv6 ACLs.
- Only layer 4 options such as ack, eq, established, fin, gt, lt, psh, ranges, rst, and syn are supported for IPv6 ALCs.
- The scale of IPv6 ACL varies based on the QoS, Layer 4 ACL, multicast, and storm features configured on the Cisco ASR 901 Router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ipv6 access-list access-list-***name* **Example:** `Router(config)# ip access-list source`	Defines an IPv6 ACL, and enters IPv6 access list configuration mode. • *name*—Name of the IPv6 access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

	Command or Action	Purpose

Step 4	Do one of the following:
	• *permit protocol {source [source-ipv6-prefix/prefix-length] | any | host source-ipv6-address | auth]}[operator [port-number]]{destination [destination-ipv6-prefix | prefix-length | any | host destination-ipv6-address | auth]} [operator [port-number]] [dest-option-type [doh-number | doh-type]] [dscp value] [flow-label value][fragments][hbh][log][log-input] [routing][routing-type routing-number] [sequence value][time-range name]*
	• or deny *protocol {source [source-ipv6-prefix/prefix-length] | any | host source-ipv6-address | auth]}[operator [port-number]]{destination [destination-ipv6-prefix | prefix-length | any | host destination-ipv6-address | auth]} [operator [port-number]] [dest-option-type [doh-number | doh-type]] [dscp value] [flow-label value][fragments][hbh][log][log-input] [routing][routing-type routing-number] [sequence value][time-range name]*
	Example:
	`Router(config-ipv6-acl)# permit ipv6 host 2001:DB8:0:4::32 any eq telnet`
	Example:
	`Router(config-ipv6-acl)# deny tcp host 2001:1::2 eq 30 any dscp af11`
		Specifies permit or deny conditions for an IPv6 ACL.
		Enters access-list configuration mode, and specifies one or more allowed or denied conditions. This determines whether the packet is passed or dropped.
		• *source*—Number of the network or host from which the packet is sent in a 32-bit quantity in four-part, dotted-decimal format.
		• *source-wildcard*—(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
		• **any**—Specifies any source or destination host as an abbreviation for the source-addr or destination-addr value and the source-wildcard, or destination-wildcard value of 0.0.0.0 255.255.255.255.
		• **log**—Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)

Configuration Example

This section shows sample configuration for creating and configuring the IPv6 ACL on the Cisco ASR 901 router.

```
ipv6 access-list source
deny tcp host 2001:1::2 eq 30 any dscp af11
permit ipv6 any any
```

Applying the IPv6 ACL to an Interface

Perform the following task to apply the IPv6 ACL to an interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 100`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**ipv6 traffic-filter** *access-list-name* **in** **Example:** `Router(config-if) # ipv6 traffic-filter source in`	Applies the specified IPv6 access list to the SVI interface specified in the previous step. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.

Configuration Example

This section shows sample configuration for applying the IPv6 ACL on an interface.

```
int vlan 100
ipv6 traffic-filter source in
end
```

QoS Treatment for Performance-Monitoring Protocols

This section contains the following topics:

Cisco IP-SLAs

For information about Cisco IP service level agreements (IP-SLAs), see Understanding Cisco IOS IP SLAs, page 3-2 .

QoS Treatment for IP-SLA Probes

The QoS treatment for IP-SLA and TWAMP probes must exactly reflect the effects that occur to the normal data traffic crossing the device.

The generating device should not change the probe markings. It should queue these probes based on the configured queueing policies for normal traffic.

Marking

By default, the class of service (CoS) marking of CFM traffic (including IP SLAs using CFM probes) is not changed. This feature cannot change this behavior.

By default, IP traffic marking (including IP SLA and TWAMP probes) is not changed. This feature can change this behavior.

Queuing

The CFM traffic (including IP SLAs using CFM probes) is queued according to its CoS value and the output policy map configured on the egress port, similar to normal traffic. This feature cannot change this behavior.

IP traffic (including IP SLA and TWAMP probes) is queued according to the markings specified in the **cpu traffic qos** global configuration command and the output policy map on the egress port. If this command is not configured, all IP traffic is statically mapped to a queue on the egress port.

QoS Marking for CPU-Generated Traffic

You can use QoS marking to set or modify the attributes of traffic from the CPU. The QoS marking action can cause the CoS bits in the packet to be rewritten or leave the CoS, DSCP, or IP precedence bits in the packet unchanged. QoS uses packet markings to identify certain traffic types and how to treat them on the local router and the network.

You can also use marking to assign traffic to a QoS group within the router. This QoS group is an internal label that does not modify the packet, but it can be used to identify the traffic type when configuring egress queuing on the network port.

You can specify and mark traffic CPU-generated traffic by using these global configuration commands:

cpu traffic qos cos {*cos_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-ma**p *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

You can mark a QoS group by configuring an explicit value or by using the **table-map** keyword. Table maps list specific traffic attributes and map (or convert) them to another attribute. A table map establishes a to-from relationship for the attribute and defines the change to be made:

- Marking CoS by using the CoS, or the IP-DSCP, or the IP precedence of IP CPU-packets
- Marking CoS by using the CoS of non-IP CPU-packets.
- Marking IP DSCP by using the CoS, or the IP-DSCP, or the IP precedence of the CPU-packet
- Marking IP precedence by using the CoS, or the IP-DSCP, or the IP precedence of the CPU-packet

You can configure either IP-DSCP or IP precedence marking.

You can also simultaneously configure marking actions to modify CoS, IP-DSCP or IP precedence, and QoS group.

The **cpu traffic qos** command specifies the traffic to which it applies: all CPU traffic, only CPU IP traffic, or only CPU non-IP traffic. All other traffic retains its QoS markings. This feature does not affect CFM traffic (including Layer 2 IP SLA probes using CFM).

QoS Queuing for CPU-Generated Traffic

You can use the QoS markings established for the CPU-generated traffic by the **cpu traffic qos** global configuration command as packet identifiers in the class-map of an output policy-map to map CPU traffic to class-queues in the output policy-map on the egress port. You can then use output policy-maps on the egress port to configure queuing and scheduling for traffic leaving the router from that port.

If you want to map *all* CPU-generated traffic to a single class in the output policy-maps without changing the CoS, IP DSCP, or IP-precedence packet markings, you can use QoS groups for marking CPU-generated traffic.

If you want to map *all* CPU-generated traffic to classes in the output policy maps based on the CoS without changing the CoS packet markings, you can use the table map:

- Configure CoS marking by using **CoS** as the **map from** value *without* a table map.
- Configure CoS marking using **CoS** as the **map from** value *with* a table map, using only the **default** and **copy** keywords.

For details about table maps, see the Table Maps, on page 397.

Using the **cpu traffic qos** global configuration command with table mapping, you can configure multiple marking and queuing policies to work together or independently. You can queue native VLAN traffic based on the CoS markings configured using the **cpu traffic qos** global configuration command.

The **cpu traffic qos** command specifies the traffic to which it applies: all CPU traffic, only CPU-IP traffic, or only CPU non-IP traffic. All other traffic is statically mapped to a CPU-default queue on the egress port. All CFM traffic (including Layer 2 IP SLA probes using CFM) is mapped to classes in the output policy map, and queued based on their CoS value.

Extending QoS for MLPPP

Configuring Class-map for Matching MPLS EXP Bits

Complete the following steps to configure class-map for matching MPLS experimental bits.

Procedure

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

	Command or Action	Purpose

Step 3	**class-map match-any** *class-map-name*
	Example:
	`Router(config)#`
	`class-map match-any mplsexp`
		Creates a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode:
		• *class-map-name*—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.

Step 4	**match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match mpls experimental topmost 5`	Matches the experimental (EXP) value in the topmost label header. • *number*—Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7. **Note** In this configuration packets with experimental bits of value 5 are matched. Repeat this step to configure more values. If any one of the values is matched, action pertaining to the class-map is performed.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.

Configuring Class-map for Matching IP DSCP Value

This classification is required for all the packets flowing without an MPLS header like normal IP packets flowing through an MLPPP Interface.

Complete the following steps to configure class-map for matching IP DSCP Values.

Procedure

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

	Command or Action	Purpose

Step 3	**class-map match-any** *class-map-name*
	Example:
	`Router(config)#`
	`class-map match-any matchdscp`
		Creates a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode:
		• *class-map-name*—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.

Step 4	**match ip dscp** *[dscp-value...dscp-value]* **Example:** `Router(config-cmap)# match ip dscp af11`	Identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Class Selector (CS) values as a match criterion. • *dscp-value*—The DSCP value used to identify a DSCP value. **Note** In this configuration packets with IP DSCP of value af11 are matched. Repeat this step to configure more values. If any one of the values is matched, action pertaining to the class-map is performed.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.

Configuring Class-map for Matching MPLS EXP Bits or IP DSCP Value

In this configuration, all MPLS packets flowing through the MLPPP Interface EXP value are matched and all the IP Packets flowing through the MLPPP Interface IP DSCP value are matched.

Complete the following steps to configure class-map for matching MPLS EXP bits or IP DSCP Values.

Procedure

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

	Command or Action	Purpose
Step 3	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any matchdscp`	Creates a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode: • *class-map-name*—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.
Step 4	**match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match mpls experimental topmost 5`	Matches the experimental (EXP) value in the topmost label header. • *number*—Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.
Step 5	**match ip dscp** *dscp-value* **Example:** `Router(config-cmap)# match ip dscp af11`	Identifies the DSCP values as a match criterion. • *dscp-value*—The DSCP value used to identify a DSCP.
Step 6	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.

Configuring a Policy-map

Complete the following steps to configure a policy-map.

Procedure

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

	Command or Action	Purpose
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map mplsomlpppqos`	Configures a policy map that can be attached to one or more interfaces and enters QoS policy-map configuration mode. • *policy-map-name*—Name of the policy map.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class mplsexp`	Specifies the name of the class whose policy you want to create. • *class-name*—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.
Step 5	**priority percent** *percentage* **Example:** `Router(config-pmap-c)# priority percent 10`	Configures priority to a class of traffic belonging to a policy map. • *percentage*—Total available bandwidth to be set aside for the priority class.
Step 6	**class** *class-name* **Example:** `Router(config-pmap-c)# class matchdscp`	Specifies the name of the class whose policy you want to create.
Step 7	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Configures the bandwidth allocated for a class belonging to a policy map. • percentage—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.
Step 8	**class** *class-name* **Example:** `Router(config-pmap-c)# class mplsexpvalues`	Specifies the name of the class whose policy you want to create.
Step 9	**set mpls experimental topmost** *mpls-exp-value* **Example:** `Router(config-pmap-c)# set mpls experimental topmost 4`	Sets the MPLS EXP field value in the topmost label on an interface. • *mpls-exp-value*—Specifies the value used to set MPLS experimental bits defined by the policy map.

	Command or Action	Purpose
Step 10	**class** *class-name* **Example:** `Router(config-pmap-c)# class matchdscpvalues`	Specifies the name of the class whose policy you want to create.
Step 11	**set dscp** *dscp-value* **Example:** `Router(config-pmap-c)# set dscp af41`	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte. • *dscp-value*—The DSCP value used to identify a DSCP.
Step 12	**class** *class-name* **Example:** `Router(config-pmap-c)# class mplsexp_or_dscp`	Specifies the name of the class whose policy you want to create.
Step 13	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Configures the bandwidth allocated for a class belonging to a policy map.
Step 14	**set mpls experimental topmost** *mpls-exp-value* **Example:** `Router(config-pmap-c)# set mpls experimental topmost 1`	Sets the MPLS EXP field value in the topmost label on an interface.
Step 15	**set dscp** *dscp-value* **Example:** `Router(config-pmap-c)# set dscp af11`	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 16	**queue-limit** *queue-limit-size* **packets** **Example:** `Router(config-pmap-c)# queue-limit 80 packets`	Configures the queue limit (size) for a class in packets. • *queue-limit-size*—The maximum size of the queue. • **packets**—Indicates that the unit of measure is packets. **Note** To configure **queue-limit**, you should configure either priority percent or bandwidth percent.

	Command or Action	Purpose
Step 17	**end** **Example:** `Router(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode.

Attaching the Policy-map to MLPPP Interface

Complete the following steps to attach the policy-map to an MLPPP interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink5`	Creates a multilink bundle and enters the interface configuration mode: • *group-number*—Number of the multilink bundle.
Step 4	**ip address** *address* [*subnet mask*] **Example:** `Router(config-if)# ip address 84.1.2.3 255.255.255.0`	Assigns an IP address to the multilink interface. • *address*— IP address. • *subnet mask* —Network mask of IP address.
Step 5	**load-interval** *interval* **Example:** `Router(config-if)# load-interval 30`	Configures the length of time for which data is used to compute load statistics. • *interval*—Length of time for which data is used to compute load statistics.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interfaces.

	Command or Action	Purpose
Step 7	**keepalive** *period* **Example:** `Router(config-if)# keepalive 1`	Enables keepalive packets and specifies the number of times that the router tries to send keepalive packets without a response before bringing down the interface. • *period*—Time interval, in seconds, between messages sent by the router to ensure that a network interface is alive.
Step 8	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface.
Step 9	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 3`	Restricts a physical link to join only one designated multilink group interface. • *group-number*—Multilink group number (a nonzero number).
Step 10	**ppp multilink endpoint string** *char-string* **Example:** `Router(config-if)# ppp multilink endpoint string ML3`	Configures the default endpoint discriminator the system uses when negotiating the use of MLPPP with the peer. • *char-string*—Uses the supplied character string.
Step 11	**service-policy output** *policy-map-name* **Example:** `Router(config-if)# service-policy output mplsomlpppqos`	Attaches a policy map to an interface that will be used as the service policy for the interface. • *policy-map-name*—The name of a service policy map (created using the **policy-map** command) to be attached.
Step 12	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Re-marking IP DSCP Values of CPU Generated Traffic

Complete the following steps to re-mark the IP DSCP values of the CPU generated traffic.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables the privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.

Step 3	**cpu traffic ppp set ip dscp cs5**
	Example:
	`Router(config)#`
	`cpu traffic ppp set ip dscp cs5`
		Re-marks the IP DSCP value to give the desired QoS treatment to CPU generated traffic.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits the configuration mode.

Re-marking MPLS EXP Values of CPU Generated Traffic

Complete the following steps to re-mark the MPLS EXP values of the CPU generated traffic.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**cpu traffic ppp set mpls experimental topmost** *number* **Example:** `Router(config)# cpu traffic ppp set mpls experimental topmost 4`	Re-marks Multiprotocol Label Switching (MPLS) experimental (EXP) topmost value to give the desired QoS treatment to CPU generated traffic. • number—MPLS EXP field in the topmost label header. Valid values are 0 to 7.
Step 4	**exit** **Example:**	Exits the configuration mode.

	Command or Action	Purpose
	`Router(config)# exit`	

Configuring a Policy-map to Match on CS5 and EXP4

Complete the following steps to configure a policy-map to match on CS5 and EXP4.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-any dscp** *cs-value* **Example:** `Router(config)# class-map match-any dscpcs5`	Configures a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode.
Step 4	**match ip dscp** *cs-value* **Example:** `Router(config-cmap)# match ip dscp cs5`	Identify one or more differentiated service code point (DSCP) CS value as a match criterion. • *cs-value* —The Class Selector(CS) value.
Step 5	**class-map match-any** *class-map-name* **Example:** `Router(config-cmap)# class-map match-any exp4`	Creates a class map to be used for matching packets to a specified class. • *class-map-name*—Name of the class for the class map.
Step 6	**match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match mpls experimental topmost 4`	Matches the experimental (EXP) value in the topmost label header. • *number*—Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

	Command or Action	Purpose
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config-cmap)# policy-map dscp_exp`	Configures a policy map that can be attached to one or more interfaces and enters QoS policy-map configuration mode. • *policy-map-name*—Name of the policy map.
Step 8	**class** *class-name* **Example:** `Router(config-pmap)# class dscpcs5`	Specifies the name of the class whose policy you want to create. • *class-name*—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.
Step 9	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Configures the bandwidth allocated for a class belonging to a policy map. • *percentage*—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.
Step 10	**set ip dscp** *cs-value* **Example:** `Router(config-pmap-c)# set ip dscp cs6`	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 11	**class** *class-name* **Example:** `Router(config-pmap-c)# class exp4`	Specifies the name of the class whose policy you want to create.
Step 12	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Configures the bandwidth allocated for a class belonging to a policy map. • *percentage*—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.
Step 13	**set mpls experimental topmost** *mpls-exp-value* **Example:** `Router(config-pmap-c)# set mpls experimental topmost 6`	Sets the MPLS EXP field value in the topmost label on an interface. • *mpls-exp-value*—Specifies the value used to set MPLS experimental bits defined by the policy map.

	Command or Action	Purpose
Step 14	**class** *class-name* **Example:** `Router(config-pmap-c)# class class-default`	Specifies the name of the class whose policy you want to create.
Step 15	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Configures the bandwidth allocated for a class belonging to a policy map.
Step 16	**end** **Example:** `Router(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode.

Attaching the Policy-map to Match on CS5 and EXP4 to MLPPP Interface

See Attaching the Policy-map to MLPPP Interface, on page 467 for configuration steps.

Note DSCP CS6 and EXP 6 are default values. If you configure the CPU generated traffic to these values using CLI, you cannot see them in the output of the **show running-configuration** command.

Configuration Examples for Extending QoS for MPLS over MLPPP

Configuring Class-map for Matching MPLS EXP Bits

The following example shows a configuration of class-map for matching MPLS EXP bits.

```
Building configuration...
Current configuration : 101 bytes
!
class-map match-any mpls_exp5
 match mpls experimental topmost 5
!
```

Configuring Class-map for Matching IP DSCP Value

The following example shows a configuration of class-map for matching IP DSCP value.

```
Building configuration...
Current configuration : 101 bytes
!
!
class-map match-any dscpaf11
```

```
 match ip dscp af11
!
```

Configuring Class-map for Matching MPLS EXP Bits or IP DSCP Value

The following example shows a configuration of class-map for matching MPLS EXP Bits or IP DSCP value.

```
Building configuration...
Current configuration : 101 bytes
!
!
class-map match-any mplsexp_or_cos
 match mpls experimental topmost 4
 match ip dscp af41
!
```

Configuring a Policy-map

The following example shows a configuration of a policy-map.

```
Building configuration...
Current configuration : 101 bytes
!
policy-map mplsomlpppqos
 class mplsexp
  priority percent 10
 class mplsexpvalues
  set mpls experimental topmost 4
 class matchdscp
  bandwidth percent 20
 class matchdscpvalues
  set dscp af41
 class mplsexp_or_dscp
  bandwidth percent 20
  queue-limit 80 packets
  set mpls experimental topmost 1
  set dscp af11
!
```

Configuring a Policy-map to Match on CS5 and EXP 4

The following example shows a configuration of a policy-map.

```
Building configuration...
Current configuration : 101 bytes
!
class-map match-any dscpcs5
 match ip dscp cs5
class-map match-any exp4
 match mpls experimental topmost 4
policy-map dscp_exp
 class dscpcs5
  bandwidth percent 20
  set ip dscp cs6
 class exp4
  bandwidth percent 20
  set mpls experimental topmost 6
 class class-default
  bandwidth percent 20
!
```

Attaching the Policy-map to MLPPP Interface

The following example shows a configuration of attaching the policy-map to MLPPP interface.

```
Building configuration...
Current configuration : 101 bytes
!
!
interface Multilink3
 ip address 84.1.2.3 255.255.255.0
 load-interval 30
 mpls ip
 keepalive 1
 ppp multilink
 ppp multilink group 3
 ppp multilink endpoint string ML3
 service-policy output mplsomlpppqos
!
```

Configuring Egress Shaping on the MLPPP Interfaces

Configuring a Class-map

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any QOS-GROUP5`	Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode.
Step 4	Choose one of the following: • **match qos-group** *qos-group-value* • **match dscp** *dscp-value* • **match mpls experimental topmost** *number* **Example:** `Router(config-cmap)# match qos-group 5`	Identifies a specific quality of service (QoS) group value or DSCP value or MPLS EXP number as a match criterion.

What to do next

Configure the policy-map with shaping and bandwidth.

Configuring the Policy-map with Shaping

The shape rate provides a maximum rate limit for the traffic class.

In this procedure, the QOS-GROUP5 traffic class is shaped to an average rate of 100 Kbps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map SHAPE_BW`	Configures a policy map that can be attached to an interface.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class QOS-GROUP5`	Specifies the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy.
Step 5	**shape average** *mean-rate* **Example:** `Router(config-pmap)# shape average 100000`	Shapes traffic to the indicated bit rate according to the algorithm specified.

What to do next

Attach the policy-map on the MLPPP interface.

Attaching the Policy-map on the MLPPP Interface

This procedure attaches the policy-map to the MLPPP interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 1`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# no ip address`	Disables IP processing.
Step 5	**service-policy output** *policy-map-name* **Example:** `Router(config-if)# service-policy output SHAPE`	Attaches a policy map to an output interface.
Step 6	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 111 ethernet`	Configures a service instance and enters service instance configuration mode.
Step 7	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 111`	Configures encapsulation type for the service instance.
Step 8	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 9	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 11`	Configures the bridge domain ID.

Verifying the Egress Shaping over MLPPP Interface

To verify the configuration of Egress Shaping over MLPPP Interface, use the **show** command as shown in the example below:

```
Router# show policy-map interface multilink multilink1

 Multilink1

  Service-policy output: pshape
```

```
    Class-map: QOS-GROUP5 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 5
      Queueing
      queue limit 25 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 100000, bc 400, be 400
      target shape rate 100000

    Class-map: class-default (match-any)
      0 packets, 4788 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any

      queue limit 125000 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
```

Example: Configuring Egress Shaping over MLPPP Interface

The following is a sample configuration of egress shaping over MLPPP interface.

```
class-map match-any QOS-GROUP5
              match qos-group 5

          policy-map SHAPE
            class QOS-GROUP5
              shape average 100000

          interface Multilink1
            no ip address
            service-policy output SHAPE
            service instance 111 ethernet
               encapsulation dot1q 111
               rewrite ingress tag pop 1 symmetric
               bridge-domain 11
```

Verifying MPLS over MLPPP Configuration

To verify the configuration of MPLS over MLPPP, use the **following** commands as shown in the examples below:

To verify the details of a class-map created for matching MPLS EXP bits, use the **following** command as shown in the example below:

```
Router# show run class-map mpls_exp1
Building configuration...
Current configuration : 76 bytes
!
class-map match-any mpls_exp1
 match mpls experimental topmost 1
!
end
```

To verify the details of a class-map created for matching IP DSCP values, use the **following** command as shown in the example below:

```
Router# show run class-map dscpaf21
Building configuration...
Current configuration : 60 bytes
!
class-map match-any dscpaf21
 match ip dscp af21
!
end
```

To verify the details of a policy-map, use the **following** command as shown in the example below:

```
Router# show run policy-map policy_match_dscpaf11
Building configuration...
Current configuration : 100 bytes
!
policy-map policy_match_dscpaf11
 class dscpaf11
  set ip dscp af22
  priority percent 10
!
end
```

To verify the details of a policy-map attached to MLPPP interface, use the **following** command as shown in the example below:

```
Router# show policy-map interface multilink3
Multilink3
  Service-policy output: match_dscp_exp
    Class-map: dscpcs4 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp cs4 (32)
      Queueing
      queue limit 38 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 10% (153 kbps)
    Class-map: dscpcs6 (match-any)
      19 packets, 1889 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp cs6 (48)
      Queueing
      queue limit 38 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 10% (153 kbps)
```

Configuration Guidelines

- This feature must be configured globally for a router; it cannot be configured per-port or per-protocol.
- Enter each **cpu traffic qos** marking action on a separate line.
- The **cpu traffic qos cos** global configuration command configures CoS marking for CPU-generated traffic by using either a specific CoS value or a table map, but not both. A new configuration overwrites the existing configuration.

- The **cpu traffic qos dscp** global configuration command configures IP-DSCP marking for CPU-generated IP traffic by using either a specific DSCP value or a table map, but not both. A new configuration overwrites the existing configuration.
- The **cpu traffic qos precedence** global configuration command configures IP-precedence marking for CPU-generated IP traffic by using either a specific precedence value or a table map, but not both. A new configuration overwrites the existing configuration.
- The **cpu traffic qos dscp** and **cpu traffic qos precedence** global configuration commands are mutually exclusive. A new configuration overwrites the existing configuration.
- When the **cpu traffic qos dscp** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked DSCP or precedence value.
- When the **cpu traffic qos precedence** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked precedence or DSCP value.
- You cannot configure a **map from** value of both DSCP and precedence. A new configuration overwrites the existing configuration.
- When the **cpu traffic qos cos** global configuration command is configured with table maps, you can configure two **map from** values at a time—CoS and either DSCP or precedence.
- If the **cpu traffic qos cos** global configuration command is configured with only a **map from** value of DSCP or precedence:
  - The CoS value of IP packets is mapped by using the DSCP (or precedence) value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets remains unchanged.
- If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of CoS:
  - The CoS value of IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of DSCP or precedence and CoS:
  - The CoS value of IP packets is mapped by using the DSCP or precedence value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.

ARP-based Classification

Address Resolution Protocol Classification

Cisco IOS release 15.5(1)S introduces support for matching Address Resolution Protocol (ARP) protocol on the Cisco ASR 901 Series Routers. The ARP classification aims at enhancing the existing QoS classification to include protocol based classification. This feature matches the ARP packets coming to the Gigabit Ethernet interface and assigns priority percent queue for the packets.

Restrictions

- ARP classification can be applied only on the ingress interface.
- Supports only on the GigabitEthernet interface and its bundle derivatives (not supported on multilink interfaces).
- Supports only match protocol on the ARP (other protocols are not supported).

Configuring ARP Classification

You should complete the following procedures to configure ARP classification:

1. Create a class map for matching packets to a specified class
2. Create a policy map for an interface to specify a service policy
3. Attach the policy map to an input interface

Configuring a Class-map

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name* **Example:** `Router(config)# class-map ARP`	Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode.

	Command or Action	Purpose
Step 4	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol arp`	Configures the match criterion for a class map on the basis of a specified protocol.

What to do next

Create a policy map for an interface to specify a service policy.

Verifying a Class-map

To verify the class map configuration, use the **show** command as shown in the example below:

```
Router# show class-map ARP

 Class Map match-all ARP (id 93)
   Match protocol arp
```

Configuring a Policy-map

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map ARP`	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class arp`	Specifies the name of the class whose policy you want to create or change or to specify the default class before you configure its policy.
Step 5	**set qos-group** *group-id* **Example:** `Router(config-pmap-c)# set qos-group 5`	Configures a quality of service (QoS) group identifier (ID) that can be used later to classify packets.

What to do next

Attach the policy map to an input interface.

Verifying a Policy-map

To verify the policy map configuration, use the **show** commands as shown in the examples below:

```
Router# show policy-map ARP

 Policy Map ARP
    Class ARP
      set qos-group 5



Router# show policy-map interface gigabitethernet 0/5

GigabitEthernet0/5

Service-policy output: policy_1

Class-map: class_2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps
Match: protocol arp

Class-map: class-default (match-any)
0 packets, 752 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

Attaching a Policy-map

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/4`	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
Step 4	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input ARP`	Attaches a policy map to an output interface.

Example: Configuring ARP Classification

```
Router# show running-config interface gigabitethernet 0/2
Building configuration...

Current configuration : 95 bytes
!
interface GigabitEthernet0/2
no ip address
negotiation auto
service-policy input ARP
end
```

Configuring to Mark ARP Packets at Egress

By default, ARP packets are sent with a COS value of 6. You can change the COS value to zero using the **platform arp-set-cos-zero** command.

```
Router> enable
Router# configure terminal
Router(config)# platform arp-set-cos-zero
```

ICMP-based ACL

ICMP-based ACL Overview

The ICMP based ACL feature provides classification based on ICMP message type and message code to filter the traffic. This feature forms part of ACL based QoS and is implemented for both IPv4 and IPv6. The matching is done through match on access-group for ACL-based QoS, router ACLs for IPv4 and IPv6 ACLs, and port ACLs for IPv4 ACLs. This feature is supported on Gigabit Ethernet interfaces and its bundle derivatives.

ICMP-based ACL Restrictions

- ICMP-based ACL (IPv4 and IPv6) are not supported on the egress interface.
- ICMP-based ACL (IPv4 and IPv6) are not supported on the EVC interface.
- ICMP-based ACL (IPv4) is supported only on Gigabit Ethernet port, VLAN interface, and on policy-map. Gigabit Ethernet port and VLAN interface supports both named and numbered IPv4 ICMP ACLs.
- ICMP-based ACL (IPv6) is supported only on VLAN interface and not on Gigabit Ethernet port and policy-map.

- ICMP-based ACL (IPv4 and IPv6) uses router ACL slice when configured on the VLAN interface.
- ICMP-based ACL (IPv4) uses port ACL slice when configured on Gigabit Ethernet port.

Configuring IPv4 Port ACL for ICMP-based ACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* **permit icmp any any echo** **Example:** `Router(config)# access-list 125 permit icmp any any echo`	Specifies the access list. **Note** You can also use the **ip access-list extended** { *access-list-name* | *access-list-number* } **permit icmp** command to specify the access list.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0`	Specifies an interface type and number.
Step 5	**ip access-group** *ip-access-list* **in** **Example:** `Router(config-if)# ip access-group 125 in`	Applies an IP access list to an interface.

Configuring IPv4 Router ACL for ICMP-based ACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 715`	Creates a dynamic Switch Virtual Interface (SVI).
Step 4	**ip access-group** *ip-access-list* **in** **Example:** `Router(config-if)# ip access-group 125 in`	Specifies the IP access group.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0`	Specifies an interface type and number.
Step 7	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 715 ethernet`	Configures an Ethernet service instance on an interface.
Step 8	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)#  encapsulation dot1q 715`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 9	**bridge-domain** *bridge-domain-no* **Example:** `Router(config-if-srv)#  bridge-domain 715`	Binds a service instance or a MAC tunnel to a bridge domain instance.

Configuring ACL-based QoS for ICMP-based ACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map match-all icmpacl`	Creates a class map, and enters class-map configuration mode.
Step 4	**match access-group name** *acl-name* **Example:** `Router(config-cmap)# match access-group name icmpacl`	Defines the match criterion to classify traffic.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0`	Specifies an interface type and number.
Step 7	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input icmpacl`	Attaches a policy map to an input interface.

Configuring IPv6 Router ACL for ICMP-based ACL

Procedure

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

	Command or Action	Purpose
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Router(config)# ipv6 access-list icmpv6acl`	Defines an IPv6 access list and to place the device in IPv6 access list configuration mode.
Step 4	**permit icmp any any echo-reply** **Example:** `Router(config-ipv6-acl)# permit icmp any any echo-reply`	Sets conditions to allow a packet to pass a named IP access list.
Step 5	**exit** **Example:** `Router(config-ipv6-acl)# exit`	Exits the interface configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface vlan 715`	Specifies an interface type and number.
Step 7	**ipv6 traffic-filter** *access-list-name* **in** **Example:** `Router(config-if)# ipv6 traffic-filter icmpv6acl in`	Filters incoming or outgoing IPv6 traffic on an interface.

Verifying ICMP based ACL Configuration

Use the following **show** commands to verify the ICMP based ACL configuration.

To display the access-lists configured for ICMP-based ACL, use the **show access-lists** command as shown in the below example:

```
Router# show access-lists

Extended IP access list 125
    10 permit icmp any any echo
IPv6 access list icmpv6acl
    permit icmp any any echo-reply sequence 10
```

To display the ICMP-based ACL configuration on a gigabitethernet interface, use the **show running interface** command as shown in the below example:

```
Router# show running interface gigabitethernet 0/0

Building configuration...

Current configuration : 173 bytes
!
interface GigabitEthernet0/0
```

```
 no ip address
 ip access-group 125 in
 negotiation auto
 service instance 715 ethernet
  encapsulation dot1q 715
  bridge-domain 715
 !
end
```

To display the ICMP-based ACL configuration on a VLAN interface, use the **show running interface** command as shown in the below example:

```
Router# show running interface VLAN715

Building configuration...

Current configuration : 108 bytes
!
interface Vlan715
 no ip address
 ip access-group 125 in
 shutdown
 ipv6 traffic-filter icmpv6acl in
end
```

Policy for DHCP Control Packet

QoS policy applied in Ingress EVC for DHCP classifies the DHCP control traffic and applies to different internal Priority.

```
ip access-list extended dhcp
  permit udp any eq 68 any eq 67
!
class-map match-any SAR-Ran-network-control
  match dscp af11  af41  af43
  match access-group name dhcp
!
policy-map DHCP_mark
class SAR-Ran-network-control
set qos-group X
```

Note The X can be any value from 0-7 based on the requirement.

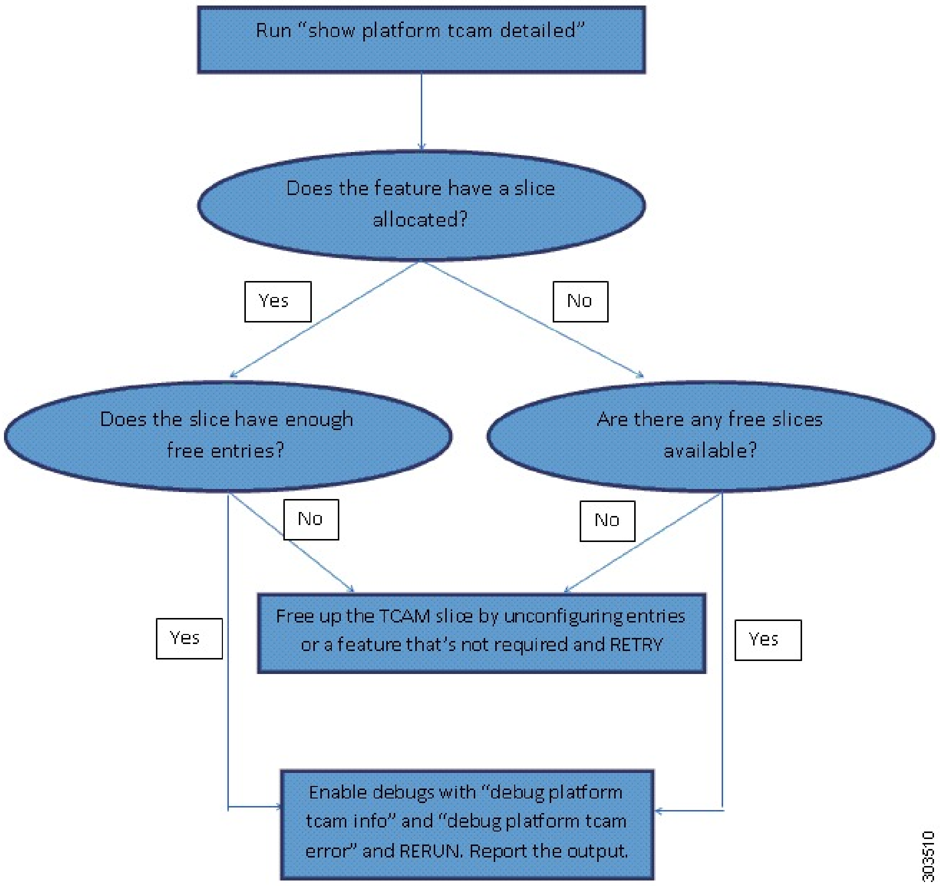
Troubleshooting Tips

The on-demand TCAM resource allocation may fail due to the unavailability of resources for the requested operation. In such scenarios, use the following troubleshooting tips:

1. Run the show platform tcam detailed command to understand the current resource allocation.
2. Use this information to find the features that are allocated resources.
3. Unconfigure the features that are no longer required to free the resources.

Figure 36: Troubleshooting Feature Scalabitlity, on page 482 shows the troubleshooting feature scalability procedure.

Figure 36: Troubleshooting Feature Scalabitlity



The following TCAM commands are used for troubleshooting feature scalability.

Command	Purpose
show platform tcam summary	Shows the current occupancy of TCAM with summary of the number of slices allocated or free.
show platform tcam detailed	Shows the current occupancy and includes per-slice information such as number of entries used or free, feature(s) using the slice, slice mode, and slice stage and ID. This command helps to understand current resource allocation and decide which feature(s) to unconfigure to free resources.
debug platform tcam error	Enables TCAM error printing. By default, the error printing is turned on and the info printing is turned off.
debug platform tcam info	Enables TCAM info printing.

Use the no form of the debug commands to disable TCAM error printing and TCAM info printing.

Danger We suggest you do not use the debug commands without TAC supervision.

The following is a sample of the output from the show platform tcam summary command.

```
Router# show platform tcam summary
Ingress    : 2/8 slices, 512/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
```

The following is a sample of the output from the show platform tcam detailed command.

```
Router# show platform tcam detailed
Ingress    : 2/8 slices, 512/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 28/256
Slice allocated to: Layer-2 Classify and Assign Group
Slice ID: 4
Stage: Pre-Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: L2CP
Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 29/128
Slice allocated to: L2 Post-Switch Processing Group
Slice ID: 3
Stage: Ingress
Mode: Single
Entries used: 13/256
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
```

Example: TCAM troubleshooting related error

In this example all the eight slices available at the Ingress stage have already been allocated. Also, the slice allocated to QoS has no free entries. If we need to configure a few more QoS rules, the following options are available:

1. To unconfigure QoS rules that are no longer required and thereby freeing up the entries
2. To free up a slice by unconfiguring features that are no longer required.

```
Router# show platform tcam detailed
Ingress    : 8/8 slices, 2048/2048 entries used [no free slices available]
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 29/256
Slice allocated to: Layer-2 Classify and Assign Group
Slice ID: 4
Stage: Pre-Ingress
```

```
Mode: Double
Entries used: 11/128
Slice allocated to: L2CP
Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 27/128
Slice allocated to: L2 Post-Switch Processing Group
Slice ID: 6
Stage: Ingress
Mode: Single
Entries used: 250/256
Slice allocated to: Port ACLs
Slice ID: 5
Stage: Ingress
Mode: Single
Entries used: 500/512
Slice allocated to: Router ACLs
Slice ID: 7
Stage: Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: OAM, Ethernet loopback, Y.1731 DMM
Slice ID: 3
Stage: Ingress
Mode: Double
Entries used: 15/128
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
Slice ID: 8
Stage: Ingress
Mode: Double
Entries used: 256/256    [no free entries available]
Slice allocated to: Quality Of Service
```

Configuring a service-policy fails because of insufficient resources.

```
Router(config-if-srv)# service-policy input policy2
Router(config-if-srv)#
*Mar  6 18:41:14.771: %Error: Not enough hardware resources to program this policy-map
*Mar  6 18:41:14.771: %QOS-6-POLICY_INST_FAILED:
 Service policy installation failed
Router(config-if-srv)#
```

In the above scenario, you can free up the TCAM rules by unconfiguring the service-policy that is no longer required or free up a slice by unconfiguring a feature that is no longer required.

```
Router(config-if-srv)# no service-policy input policy1
Router(config-if-srv)# end
Router#
Router# show platform tcam detailed
Ingress    : 8/8 slices, 2048/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 29/256
Slice allocated to: Layer-2 Classify and Assign Group
Slice ID: 4
Stage: Pre-Ingress
Mode: Double
Entries used: 11/128
Slice allocated to: L2CP
```

```
Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 27/128
Slice allocated to: L2 Post-Switch Processing Group
Slice ID: 6
Stage: Ingress
Mode: Single
Entries used: 250/256
Slice allocated to: Port ACLs
Slice ID: 5
Stage: Ingress
Mode: Single
Entries used: 500/512
Slice allocated to: Router ACLs
Slice ID: 7
Stage: Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: OAM, Ethernet loopback, Y.1731 DMM
Slice ID: 3
Stage: Ingress
Mode: Double
Entries used: 15/128
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
Slice ID: 8
Stage: Ingress
Mode: Double
Entries used: 195/256    [after unconfiguring policy1]
Slice allocated to: Quality Of Service
```

We now have enough free entries to configure policy2.

```
Router(config-if-srv)# service-policy input policy2
Router(config-if-srv)#
Router# show platform tcam detailed
Ingress    : 8/8 slices, 2048/2048 entries used
Pre-Ingress: 3/4 slices, 768/1024 entries used
Egress     : 0/4 slices, 0/512 entries used
Slice ID: 1
Stage: Pre-Ingress
Mode: Single
Entries used: 29/256
Slice allocated to: Layer-2 Classify and Assign Group
Slice ID: 4
Stage: Pre-Ingress
Mode: Double
Entries used: 11/128
Slice allocated to: L2CP
Slice ID: 2
Stage: Ingress
Mode: Double
Entries used: 27/128
Slice allocated to: L2 Post-Switch Processing Group
Slice ID: 6
Stage: Ingress
Mode: Single
Entries used: 250/256
Slice allocated to: Port ACLs
Slice ID: 5
Stage: Ingress
Mode: Single
Entries used: 500/512
Slice allocated to: Router ACLs
```

```
Slice ID: 7
Stage: Ingress
Mode: Double
Entries used: 10/128
Slice allocated to: OAM, Ethernet loopback, Y.1731 DMM
Slice ID: 3
Stage: Ingress
Mode: Double
Entries used: 15/128
Slice allocated to: CESoPSN-UDP, CEF, Layer-3 Control Protocols
Slice ID: 8
Stage: Ingress
Mode: Double
Entries used: 220/256 [after configuring policy2]
Slice allocated to: Quality Of Service
```

Additional References

The following sections provide references related to configuring QoS.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS MQC Commands	Cisco IOS Quality of Service Solutions Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Configuring QoS

Table 27: Feature Information for Configuring QoS, on page 487 lists the features in this module and provides links to specific configuration information.

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 Table 27: Feature Information for Configuring QoS, on page 487 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 27: Feature Information for Configuring QoS

Feature Name	Releases	Feature Information
ACL-based QoS	15.2(2)SNH1	This feature was introduced.
Shaper Burst Commit Size Down to 1 ms	15.2(2)SNI	The following section provides information about this feature: • Traffic Shaping, on page 403
Egress Policing	15.3(3)S	Support for Egress Policing was introduced on the Cisco ASR 901 routers.
Multiaction Ingress Policer on EVC	15.3(3)S	Support for Multiaction Ingress Policer on EVC was introduced on the Cisco ASR 901 routers.
QoS for MPLS over MLPPP	15.4(1)S	This feature was introduced on the Cisco ASR 901 routers.
ACL-based QoS IPv6 Services: Extended Access Control Lists	15.4(2)S	This feature was introduced on the Cisco ASR 901 routers.
MLPPP QoS Egress Shaping	15.5(1)S	This feature was introduced on the Cisco ASR 901 routers.

Feature Name	Releases	Feature Information
ARP-based Classification	15.5(1)S	This feature was introduced on the Cisco ASR 901 routers.
ICMP-based ACL	15.5(2)S	This feature was introduced on the Cisco ASR 901 routers.

CHAPTER 25

Configuring MLPPP

The Multilink Point-to-Point (MLPPP) feature provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load calculation on both inbound and outbound traffic.

Note To get information on the basic configuration of MLPPP, see http://www.cisco.com/en/US/docs/ios/12_2/dial/configuration/guide/dafppp.html.

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 MLPPP, on page 507.

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

- Cisco IOS Release 15.2(2)SNI or a later release that supports the Multiprotocol Label Switching (MPLS) over MLPPP feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- Cisco Express Forwarding (CEF) or distributed Cisco Express Forwarding (dCEF) should be enabled.

- MPLS should enabled on PE and P routers.
- Before enabling MPLS over MLPPP link, configure the following commands:
  - mpls label protocol ldp
  - mpls ip (configure this command over MLPPP link where IP address has been enabled)

Restrictions

- TE-FRR/LFA FRR feature is not supported on the MLPPP interface.
- Virtual Routing and Forwarding (VRF) configuration is not supported on the MLPPP interface.
- You need to shut down and bring up the MLPP interface for the following conditions:
  - On the fly fragmentation enable or disable
  - On the fly changes to the fragment size
  - Link fragmentation interleave
  - Enabling multiclass
- If the CPU command is modified when IS-IS is configured, you should remove and re-apply the service-policy in MLPPP.
- For MLPPP, you can use only up to 1500 maximum transmission unit (MTU) for control plane traffic from the router. Traffic drop is observed while sending ICMP packets over 1500 MTU with Do not Fragment (DF) bits.
- For data-plane traffic, the MTU configuration has no impact. Though you can configure Multilink Maximum Received Reconstructed Unit (MRRU) to any value, it does not serve any purpose to configure it above 1536, as MTU is hardcoded to 1536.
- For MPLS backbone, you can use only up to 1492 MTU with DF bit set, which results in 1492 MTU and 2 MPLS headers with DF. ICMP traffic drop is observed for anything beyond this.

MLPPP Optimization Features

The Cisco ASR 901 supports several features that improve the performance of Multilink Point-to-Point Protocol (MLPPP) connections and related applications such as IP over MLPPP. Some important features are given below:

Distributed Multilink Point-to-Point Protocol Offload

Distributed Multilink Point-to-Point Protocol (dMLPPP) allows you to combine T1 or E1 connections into a bundle that has the combined bandwidth of all of the connections in the bundle, providing improved capacity and CPU utilization over MLPPP. The dMLPPP offload feature improves the performance for traffic in dMLPPP applications such as IP over MLPPP by shifting processing of this traffic from the main CPU to the network processor.

The Cisco ASR 901 supports one serial links per T1/E1 connection and up to 16 MLPPP bundles. You can use the fixed T1/E1 ports to create up to 16 MLPPP links.

The Cisco ASR 901 implementation of multilink (dMLPPP) uses interleaving to allow short, delay-sensitive packets to be transmitted within a predictable amount of time. Interleaving allows the Cisco ASR 901 to interrupt the transmission of delay-insensitive packets in order to transmit delay-sensitive packets. You can also adjust the responsiveness of the Cisco ASR 901 to delay-sensitive traffic by adjusting the maximum fragment size; this value determines the maximum delay that a delay-sensitive packet can encounter while the Cisco ASR 901 transmits queued fragments of delay-insensitive traffic.

Multiclass MLPPP

The Cisco ASR 901 implementation of dMLPPP also supports Multiclass MLPPP. Multiclass MLPPP is an extension to MLPPP functionality that allows you to divide traffic passing over a multilink bundle into several independently sequenced streams or classes. Each multiclass MLPPP class has a unique sequence number, and the receiving network peer processes each stream independently. The multiclass MLPPP standard is defined in RFC 2686.

The Cisco ASR 901 supports the following multiclass MLPPP classes:

- Class 0- Data traffic that is subject to normal MLPPP fragmentation. Appropriate for non-delay-sensitive traffic.
- Class 1- Data traffic that can be interleaved but not fragmented. Appropriate for delay-sensitive traffic such as voice.

You can use the QoS configuration to classify the LLQ traffic inorder to prioritize the Class 1 traffic and bandwidth queues for Class 0 traffic to guarantee bandwidth when multiclass multilink PPP (MCMP) is enabled.

Note By default, Multiclass MLPPP is enabled with two classes. Maximum number of classes supported is also two.

Note The Cisco ASR 901 does not support some PPP and MLPPP options when the bundle is offloaded to the network processor; you can retain these options by disabling MLPPP and IPHC offloading for a given bundle. For more information, see MLPPP Offload, on page 500.

Note The output for the **show ppp multilink** command for an offloaded MLPPP bundle differs from the output for a non-offloaded bundle.

MPLS over MLPPP

The Multiprotocol Label Switching (MPLS) support over Multilink PPP feature allows you to use labeled switch paths (LSPs) over MLPPP links. In a network with Ethernet and MLPPP connections, this feature supports MPLS over MLPPP links in the edge (PE-to-CE) or in the MPLS core (PE-to-PE and PE-to-P) or at the end of MPLS labeled path (CE-to-PE) as PE router.

Note QoS is not supported for MPLS over MLPPP.

This section contains the following topics:

MPLS Features Supported for MLPPP

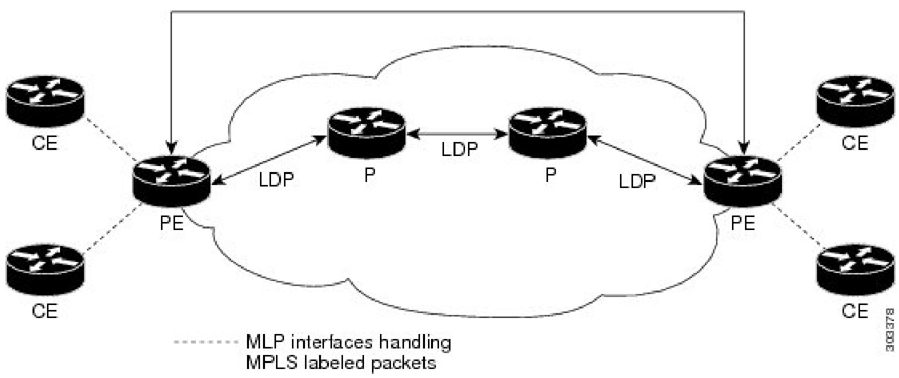
The following features are supported.

- MPLS Label imposition (LER)
- MPLS Label switching (LSR)
- MPLS VPN (L3VPN): User-Network Interface (UNI) on which virtual routing and forwarding (VRF) is configured should be switch virtual interface (SVI) on Gigabit interfaces and Network-to-Network Interface(NNI) can be MLPPP link
- Routing Protocols – ISIS/OSPF/BGP on MLPPP
- Label Distribution Protocol (LDP) as MPLS label protocol
- Equal Cost Multipath (ECMP) support on MLPPP links for IP to Tag (LER cases)

MPLS over MLPPP on PE-to-CE Links

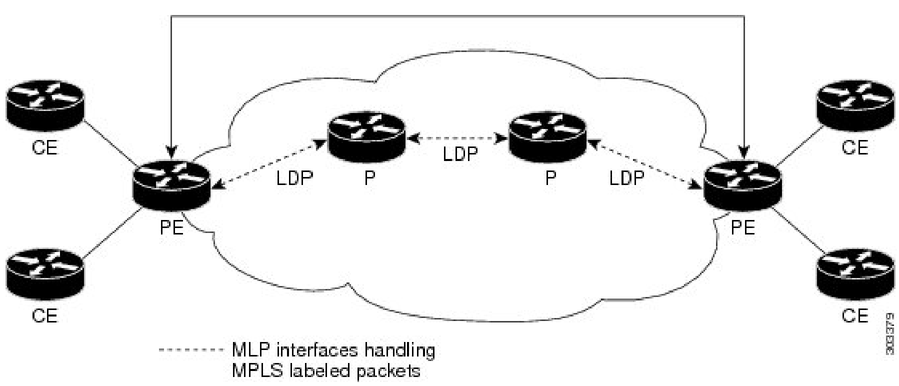
The following figure shows a typical MPLS network in which the PE router is responsible for label imposition (at ingress) and disposition (at egress) of the MPLS traffic.

In this topology, MLPPP is deployed on the PE-to-CE links.



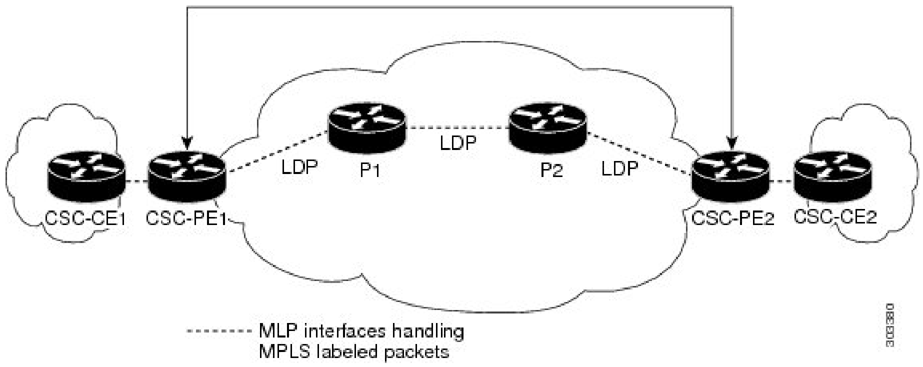
MPLS over MLPPP on Core Links

The following figure shows a sample topology in which MPLS is deployed over MLPPP on PE-to-P and P-to-P links. Enabling MPLS on MLPPP for PE-to-P links is similar to enabling MPLS on MLPPP for P-to-P links.



MPLS over MLPPP on CE to PE Links

The following figure shows a sample topology in which MPLS is deployed over MLPPP between CE and PE links with LDP.



Configuring MLPPP Backhaul

To configure an MLPPP backhaul, complete the following tasks:

Configuring the Card Type, E1 and T1 Controllers

For information on configuring the card type, E1 and T1 controllers, see Chapter 18, Configuring T1/E1 Controllers .

Configuring a Multilink Backhaul Interface

A multilink interface is a virtual interface that represents a multilink PPP bundle. The multilink interface coordinates the configuration of the bundled link, and presents a single object for the aggregate links. However, the individual PPP links that are aggregated must also be configured. Therefore, to enable multilink PPP on multiple serial interfaces, you first need to set up the multilink interface, and then configure each of the serial interfaces and add them to the same multilink interface.

Note In the following procedure, press the Return key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering disable at the Router# prompt.

The Cisco ASR 901 router can support up to 16 E1/T1 connections through the multilink interface, ranging from 16 bundles of one E1/T1 each to a single bundle containing 12 E1/T1 bundles.

Complete the following tasks to configure a multilink backhaul interface.

Creating a Multilink Bundle

Complete the following steps to create a multilink bundle:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink5`	Creates a multilink bundle and enters the interface configuration mode: • *group-number*—Number of the multilink bundle. The example creates a multilink bundle 5. To remove a multilink bundle, use the no form of this command.
Step 4	**ipaddress** *address subnet mask* **Example:** `Router(config-if)# ip address 10.10.10.2 255.255.255.0`	Assigns an IP address to the multilink interface. • *address*— IP address. • *subnet mask*—Network mask of IP address. The example configures an IP address and subnet mask.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode.

Configuring MRRU

You should configure the local maximum received reconstructed unit (MRRU) of the multilink bundle to a value greater than or equal to 1508 bytes(or equal to the maximum packet length expected on the bundle at any point in time). The maximum MTU supported on the Cisco ASR 901 router is 1536, and MTU drops occur when the packet length is more than 1536.

Complete the following steps to configure MRRU:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *multilink-bundle-number* **Example:** `Router(config)# interface multilink 1`	Creates a multilink bundle and enters the multilink interface configuration mode to configure the multilink bundle. • *multilink-bundle-number*—Number of the multilink bundle. The range is from 1 to 65535.
Step 4	**ppp multilink mrru local** *bytes* **Example:** `Router(config-if)# ppp multilink mrru local 1536`	Configures the MRRU value negotiated on a Multilink PPP bundle. • **local**—Configures the local MRRU value. • *bytes*—MRRU value, in bytes. Valid value range is 128 to 16384.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Configuring PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (AFC) are PPP compression methods defined in RFCs 1661 and 1662. PFC allows for compression of the PPP Protocol field; ACFC allows for compression of the PPP Data Link Layer Address and Control fields.

Follow these steps to configure PFC and ACFC handling during PPP negotiation to be configured. By default, PFC/ACFC handling is not enabled.

Note The recommended PFC and ACFC handling in the Cisco ASR 901 router is: acfc local request, acfc remote apply, pfc local request, and pfc remote apply.

Configuring PFC

Complete the following steps to configure PFC handling during PPP negotiation:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink5`	Creates a multilink bundle and enters the interface configuration mode: • *group-number*—Number of the multilink bundle. The example creates a multilink bundle 5. To remove a multilink bundle, use the no form of this command.
Step 4	**ppp pfc local** {**request** | **forbid**} **Example:** `Router(config-if)# ppp pfc local request`	Configures how the router handles PFC in its outbound configuration requests, use the **ppp pfc local** command. The syntax is as follows: • **request**—The PFC option is included in outbound configuration requests. • **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted. The example shows how to create a method for the router to manage PFC.
Step 5	**ppp pfc remote** {**apply** | **reject** | **ignore**} **Example:** `Router(config-if)# ppp pfc remote apply`	Specifies how the router manages the PFC option in configuration requests received from a remote peer. The syntax is as follows: • **apply**—Specifies that PFC options are accepted and PFC may be performed on frames sent to the remote peer. • **reject**—Specifies that PFC options are explicitly ignored. • **ignore**—Specifies that PFC options are accepted, but PFC is not performed on frames sent to the remote peer. The example shows how to allow PFC options to be accepted.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Configuring ACFC

Complete the following steps to configure ACFC handling during PPP negotiation:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 5`	Creates a multilink bundle and enter the interface configuration mode: • *group-number*—Number of the multilink bundle. The example creates a multilink bundle 5. To remove a multilink bundle, use the no form of this command.
Step 4	**ppp acfc local** {*request* | *forbid*} **Example:** `Router(config-if)# ppp acfc local request`	Specifies how the router handles ACFC in outbound configuration requests. The syntax is as follows: • *request*—Specifies that the ACFC option is included in outbound configuration requests. • *forbid*—Specifies that the ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.

	Command or Action	Purpose
Step 5	**ppp acfc remote** {*apply* | *reject* | *ignore*} **Example:** `Router(config-if)# ppp acfc remote apply`	Specifies how the router handles the ACFC option in configuration requests received from a remote peer. The syntax is as follows: • *apply*—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • *reject*—ACFC options are explicitly ignored. • *ignore*—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer. The example allows ACFC options to be accepted.
Step 6	**exit** **Example:** `Router(config)# exit`	Exit configuration mode.

Enabling Multilink and Identifying the Multilink Interface

Complete the following steps to enable multilink and identify the multilink interface:

Note If you modify parameters for an MLPPP bundle while it is active, the changes do not take effect until the Cisco ASR 901 renegotiates the bundle connection.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface multilink** *group-number* **Example:**	Creates the multilink group interface corresponding to the specified group number. This command enables the following commands under the interface multilink group number:

	Command or Action	Purpose
	`Router(config-if)# interface multilink 5`	a. **keepalive** b. **ppp multilink group** *group-number* where *group-number* is the Multilink group number. The example restricts (identifies) the multilink interface that can be negotiated to multilink interface 5.
Step 4	**keepalive** [*period*[*retries*]] **Example:** `Router(config-if)# keepalive 1 5`	Enables keepalive packets on the interface and specifies the number of times the keepalive packets are sent without a response before the router disables the interface. The syntax is as follows: • *period*—(Optional) Integer value in seconds greater than 0. The default is 10. Using 0 disables the keepalive option. • *retries*—(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. Integer value greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default of 5 is used.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits the configuration mode.

Configuring a Serial Interface as a Member Link of a MLPPP Group

Complete the following steps to configure a serial interface as a member link of a MLPPP group:

Procedure

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

	Command or Action	Purpose
Step 3	**interface serial slot/port:** *channel-group-number* **Example:** `Router(config-if)# interface serial 0/5:5`	Identifies and accesses the serial interface on the specified slot and port. • *channel-group-number*—The number to identify the channel group. The valid range is from 0–30 for E1 controllers and 0–23 for T1 controllers.
Step 4	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP encapsulation on the serial interface.
Step 5	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables multilink PPP on the serial interface.
Step 6	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 5`	Configures the serial interface as a member link to the multilink interface identified by the group-number. • *group-number* —Multilink group number. The example identifies the multilink interface to which the serial interface should be bound to as a member-link.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

MLPPP Offload

By default, the Cisco ASR 901 router offloads processing for distributed MLPPP (dMLPPP) to the network processor for improved performance. However, the Cisco ASR 901 does not support some dMLPPP settings on offloaded bundles. The Cisco ASR 901 does not support the following options on offloaded dMLPPP bundles:

- **ppp multilink idle-link**
- **ppp multilink queue depth**
- **ppp multilink fragment maximum**
- **ppp multilink slippage**
- **ppp timeout multilink lost-fragment**

Note If you have a bundle that requires the use of these options, contact Cisco support for assistance.

Configuring Additional MLPPP Settings

You can perform a variety of other configurations on an MLPPP bundle, including the following:

- Modifying the maximum fragment size
- Modifying fragmentation settings
- Enabling or disabling fragmentation
- Enabling or disabling interleaving
- Configuring multiclass MLPPP

Note For more information about configuring MLPPP, see the Dial Configuration Guide, Cisco IOS Release 15.0S .

Configuring MPLS over the MLPPP on a Serial Interface

Complete the following steps to configure MPLS over the MLPPP link on a serial interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *slot/port:time-slot* **Example:** `Router(config-if)# interface Serial0/0:0`	Specifies a serial interface created on a channelized E1 or channelized T1 controller: • *slot*—Slot number where the channelized E1 or T1 controller is located. • *port*—Port number where the channelized E1 or T1 controller is located. • *time-slot* —For ISDN, the D channel time slot, which is the :23 channel for channelized T1 and the :15 channel for channelized E1. PRI time slots are in the range from 0 to 23 for channelized T1 and in the range from 0 to 30 for channelized E1.
Step 4	**no ip address** **Example:**	Disabled IP address processing.

	Command or Action	Purpose
	`Router(config-if)# no ip address`	
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Configures the encapsulation method used by the interface. • *encapsulation-type*—Encapsulation type.
Step 6	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP on an interface .
Step 7	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 2`	Restricts a physical link to join only one designated multilink group interface. • *group-number*—Multilink-group number (a non-zero number).
Step 8	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring MPLS over MLPPP for OSPF

Complete the following steps to configure MPLS over the MLPPP link for OSPF:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 2`	Creates the multilink group interface corresponding to the specified group number, and enters the interface configuration mode. • *group-number* —Multilink group number.

	Command or Action	Purpose
Step 4	**ip address** *ip-address* [*subnet mask*] **Example:** `Router(config-if)# ip address 11.11.11.2 255.255.255.0`	Assigns an IP address to the multilink interface. • *ip-address*—IP address. • *subnet mask*—Network mask of IP address.
Step 5	**ip ospf** *process-id* **area** *area-id* **Example:** `Router(config-if)# ip ospf 10 area 0`	Enables OSPF on an interface. • *process-id*—A decimal value in the range from 1 to 65535. • *area-id*—A decimal value in the range from 0 to 4294967295, or an IP address.
Step 6	**ip ospf authentication null** **Example:** `Router(config-if)# ip ospf authentication null`	Specifies the authentication type for an interface. • **null** —No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.
Step 7	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
Step 8	**no keepalive** **Example:** `Router(config-if)# no keepalive`	Disables keepalive packets.
Step 9	**ppp pfc local request** **Example:** `Router(config-if)# ppp pfc local request`	Configures protocol field compression (PFC) in configuration requests.
Step 10	**ppp pfc remote apply** **Example:** `Router(config-if)# ppp pfc remote apply`	Configures how the PFC option in configuration requests is received from a remote peer.
Step 11	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP on an interface.

	Command or Action	Purpose
Step 12	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 2`	Restricts a physical link to join only one designated multilink group interface. • *group-number* —Multilink-group number (a nonzero number).
Step 13	**ppp multilink endpoint string** *char-string* **Example:** `Router(config-if)# ppp multilink endpoint string 22`	Restricts a physical link to join only one designated multilink group interface. • *char-string*—Character string.
Step 14	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.
Step 15	**router ospf** *process-id* [**vrf** *vrf-name*] **Example:** `Router(config)# router ospf 1234`	Configures an OSPF routing process and enters the router configuration mode. • *process-id* — Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
Step 16	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# network 6.6.6.6 0.0.0.0 area 2`	Configures the interfaces on which OSPF runs and to define the area ID for those interfaces. • *ip-address*—IP address. • *wildcard-mask* —IP-address-type mask that includes optional bits. • *area-id*—Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the area-id argument. **Note** Repeat this step to configure different interfaces on which OSPF runs, and to define the area ID for those interfaces.
Step 17	**exit** **Example:** `Router(config-router)# exit`	Exits the router configuration mode.

Configuration Examples for MPLS over MLPPP

The following example shows a sample configuration of MPLS over MLPPP for OSPF.

```
Building configuration...
Current configuration : 234 bytes
!
interface Multilink2
ip address 11.11.11.2 255.255.255.0
ip ospf 1234 area 0
ip ospf authentication null
mpls ip
no keepalive
ppp pfc local request
ppp pfc remote apply
ppp multilink
ppp multilink group 2
ppp multilink endpoint string 22
router ospf 1234
network 6.6.6.6 0.0.0.0 area 2
network 11.11.11.0 0.0.0.255 area 0
network 12.12.12.0 0.0.0.255 area 2
```

The following example shows a sample configuration of MPLS over MLPPP for a Serial Interface.

```
Building configuration...
Current configuration : 101 bytes
!
interface Serial0/0:0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 2
```

The following example shows a sample configuration of MCMP enabled in MLPPP with classification based on DSCP

```
Configuring the class-map to match on priority queue (DSCP EF). When Priority percent is
configured, it expedites the Class 1 traffic.
class-map match-any DSCP_EF
match ip dscp ef
policy-map BCP_MLPPP
class  DSCP_EF
  priority percent 10
class class-default
  bandwidth percent 5
```

Verifying MPLS over MLPPP Configuration

To verify the configuration of MPLS over MLPPP, use the **following** commands as shown in the examples below:

```
Router# ping mpls ipv4 6.6.6.6/32
Sending 5, 100-byte MPLS Echos to 6.6.6.6/32,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
```

```
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
Total Time Elapsed 40 ms
Router# show mpls ldp bindings 6.6.6.6 32
lib entry: 6.6.6.6/32, rev 8
        local binding:  label: 17
        remote binding: lsr: 6.6.6.6:0, label: imp-null


Router# traceroute mpls ipv4 6.6.6.6/32
Tracing MPLS Label Switched Path to 6.6.6.6/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
  0 11.11.11.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 11.11.11.2 4 ms
```

Additional References

The following sections provide references related to MLPPP feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Dial Technologies Configuration Guide	http://www.cisco.com/en/US/docs/ios/12_2/dial/configuration/guide/dafppp.html Configuring Media-Independent PPP and Multilink PPP
MPLS over MLPPP	MPLS—Multilink PPP Support

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for MLPPP

Table 28: Feature Information for MLPPP, on page 507 lists the features in this module and provides links to specific configuration information.

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 Table 28: Feature Information for MLPPP, on page 507 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 28: Feature Information for MLPPP

Feature Name	Releases	Feature Information
MPLS over MLPPP	15.2(2)SNI	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:

CHAPTER 26

Onboard Failure Logging

Onboard Failure Logging (OBFL) captures and stores hardware failure and environmental information into nonvolatile memory. OBFL permits improved accuracy in hardware troubleshooting and root cause isolation analysis. Stored OBFL data can be retrieved in the event of a router crash or failure.

Understanding OBFL

OBFL provides a mechanism to store hardware, software, and environment related critical data in a non-volatile memory, such as flash EPROM or EEPROM on routers. The logging information is used by the TAC team to troubleshoot and fix hardware issues.

OBFL collects data like temperatures and voltages. It stores the data in a dedicated area of the flash memory of the router. This data is retrieved by TAC personnel to troubleshoot routers. It can also be analyzed by back-end software to detect failure patterns, and possibly to recommend specific quality improvements.

Retrieval of the OBFL message

If the hardware is defective and the system cannot boot up, any data in flash is inaccessible. In that case, use any one of the following methods to recover OBFL data:

- Read the flash through JTAG: this requires provisions in hardware design and back-end hardware and software support tools.
- Repair the system; boot it; use the OBFL CLI commands.

Recording OBFL Messages

Data is recorded in any of the following formats:

- Continuous information that displays a snapshot of measurements.
- Samples in a continuous file, and summary information about the data being collected.

Configuring OBFL

Use the following commands to configure and verify OBFL:

Command	Purpose
Router(conf)# **hw-module** *{all|slot|module}* *{slotnumber/subslotnumber|modulenumber}* **logging onboard** Router(conf)# **hw-module** *module 0* **logging onboard**	Enables OBFL on the specified hardware module. The **no** form of the command disables OBFL.
Router> **show logging onboard** {slot|module} {slotnumber/subslotnumber|modulenumber} [**status**]	Shows the status of OBFL logging. OBFL is enabled by default in Cisco ASR 901.
Router(conf)# **clear logging onboard**	Clears OBFL logging.

Verifying OBFL Configuration

Example 1

```
Router# show logging onboard status
Devices registered with infra
Slot no.: 0 Subslot no.: 0, Device obfl0:
Application name clilog :
Path : obfl0:
CLI enable status : enabled
Platform enable status: enabled
Application name temperature :
Path : obfl0:
CLI enable status : enabled
Platform enable status: enabled
```

Example 2

```
Router # show logging onboard temperature ?
continuous Onboard logging continuous information
detail Onboard logging detailed information
end ending time and date
raw Onboard logging raw information
start starting time and date
status Onboard logging status information
summary Onboard logging summary information
Router# show logging onboard temperature continuous
--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor | ID |
--------------------------------------------------------------------------------
System 1
--------------------------------------------
Time Stamp |Sensor Temperature 0C
```

```
MM/DD/YYYY HH:MM:SS | 1
--------------------------------------------
03/01/2000 00:06:02 37
03/01/2000 00:16:02 37
03/01/2000 00:05:57 36
Router# show logging onboard voltage continuous
------------------------------------------------------------------------------------------
-------------------------
VOLTAGE CONTINUOUS INFORMATION
------------------------------------------------------------------------------------------
-------------------------
Sensor | ID |
------------------------------------------------------------------------------------------
-------------------------
12.00VA 0
1.50V 1
1.25V 2
12.00VB 3
2.50V 4
1.05V 5
1.20V 6
1.80V 7
------------------------------------------------------------------------------------------
-------------------------
Time Stamp |Sensor Voltage
MM/DD/YYYY HH:MM:SS | 12.00VA 1.50V 1.25V 12.00VB 2.50V 1.05V 1.20V
1.80V
------------------------------------------------------------------------------------------
-------------------------
02/24/2000 21:41:58 11.764 1.176 1.176 7.843 2.352 0.784 1.176
1.568
02/24/2000 21:46:00 11.764 1.176 1.176 7.843 2.352 0.784 1.176
1.568
02/25/2000 14:29:53 11.764 1.176 1.176 7.843 2.352 0.784 1.176
1.568
02/25/2000 14:33:54 11.764 1.176 1.176 7.843 2.352 0.784 1.176
1.568
Router# sh logging onboard clilog summary
--------------------------------------------------------------------------------
CLI LOGGING SUMMARY INFORMATION
--------------------------------------------------------------------------------
COUNT COMMAND
--------------------------------------------------------------------------------
   1 clear logging onboard
   2 hw-module module 0 logging onboard message level 1
   1 hw-module module 0 logging onboard message level 2
   5 hw-module module 0 logging onboard message level 3
   2 no hw-module module 0 logging onboard message level
   5 show logging onboard
   2 show logging onboard clilog
   2 show logging onboard clilog continuous
   1 show logging onboard clilog summary
   2 show logging onboard continuous
   1 show logging onboard environment
   9 show logging onboard message
   9 show logging onboard message continuous
   1 show logging onboard message summary
   3 show logging onboard status
   1 show logging onboard temperature
   1 show logging onboard voltage
   1 test logging onboard error 3
   1 test logging onboard error1 3
   1 test logging onboard try 1
--------------------------------------------------------------------------------
```

CHAPTER 27

Hot Standby Router Protocol and Virtual Router Redundancy Protocol

This feature module describes the HOT Standby Router Protocol(HSRP) and Virtual Router Redundancy Protocol(VRRP) features. The Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) designed to allow transparent fail-over of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet, Fiber Distributed Data Interface (FDDI), Bridge-Group Virtual Interface (BVI), LAN Emulation (LANE), or Token Ring networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router.

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment . VRRP is not an election protocol in itself; rather it specifies an election protocol that dynamically assigns responsibility for a virtual router.

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 table at the end of this module.

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.

Information About HSRP and VRRP

Overview of HSRP and VRRP

Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, which helps maximum network uptime. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router. The members of the virtual router group continuously exchange status messages. This way, one router can assume the routing responsibility of another, should the first one go out of commission for either planned or unplanned reasons. Hosts continue to forward IP packets to a consistent IP and MAC address, and the changeover of devices that route is transparent.

A Virtual Router Redundancy Protocol (VRRP) router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails. VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network. You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, to balance the load on available routers.

Text Authentication

HSRP and VRRP ignore unauthenticated protocol messages. The default authentication type is text authentication. HSRP or VRRP authentication protects against false hello packets causing a denial-of-service attack. For example, suppose Router A has a priority of 120 and is the active router. If a host sends spoof hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof hello packets are ignored, Router A remains the active router. Packets are rejected in any of the following cases:

- The authentication schemes differ on the router and in the incoming packets.
- Text authentication strings differ on the router and in the incoming packets.

Preemption

Preemption occurs when a virtual router backup with a higher priority takes over another virtual router backup that was elected to become a virtual router master, and a preemptive scheme is enabled automatically. When a newly reloaded router becomes active, despite an active router already existent on the network, it may appear that preemption is not functioning but that is not true. The newly active router did not receive any hello packets from the current active router, and the preemption configuration was not factored into the new routers decision making.

In general, we recommend that all HSRP routers have the following configuration:

```
standby delay minimum 30 reload 60
```

The standby delay minimum reload interface configuration command delays HSRP groups from initializing for the specified time after the interface comes up.

This command is different from the standby preempt delay interface configuration command, which enables HSRP preemption delay. You can disable the preemptive scheme by using the **no vrrp preempt** command. If preemption is disabled, the virtual router backup that is elected to become virtual router master remains the master until the original virtual router master recovers and becomes the master again.

How to Configure HSRP

This section contains the following procedures:

Configuring HSRP

Complete the following steps to configure HSRP:

Restrictions

- HSRP is supported only on IPv4 devices and not on IPv6 devices.
- HSRP is supported only on layer 3 SVI interfaces. The configuration is not supported on Gigabit Ethernet or Fast Ethernet interfaces.
- Bidirectional Forwarding Detection (BFD) protocol is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 10`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	Specifies an primary or secondary IP address for an interface.
Step 5	**standby** [*group-number*] **timers** [*msec*] **hellotime** [*msec*] **holdtime** **Example:**	Configures the interval at which packets are sent to refresh the MAC cache when HSRP is running.

	Command or Action	Purpose
	`Router(config-if)# standby 1 timers 14`	
Step 6	**standby** [*group-number*] **preempt [delay {minimum** *delay* **| reload** *delay* **| sync** *delay***}]** **Example:** `Router(config-if)# standby 1 preempt delay minimum 380`	Configures preemption and preemption delay.
Step 7	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 8	**standby** [*group-number*] **authentication text** *string* **Example:** `Router(config-if)# standby 1 authentication text authentication 1`	Configures an authentication string for HSRP text authentication.
Step 9	**standby** [*group-number*] **track** *object-number* **[decrement** *priority-decrement***]** **Example:** `Router(config-if)# standby 1 track 100 decrement 20`	Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object.
Step 10	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for HSRP

This section provides the following configuration examples:

Example: Configuring HSRP Active Router

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10
```

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

Router# configure terminal
Router(config)# interface Vlan10
Router(config-if)# ip address 10.10.10.21 255.255.255.0
Router(config-if)# standby 1 ip 10.10.10.20
Router(config-if)# standby 1 timers 1 4
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 preempt delay minimum 10
Router(config-if)# standby 1 authentication cisco6
Router(config-if)# standby 1 track 1 decrement 20
Router(config-if)# end
```

Example: Configuring HSRP Backup Router

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# end
Router# configure terminal
Router(config)# interface Vlan10
Router(config-if)# ip address 10.10.10.22 255.255.255.0
Router(config-if)# standby 1 ip 10.10.10.20
Router(config-if)# standby 1 timers 1 4
Router(config-if)# standby 1 priority 90
Router(config-if)# standby 1 preempt delay minimum 10
Router(config-if)# standby 1 authentication cisco6
Router(config-if)# standby 1 track 1 decrement 20
Router(config-if)# end
```

Example: HSRP Text Authentication

The following example shows how to configure HSRP text authentication using a text string:

```
Router# configure terminal
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication text company2
Router(config-if)# standby 1 ip 10.21.0.10
```

Information About HSRP Version 2

HSRP Version 2 Design

HSRP version 2 is designed to address the following restrictions in HSRP version 1:

- In HSRP version 1, millisecond timer values are not advertised or learned. HSRP version 2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.

- In HSRP version 1, group numbers are restricted to the range that is from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
- HSRP version 2 provides improved management and troubleshooting. With HSRP version 1, you cannot use HSRP active hello messages to identify the physical device that sends the message because the source MAC address is the HSRP virtual MAC address. The HSRP version 2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.
- The multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing.

Version 1 is the default version of HSRP.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, used by HSRP version 1. This new multicast address allows CGMP leave processing to be enabled at the same time as HSRP.

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF. The increased group number range does not imply that an interface can, or should, support that number of HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

HSRP version 2 has a different packet format than HSRP version 1. The packet format uses a type-length-value (TLV) format. HSRP version 2 packets received by an HSRP version 1 device will have the type field mapped to the version field by HSRP version 1 and subsequently ignored.

HSRP version 2 is effective from Cisco IOS Release 15.5(03)s.

How to Configure HSRP Version 2

Changing to HSRP Version 2

HSRP version 2 was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.

Note

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 does not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same device. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).
- HSRP version 2 is supported only on IPv4 devices and not on IPv6 devices.
- HSRP version 2 configuration is supported only on layer 3 SVI interfaces. The configuration is not supported on Gigabit Ethernet or Fast Ethernet interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vlan 350`	Configures an interface type and enters interface configuration mode.
Step 4	**standby version** {**1** | **2**} **Example:** `Device(config-if)# standby version 2`	Changes the HSRP version.
Step 5	**standby** [*group-number*] **priority** [*priority*] **Example:** `Device(config-if)# standby 350 priority 100`	Configures HSRP priority.
Step 6	**standby** [*group-number*] **preempt** **Example:** `Router(config-if)# standby 350 preempt`	Configures preemption.
Step 7	**standby** [*group-number*] **timers** [*msec*] **Example:** `Router(config-if)# standby 350 timers 515`	Configures timers.
Step 8	**standby**[*group-number*] **ip address** *ip-address mask* [*secondary*] **Example:** `Router(config-if)# standby 350 ip 172.20.100.10`	Specifies an primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 10	**show standby** **Example:** `Device# show standby`	(Optional) Displays HSRP information. • HSRP version 2 information will be displayed if configured.

Configuration Examples for HSRP Version 2

Example: Configuring HSRP Version 2

The following example shows how to configure HSRP version 2 on an interface with a group number of 350:

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

How to Configure VRRP

This section contains the following procedures:

• Configuring VRRP , on page 520
• Configuration Examples for VRRP, on page 522

Configuring VRRP

Complete the following steps to configure VRRP:

Restrictions

- VRRP is supported only on IPv4 devices and not IPv6 devices.
- VRRP is supported only on gigabyte etherchannel interfaces of the Layer 3 SVI.
- Bidirectional Forwarding Detection (BFD) protocol is not supported.
- MD5 authentication is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Vlan10`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.25 255.255.255.0`	Specifies a primary or secondary IP address for an interface.
Step 5	**vrrp [group-number] timers advertise [msec]** **Example:** `Router(config-if)# vrrp 2 timers advertise 2`	Configures the interval at which packets are sent to refresh the MAC cache when VRRP is running

Step 6	**vrrp [group-number] preempt [delay minimum seconds]**
	Example:
	`Router(config-if)# vrrp 2 preempt delay`
	`minimum 10`
		Configures preemption delay.

Step 7	**vrrp [group-number] priority priority** **Example:** `Router(config-if)# vrrp 2 priority 200`	Configures VRRP priority.
Step 8	**vrrp [group-number] authentication text string** **Example:**	Configures an authentication string for VRRP text authentication.

	Command or Action	Purpose
	`Router(config-if)# vrrp 2 authentication text cisco7`	
Step 9	**vrrp [group-number] track object-number [decrement priority-decrement]** **Example:** `Router(config-if)# vrrp 2 track 1 decrement 20`	Configures VRRP to track an object and change the Hot Standby priority on the basis of the state of the object.
Step 10	**end** **Example:** `Router(config-if)# end`	Returns to the privileged EXEC mode.

Configuration Examples for VRRP

This section provides the following configuration examples:

Example: Configuring a VRRP Master Router

This example shows how to configure a VRRP Master router.

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# end
Router# configure terminal
Router(config)# interface Vlan10
Router(config-if)# ip address 10.10.10.25 255.255.255.0
Router(config-if)# vrrp 2 ip 10.10.10.30
Router(config-if)# vrrp 2 timers advertise 2
Router(config-if)# vrrp 2 preempt delay minimum 10
Router(config-if)# vrrp 2 priority 110
Router(config-if)# vrrp 2 authentication text cisco7
Router(config-if)# vrrp 2 track 1 decrement 20
Router(config-if)# end
```

Example: Configuring a VRRP Backup Router

This example shows how to configure a VRRP Backup router.

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
```

```
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# end
Router# configure terminal
Router(config)# interface Vlan10
Router(config-if)# ip address 10.10.10.26 255.255.255.0
Router(config-if)# vrrp 2 ip 10.10.10.30
Router(config-if)# vrrp 2 timers advertise 2
Router(config-if)# vrrp 2 preempt delay minimum 10
Router(config-if)# vrrp 2 priority 90
Router(config-if)# vrrp 2 authentication text cisco7
Router(config-if)# vrrp 2 track 1 decrement 20
```

Router(config-if)# end

Example: VRRP Text Authentication

The following example shows how to configure VRRP text authentication using a text string:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
```

Where to Go Next

For additional information on configuring HSRP and VRRP, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for HSRP and VRRP

Table 29: Feature Information for HSRP and VRRP, on page 525 lists the release history for this feature and provides links to specific configuration information.

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 Table 29: Feature Information for HSRP and VRRP, on page 525 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 29: Feature Information for HSRP and VRRP

Feature Name	Releases	Feature Information
HSRP and VRRP	15.2(2)SNG	The following sections provide information about this feature: • Overview of HSRP and VRRP, on page 514 • Text Authentication, on page 514 • Preemption, on page 514 • Configuring HSRP , on page 515 • Configuration Examples for HSRP, on page 516 • Configuring VRRP , on page 520 • Configuration Examples for VRRP, on page 522

CHAPTER 28

Configuring Link Layer Discovery Protocol

This feature module describes how to configure Link Layer Discovery Protocol (LLDP) on the Cisco ASR 901 Aggregation Series Router. The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over the data-link layer (Layer 2) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network.

To permit the discovery of non-Cisco devices, Cisco ASR 901supports LLDP, a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network.

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 LLDP, on page 532.

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.

Restrictions for LLDP

The following are the restrictions for LLDP:

- The memory available on a given end network device dictates the number of neighbor entries recorded. However, under most operating conditions, end devices such as printers, IP phones, workstations and so on, are typically operated in the receive mode only.
- If Entity MIB are used for LLDP broadcast, such as to create a sender ID. LLDP can be configured only when these MIBs are available.

Overview of LLDP

It is an optional element of a protocol stack in the 802 LAN station. LLDP uses the logical link control (LLC) services to transmit and receive information to and from other LLDP agents. LLC provides a Link Service Access Point (LSAP) for access to LLDP. Each LLDP frame is transmitted as a single MAC service request. Each incoming LLDP frame is received at the MAC Service Access Point (MSAP) by the LLC entity as a MAC service indication.

The LLDP protocol operates through the LLDP agent. The tasks of the LLDP agent are to:

- Collect information from the LLDP local system MIB and transmit it periodically.
- Receive LLDP frames from neighbors and populate LLDP remote devices MIBs.

LLDP supports a set of attributes used to find the neighbor devices. These attributes are type, length, and value descriptions of devices, and are referred to as Type Length Value (TLV). LLDP supported devices use TLVs to send and receive information from their neighbors. Details such as configuration information, device capabilities, and device identity are also advertised using this protocol.

How to Configure LLDP

This section contains the following procedures:

Configuring LLDP

Complete the following steps to configure LLDP on the Cisco ASR 901 platform:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **lldp run**	• The **lldp run** command enables LLDP globally on all the interfaces on the router.

	Command or Action	Purpose

	• **lldp holdtime** *seconds*
	• **lldp reinit** *seconds*
	• **lldp timer** *rate*
	• **lldp lldp tlv-select**
	
	Example:
	
	`Router(config)# lldp run`
	
	Example:
	
	`Router(config)# lldp holdtime 100`
	
	Example:
	
	`Router(config)# lldp reinit 2`
	
	Example:
	
	`Router(config)# lldp timer 75`
	
	Example:
	
	`Router(config-if)# lldp tlv-select system-description`
		• The **lldp holdtime** command specifies the hold time. The value ranges from 0 to 65535 seconds. The default value is 120 seconds.
		• The **lldp reinit** command specifies the delay time in seconds for LLDP to initialize on any interface. The value ranges from 2 to 5 seconds. The default value is 2 seconds.
		• The **lldp timer** command specifies the rate at which LLDP packets are sent. The value ranges from 5 to 65534 seconds. The default value is 30 seconds.
		• The **lldp tlv-select** command enables a specific LLDP TLV on a supported interface. Cisco ASR 901 LLDP supports the following TLVs:
		  • Port Description—Information about the interface that includes the name of the manufacturer, product name, and the version of the interface.
		  • System Description—Textual description of the device.
		  • System Name—Assigned name of the device.
		  • System Capabilities—Capability of the device and its primary function.
		  • Management Address—IP or MAC address of the device.

Step 4	**end** **Example:** `Router(config-if)# end`	Returns the CLI to privileged EXEC mode.

Verifying LLDP

To verify LLDP on the Cisco ASR 901 router, use the show command as shown in the following example.

```
Router# show lldp ?

entry      Information for specific neighbor entry
```

```
errors     LLDP computational errors and overflows
interface  LLDP interface status and configuration
neighbors  LLDP neighbor entries
traffic    LLDP statistics
|          Output modifiers
<cr>


Router# show lldp entry *


Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

Configuration Example for LLDP

This section provides the following configuration examples:

Example: Enabling LLDP Globally

```
Router> enable
Router# configure terminal
Router(config)# lldp run
Router(config)# end
```

Example: Configuring Hold Time

```
Router> enable
Router# configure terminal
Router(config)# lldp holdtime 100
Router(config)# end
```

Example: Configuring Delay Time

```
Router> enable
Router# configure terminal
Router(config)# lldp reinit 2
Router(config)# end
```

Example: Configuring Intervals

```
Router> enable
Router# configure terminal
Router(config)# lldp timer 75
Router(config)# end
```

This is an example to enable an LLDP TLV on a supported interface:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# lldp tlv-select system-description
Router(config-if)# end
```

Where to go Next

For additional information on configuring Multihop BFD, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for LLDP

LLDP is a one-way protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

Table 30: Feature Information for LLDP, on page 532 lists the release history for this feature and provides links to specific configuration information.

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 Table 30: Feature Information for LLDP, on page 532 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 30: Feature Information for LLDP

Feature Name	Releases	Feature Information
LLDP	12.2(2)SNG	See Overview of LLDP, on page 528 for more information about this feature.

CHAPTER 29

Configuring Multihop Bidirectional Forwarding Detection

Cisco ASR 901 supports Bidirectional Forwarding Detection(BFD) on arbitrary paths, which can span multiple network hops. The multihop BFD feature provides subsecond forwarding failure detection for a destination with more than one hop and up to 255 hops. A multihop BFD session is set up between a unique source-destination address pair provided by the client. A session can be set up between two endpoints that have IP connectivity.

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 LLDP, on page 532.

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.

Restrictions for Multihop BFD

The following are the restrictions for multihop BFD:

- BFD does not support echo mode. You can configure sessions for minimum timer interval.
- The minimum guaranteed timer depends on the topology, scale, number of hops, and control plane processing. All the packets must reach the control plane since echo mode is not supported.

- Supports IPv4 deployments only.
- Authentication for multihop BFD is not enabled on Cisco ASR901 routers.

Information About Multihop BFD

Overview of Multihop BFD

Cisco ASR 901 supports BFD on arbitrary paths, which can span multiple network hops. You must configure the **bfd-template** and **bfd map** commands to create a multihop template and associate it with one ore more maps of destinations and associated timers. You can enable authentication and configure a key chain for multihop BFD sessions.

How to Configure Multihop BFD

This section contains the following procedures:

Configuring Multihop BFD Template

Complete the following steps to create a multihop BFD template and configure BFD interval timers, authentication, and key chain:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bfd-template multi-hop** *template-name* **Example:** `Router(config)# bfd-template multi-hop mh-template1`	Creates a BFD multihop BFD template and enters BFD configuration mode.
Step 4	**interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value* **Example:**	Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.

	Command or Action	Purpose
	`Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	
Step 5	**authentication** *authentication-type* **keychain** *keychain-name* **Example:** `Router(bfd-config)# authentication keyed-sha-1 keychain bfd-multihop`	Configures authentication for the multihop template and the authentication type.
Step 6	**end** **Example:** `Router(bfd-config)# end`	Returns the router to privileged EXEC mode.

Configuring a Multihop BFD Map

After configuring the interval timers and authentication in a template, you must configure a map to associate the template with unique source-destination address pairs for multihop BFD sessions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bfd mapipv4 vrf** *vrf-name destination-address/length source-address/length template-name* **Example:** `Router(config)# bfd-template multi-hop mh-template1`	Configures a BFD map and associates it with the template.
Step 4	**end** **Example:** `Router(config)# end`	Returns the router to privileged EXEC mode.

Configuration Examples for Multihop BFD

This section provides the configuration example for multihop BFD.

Example : Configuring Multihop BFD

The following example shows how to configure BFD in a BGP network. In the following example, the simple BGP network consists of Router A and Router B. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 in Router B.

Configuration for Router A

```
!
interface Fast Ethernet 0/1
ip address 172.16.10.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
!
router bgp 40000
bgp log-neighbor-changes
neighbor 172.16.10.2 remote-as 45000
neighbor 172.16.10.2 fall-over bfd
!
address-family ipv4
neighbor 172.16.10.2 activate
no auto-summary
no synchronization
network 172.18.0.0 mask 255.255.255.0
exit-address-family
!
```

Configuration for Router B

```
!
interface Fast Ethernet 6/0
ip address 172.16.10.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
ip address 172.18.0.1 255.255.255.0
!
router bgp 45000
bgp log-neighbor-changes
neighbor 172.16.10.1 remote-as 40000
neighbor 172.16.10.1 fall-over bfd
!

address-family ipv4
neighbor 172.16.10.1 activate
no auto-summary
no synchronization
network 172.17.0.0 mask 255.255.255.0
exit-address-family
```

!

Where to Go Next

For additional information on configuring Multihop BFD, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for Multihop BFD

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.

Table 31: Feature Information for Multihop BFD, on page 538 lists the release history for this feature and provides links to specific configuration information.

Note Table 31: Feature Information for Multihop BFD, on page 538 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 31: Feature Information for Multihop BFD

Feature Name	Releases	Feature Information
Multihop BFD	15.2(2)SNG	See the following links for more information about this feature: • Restrictions for Multihop BFD, on page 533 • Configuring Multihop BFD Template, on page 534 • Configuring a Multihop BFD Map, on page 535 • Configuration Examples for Multihop BFD, on page 536

CHAPTER 30

Bit Error Rate Testing

This feature module describes how to configure a Bit Error Rate Test (BERT) and display the test results for channelized line cards in the Cisco ASR 901 Series Aggregation Services Routers.

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 Bit Error Rate Testing, on page 543.

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 BERT

- To run BERT in unframed mode on a controller, you should set the “framing” configuration of the controller to “unframed”.
- When running BERT, your system expects to receive the same pattern that it is transmitting. If traffic is not being transmitted or received, create a back-to-back loopback BERT on the link or in the network, and send out a predictable stream to ensure that you receive the same data that was transmitted.
- To determine if the remote serial port returns the BERT pattern unchanged, you must manually enable network loopback at the remote serial port while you configure a BERT pattern to use in the test at specified time intervals on the local serial port.

Restrictions

- BERT affects the functionality of any configured protocol on a controller on which it is initiated. The configured protocol functionality is resumed after the BERT process is completed or successfully canceled.
- BERT is not supported for channelized E1/T1 (per time slot).

Feature Overview

The BERT feature is used to test the integrity of the physical layer. Using this feature, you can test cables and diagnose signal problems in the field.

BERT generates a specific pattern on to the egress data stream of a E1/T1 controller and then analyzes the ingress data stream for the same pattern. The bits that do not match the expected pattern are counted as bit errors.

The bit error rate (BER) is determined by comparing the erroneous bits received with the total number of bits received. You can display and analyze the total number of error bits transmitted and the total number of bits received on the link. You can retrieve error statistics anytime during the BERT.

The ASR 901 router uses Pseudo-Random Binary Sequences (PRBSs) for the BERT. The following table lists the PRBSs supported on the ASR 901 routers.

Table 32: BERT Pattern Supported in Cisco ASR 901 Routers

BERT Pattern	Description
0’s	Test pattern consisting of all 0’s that is used to test line coding
1’s	Test pattern consisting of all 1’s that is used to test alternating line volt and repeaters
2^11	Pseudo-random repeating test pattern that consists of 2,048 bits
2^15	Pseudo-random repeating test pattern that consists of 32,767 bits
2^20 QRSS	Pseudo-random repeating test pattern that consists of 1,048,575 bits
Alt 0’s and 1’s	Test pattern consisting of alternating 0’s and 1’s that is used to test the preamp and equalizer

How to Configure BERT

The ASR 901 router supports BERT on all 16 E1/T1 controllers simultaneously. Additionally, you can cancel an already initiated BERT.

This section describes how to configure and perform a BERT on E1/T1 controllers, and how to stop or verify the test:

Performing BERT on a T1/E1 Line

To enable BERT pattern on a T1 or E1 controller, perform the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller T1 0/5`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**bert pattern** *pattern* **interval** *time* **Example:** `Router(config-controller)# bert pattern 0s interval 30`	Sends a BERT pattern through the T1 or E1 line for the specified time interval. • *pattern*—Length of the repeating BERT. • **interval**—Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.

Terminating BERT on a T1/E1 Controller

Procedure

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

	Command or Action	Purpose
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller T1 0/5`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**no bert pattern** *pattern* **interval** *time* **Example:** `Router(config-controller)# no bert pattern`	Terminates the BER test running on the specified T1 or E1 line.

Verifying BERT on a T1/E1 Controller

To verify that BERT is running on a T1/E1 controller, enter the **show controllers** command at any time during the test.

```
Router# show controllers e1 0/9
E1 0/9 is up.
Applique type is Channelized E1 - balanced
DSX1 BERT pattern : 2^15
DSX1 BERT sync : sync
DSX1 BERT sync count : 1
DSX1 BERT interval : 1
DSX1 BERT time remain : 49
DSX1 BERT total errs : 0
DSX1 BERT total k bits: 21068
DSX1 BERT errors (last): 0
DSX1 BERT k bits (last): 21068
Last clearing of BERT counters never
No alarms detected.
alarm-trigger is not set
Framing is crc4, Line Code is HDB3, Clock Source is Internal.
Data in current interval (68 seconds elapsed):
1 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 1 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Configuration Examples

The following is a sample configuration of the BERT feature.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#controller e1 0/9
Router(config-controller)#bert pattern 2^15 interval 1
```

Additional References

The following sections provide references related to bit error rate testing.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Bit Error Rate Testing

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 33: Feature Information for Bit Error Rate Testing

Feature Name	Releases	Feature Information
Bit Error Rate Testing	15.2(2)SNG	This feature was introduced.

CHAPTER 31

Microwave ACM Signaling and EEM Integration

This feature module describes the Microwave Adaptive Code Modulation (ACM) Signaling and Embedded Event Manager (EEM) integration, which enables the microwave radio transceivers to report link bandwidth information to an upstream Ethernet switch and take action on the signal degradation to provide optimal bandwidth.

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 table at the end of this module.

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 Microwave ACM Signaling and EEM Integration

- The microwave transceiver in the network topology must support adaptive bandwidth modulation, and the microwave transceiver must support the Ethernet Connectivity Fault Management (CFM) extension for microwave devices as defined by Cisco.
- In a heterogeneous ring topology, all devices connected directly to the microwave transceiver must support signal degradation (SD) functions. Devices not connected directly to the microwave transceiver can be standard-compliant nodes or enhanced SD-capable nodes.

- In a homogeneous ring topology, all links must be microwave links and all devices must support microwave SD-based ring protection.
- A ring topology with multiple microwave links can experience a signal degradation condition on one or more of the microwave links. Only one signal degradation condition per ring instance is supported. This support is provided on a first-come, first-serve basis, per ring instance.
- The source MAC address must be an unique MAC address. It can be the MAC address of the Ethernet port or the Bridge.
- The destination MAC address must be set to the CCM multicast address for the associated maintenance level (a multicast address is used to avoid discovery of MAC addresses).
- The microwave transceiver in the network topology must support bandwidth vendor specific message (BW-VSM1).
- The BW-VSM may be sent untagged, or it may be transmitted with a configurable valid IEEE 802.1Q VLAN tag.
- The BW-VSM must be associated with maintenance level 0. The microwave equipment should allow the network operator to associate the message with a valid maintenance level in the range 0 to 7 per ITU-T Y.1731 / IEEE 802.1ag-2007.

Feature Overview

Microwave links are often used in Ethernet access ring topologies and the bandwidth provided by the microwave link depends on environmental factors like fog, rain, and snow, which can drastically affect the bandwidth.

This feature relies on the Ethernet CFM to assess the environmental conditions on either end of the microwave link and automatically change the modulation to provide optimal bandwidth. The Ethernet CFM monitors the microwave link bandwidth, and when a link degradation is detected, notifies the router to take action on the degraded microwave link.

In IP/MPLS, the nodes are unaware of any changes to the bandwidth on the microwave link and the Gigabit Ethernet connection to the nodes remain constant. To ensure optimal routing and traffic transport across the access network, a mechanism has been implemented to notify the IP/MPLS access nodes of any ACM events on the microwave links. This enables microwave radio transceivers, which support ACM, to report link bandwidth information to an upstream Ethernet switch.

The vendor-specific message (VSM) in Y.1731 is used to notify Cisco routers of ACM events, and the bandwidth available on the microwave link. Acting on this information, the node can change the Hierarchical Quality of Service (H-QoS), adjust the Interior Gateway Protocol (IGP) metric of the link to the new capacity or remove the degraded link.

H-QoS Policy Adjustment

H-QoS policy adjustment is the process of adjusting the egress H-QoS policy parameters on the IP/MPLS access node connected to the microwave link. This modifies the parent shaper rate to match the current bandwidth of the microwave link. It also adjusts the child class parameters to ensure correct priority and bandwidth-guaranteed traffic.

If the available bandwidth is less than the total bandwidth required by Expedited Forwarding (EF) and Assured Forwarding (AF) classes, the operator can choose to drop AF class traffic or remove the link from the service.

IGP Metric Adjustment

The IP/MPLS access node can adjust the IGP metric on the microwave link to align it with the available bandwidth. This will trigger an IGP SPF recalculation, allowing the IGP to get the correct bandwidth for routing traffic.

Link Removal

Link removal is the process of removing the microwave link from the IGP. This occurs when the bandwidth loss breaches the threshold set by the operator. It sets off the resiliency mechanisms in the network, and the degraded link is bypassed, resulting in minimal traffic loss. The degraded link is not brought administratively down. When it is up, the microwave equipment can signal to the access node about its status and usability.

Benefits

- The IP/MPLS access network adapts intelligently to the microwave capacity change by:
  - optimizing routing
  - controlling congestion
  - enabling loss protection.
- Microwave ACM changes are signaled through a Y.1731 VSM to the IP/MPLS access node.
- The IP/MPLS access node adapts the IGP metric of the link to the new capacity.
- The IP/MPLS access node can change the H-QOS policy on the interface with the microwave system allowing EF traffic to survive.
- The IP/MPLS access node can remove a degraded link from SPF triggering a loss protection.

How to Configure Microwave ACM Signaling and EEM Integration

This section describes how to configure Microwave ACM Signaling and EEM Integration:

Configuring Connectivity Fault Management

To configure CFM between the microwave outdoor unit (ODU) and the router, complete the following steps:

Note For a ring topology, you should configure CFM between the microwave ODU and the router. You must configure two VLANs to the two microwave ODUs, to process the vendor specific message (VSM) and trigger the Embedded Event Manager (EEM).

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Router(config)# ethernet cfm domain outer level 3`	Defines a CFM maintenance domain at a particular maintenance level and enter Ethernet CFM configuration mode. • *domain-name*—String of a maximum of 154 characters that identifies the domain. • *level-id*—Integer from 0 to 7 that identifies the maintenance level.
Step 4	**service** *csi-id evc evc-name* **vlan** *vlan-id* **direction down** **Example:** `Router(config-ether-cfm)# service microwave1 evc V60 vlan 60 direction down`	Sets a universally unique ID for a customer service instance (CSI) within a maintenance domain. • *csi-id*—String of a maximum of 100 characters that identifies the CSI. • **evc**—Specifies the EVC. • *evc-name*—String that identifies the EVC. • **vlan**—Specifies the VLAN. • *vlan-id*—String that identifies the VLAN ID. Range is from 1 to 4094. • **direction**—Specifies the service direction. • **down**—Specifies the direction towards the LAN.
Step 5	**continuity-check** **Example:** `Router(config-ecfm-srv)# continuity-check`	Enables the transmission of continuity check messages (CCMs).
Step 6	**exit** **Example:** `Router(config-ecfm-srv)# exit`	Exits Ethernet CFM service configuration mode and enters global configuration mode.
Step 7	**ethernet evc** *evc-id* **Example:** `Router(config)# ethernet evc V60`	Defines an EVC and enters EVC configuration mode. • *evc-id*—String from 1 to 100 characters that identifies the EVC.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-evc)# exit`	Exits Ethernet EVC configuration mode and enters global configuration mode.
Step 9	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/11`	Specifies an interface type and number, and enters interface configuration mode.
Step 10	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 60 ethernet 60`	Configures an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface.
Step 11	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if)# encapsulation dot1q 60`	Enables IEEE 802.1Q encapsulation of traffic on a specified interface in a VLAN. • *vlan-id*—Virtual LAN identifier.
Step 12	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. • **pop**—Removes a tag from a packet. • **1** —Specifies the outermost tag for removal from a packet. • **symmetric**—Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
Step 13	**bridge-domain** *bridge-domain-id* **Example:** `Router(config-if)# bridge-domain 60`	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). • *bridge-domain-id*—Bridge domain identifier.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Configuring EEP Applet Using CLIs

To configure EEP applet, complete the following steps:

Before you begin

- One switch virtual interface (SVI) or bridge domain is required per physical link.
- One EEM script is required per physical link.

Note The EEM script configures the metric on the microwave link and adjusts the QoS policy based on the Ethernet event parameters. You can download the scripts from the following location:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**event manager applet** *applet-name* **Example:** `Router(config)# event manager applet ACM61`	Registers an applet with the Embedded Event Manager (EEM) and enters applet configuration mode. • *applet-name*—Name of the applet file.
Step 4	**event tag** *event-tag* **ethernet microwave clear-sd** {**interface** *type number*} **Example:** `Router(config-applet)# event tag event_cd ethernet microwave clear-sd interface GigabitEthernet0/10`	Specifies the event criteria for an EEM applet that is run by matching a Cisco IOS command-line interface (CLI). • **tag**—Specifies a tag using the event-tag argument that can be used with the trigger command to support multiple event statements within an applet. • *event-tag*—String that identifies the tag.
Step 5	**event tag** *event-tag* **ethernet microwave sd {interface** *type number*} **threshold** *mbps* **Example:** `Router(config-applet)# event tag event_sd ethernet microwave`	Specifies the event criteria for an EEM applet that is run by matching a Cisco IOS CLI.

	Command or Action	Purpose
	`sd interface GigabitEthernet0/10 threshold 1000`	
Step 6	**action** *action-id* **set** *variable-name variable-value* **Example:** `Router(config-applet)# action 110 set ifname "vlan $_svi61"`	Sets the value of a variable when an EEM applet is triggered. • *action-id*—Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks. • *variable-name*—Name assigned to the variable to be set. • *variable-value*—Value of the variable.
Step 7	**action** *action-id* **cli command** *cli-string* **Example:** `Router(config-applet)# action 458 cli command "event manager applet ACM61"`	Specifies the action of executing a Cisco IOS CLI when an EEM applet is triggered. • *action-id*—Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks. • **command**—Specifies the message to be sent to the Cisco IOS CLI. • *cli-string*—CLI string to be executed. If the string contains embedded blanks, enclose it in double quotation marks.
Step 8	**action** *action-id* **cli command** *cli-string* **Example:** `Router(config-applet)# action 460 cli command "event tag event_sd ethernet microwave sd interface GigabitEthernet0/10 threshold $nb"`	Specifies the action of executing a Cisco IOS CLI command when an EEM applet is triggered. • *action-id*—Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks. • **command**—Specifies the message to be sent to the Cisco IOS CLI. • *cli-string*—CLI string to be executed. If the string contains embedded blanks, enclose it in double quotation marks.
Step 9	**exit** **Example:** `Router(config-applet)# exit`	Exits applet configuration mode.

Configuring Event Handler

To configure the microwave event handler, which runs hold-off timer, loss threshold, and fading wait-to-restore (WTR) timers that are configurable per interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ethernet event microwave hold-off** *seconds* **Example:** `Router(config-if)# ethernet event microwave hold-off 30`	Configures the settings of the Ethernet microwave event. • **hold-off**—Specifies the microwave bandwidth degradation hold-off time, in seconds. This time is used to prevent changes in the state of the network node as a result of signal degradation (SD) occurrences. • *seconds*—Hold off time, in seconds. The valid values range from 0 to 600, with a default value of 0.
Step 5	**ethernet event microwave loss-threshold** *number-of-messages* **Example:** `Router(config-if)# ethernet event microwave loss-threshold 100`	Configures the settings of the Ethernet microwave event. • **loss-threshold**—Specifies the number of bandwidth Vendor-Specific Messages (VSM) sent from the microwave transceiver to the Cisco device. • *number-of-messages*—Number of bandwith VSMs. The valid values range from 2 to 255, with a default value of 3.
Step 6	**ethernet event microwave wtr** *seconds* **Example:**	Configures the settings of the Ethernet microwave event.

	Command or Action	Purpose
	`Router(config-if)# ethernet event microwave wtr 45`	• **wtr**—Specifies the wtr time. This time is used to prevent changes in the state of the network node as a result of recovery events after an SD occurrence. • *seconds*—WTR time, in seconds. The valid values range from 0 to 600, with a default value of 10.

Verifying Microwave Microwave ACM Signaling and EEM Integration Configuration

To verify the microwave ACM and EEM integration configuration, use the show commands described in the following examples.

To display microwave bandwidth status information of an interface, use the following show command.

```
Router# show ethernet event microwave status [interface]
Microwave Bandwidth Status for GigabitEthernet0/0/2
 State : Degraded
 Elapsed time in this state : 1:25:33
 Nominal Bandwidth : 512Mbps
 Current Bandwidth : 256Mbps
 Lowest Bandwidth Since Entering Degraded : 64Mbps
 Last VSM Received : Oct 27 14:06:19.983
 Sender Transmit Period : 1 second
 Sender Address : 01AB.CC00.1881
 Hold Timer : Not Running
 Restore Timer : Not Running
 Periodic Timer : 2333 msec
 Hold Time : 0 seconds
 Restore Time : 10 seconds
 Loss-Threshold: 3
```

To display microwave bandwidth statistics of an interface, use the following show command.

```
Router# show ethernet event microwave statistic [interface]
Microwave Bandwidth Statistics for GigabitEthernet0/0/2
 Total VSM Receive Count : 145
 Total VSM Drop Count : 0
 Number of transitions into Degraded state : 2
```

Configuration Examples for Microwave ACM Signaling and EEM Integration

This section provides sample configuration examples for Microwave ACM Signaling and EEM Integration feature on the Cisco ASR 901 router.

Example: Configuring CFM

The following is a sample configuration of CFM.

```
!
ethernet cfm domain outer level 3
service microwave1 evc V60 vlan 60 direction down
  continuity-check
!
ethernet evc V60
!
interface GigabitEthernet0/11
!
service instance 60 ethernet V60
  encapsulation dot1q 60
  rewrite ingress tag pop 1 symmetric
  bridge-domain 60
!
```

Example: Configuring EEP Applet

The following is a sample EEM script to configure metric on a microwave link and adjust a QoS policy according to the ethernet event parameters sent through OAM.

Note You should have one SVI/BD per physical link. Also, one EEM script is required per physical link. In all, there should be two EEM scripts and two SVI/BDs:

```
! ACM script
no event manager applet ACM62
event manager applet ACM62
 event tag event_cd ethernet microwave clear-sd interface GigabitEthernet0/10
 event tag event_sd ethernet microwave sd interface GigabitEthernet0/10 threshold 1000
 trigger
  correlate event event_cd or event event_sd
! Variable settings
 action 100 set olc "100"
 action 102 set dlc "1"
 action 104 set n "$_ring_nodes"
 action 106 set cb "$_ethernet_current_bw"
 action 108 set nb "$_ethernet_nominal_bw"
 action 110 set ifname "vlan $_svi61"
 action 112 set cpmap_bw 0
 action 114 set pri_bw 0
 action 116 set ppmap 0
 action 118 set s1 "EEM-"
 action 120 set zeros "000000"
 action 122 set cb_bps "$cb$zeros"
 action 124 set nb_bps "$nb$zeros"
 action 126 set ifcfg 1
 action 130  cli command "enable"
 action 132  cli command "conf t"
! Restore the original QoS policy
 action 160 if $cb eq $nb
 action 162  cli command "interface $_ethernet_intf_name"
 action 163  cli command "no service-policy output $s1$ppmap"
 action 164  cli command "service-policy output $ppmap"
```

```
! QoS block
! Find an original parent policy-map name and create a new name
 action 180 elseif $_eem_mode le "1"
 action 181  if $ppmap eq "0"
 action 182   cli command "do show run int $_ethernet_intf_name | i service-policy output"
# action 184   syslog msg "cli_result 184: $_cli_result, into: $_ethernet_intf_name"
 action 186   regexp "service-policy output (.*)\n" "$_cli_result" line pmap
# action 188   syslog msg "line 196: $line"
# action 190   string replace "$line" 0 21 ""
 action 192   string trimright "$pmap"
# action 194   syslog msg "QoS done. string 194: $_string_result, line: $line"
 action 196   set pmap $_string_result
 action 197  else
 action 198   set pmap $ppmap
 action 199  end
 action 200  syslog msg "s1pmap 200: $s1$pmap"
! Find an original child policy-map name and create a new name
 action 214  cli command "do show run policy-map $pmap | i service-policy"
# action 215  syslog msg "cli_result 215: $_cli_result"
 action 216  regexp "service-policy (.*)\n" "$_cli_result" line cpmap
 action 217  string trimright "$cpmap"
 action 218  set cpmap "$_string_result"
# action 219  syslog msg "cpmap 219: $s1$cpmap"
 action 220  cli command "do show run policy-map $cpmap"
 action 221  regexp "class .*!" $_cli_result string
! Configuration of a new child policy-map
 action 223  cli command "policy-map $s1$cpmap"
 action 226  foreach var "$string" "\n"
 action 228   regexp "class (.*)" $var match cname
 action 230   if $_regexp_result eq 1
# action 233    syslog msg "233: cname: $cname"
 action 234   end
! Calculate bandwidth for each of the classes
 action 236   regexp "(priority|bandwidth) percent (.*)" $var line cmd ef_bw_perc
 action 238   if $_regexp_result eq 1
 action 256    string trimright "$ef_bw_perc"
# action 258    syslog msg "258: cb_bps: $nb_bps, ef_bw_perc:$_string_result"
 action 260     divide $nb_bps 100
 action 262     multiply $_result $_string_result
 action 263     set bw_demand $_result
 action 264     add $cpmap_bw $_result
 action 266     syslog msg "266: cpmap_bw: $_result, bw_demand: $bw_demand"
 action 268    set cpmap_bw $_result
 action 269    syslog msg "269: cpmap_bw sub-sum: $cpmap_bw"
 action 270    regexp "priority percent (.*)" $line match
 action 272    if $_regexp_result eq 1
 action 274     add $pri_bw $bw_demand
 action 276     multiply $bw_demand 100
 action 278     divide $_result $cb_bps
 action 279     if $_remainder gt 0
 action 280      increment _result
 action 281     end
 action 282     set match1 "priority percent $_result"
 action 283     set match2 "priority percent $_result"
 action 284    end
 action 286    regexp "bandwidth percent (.*)" $line match
 action 288    if $_regexp_result eq 1
 action 290     set match1 "$match"
 action 292     set match2 "bandwidth percent 1"
 action 294    end
 action 296    else
 action 298     set match1 "$var"
 action 300     set match2 "$var"
 action 302   end
```

```
 action 304   append cfg_out1 "$match1 \n"
 action 306   append cfg_out2 "$match2 \n"
 action 308  end
! Check if there is enough bandwidth on a uwave link
 action 310  syslog msg "310: cpmap_bw sum: $cpmap_bw"
 action 312  if $cpmap_bw lt $cb_bps
 action 314   set cfg_out "$cfg_out1"
 action 316  elseif $pri_bw lt $cb_bps
 action 318   set cfg_out "$cfg_out2"
 action 320  else
 action 322   set metric 1000000
 action 323   set ifcfg 0
 action 324  end
! Configuration of a child QoS policy
 action 325  if $ifcfg eq 1
 action 326   foreach var "$cfg_out" "\n"
 action 328    cli command "$var"
 action 330   end
 action 331  end
! Configuration of a parent QoS policy
 action 332  cli command "policy-map $s1$pmap"
 action 334  syslog msg "config 334: policy-map $s1$pmap"
 action 336  cli command "class class-default"
 action 338  cli command "shape average $cb_bps"
 action 340  cli command "service-policy $s1$cpmap"
! Apply the QoS policy on a PHY interface
 action 344  cli command "int $_ethernet_intf_name"
 action 346  cli command "no service-policy output $pmap"
 action 348  cli command "service-policy output $s1$pmap"
 action 390 end
! End of the QoS part
! IGP metric block
 action 400 if $_eem_mode ge 1
 action 402  multiply $n $cb
 action 404 divide $_result $nb
 action 406  syslog msg "406: cb: $cb nb: $nb result: $_result"
 action 408  set m $_result
 action 410  syslog msg "m: $m"
 action 412  increment n
 action 414  subtract $n $m
 action 416  multiply $_result $olc
 action 418  if $ifcfg eq 0
 action 420   set dlc $metric
 action 422  else
 action 424   set dlc $_result
 action 426  end
 action 428  syslog msg "428: n:$n m:$m olc:$olc dlc:$dlc result:$_result intf: $ifname"
# action 430  cli command "enable"
# action 432  cli command "conf t"
 action 434  cli command "int $ifname"
 action 436  cli command "do show run int $ifname"
 action 438  string first "ip router isis" "$_cli_result"
 action 440  if $_string_result ne "-1"
 action 442   cli command "isis metric $dlc"
 action 444   cli command "do show ip ospf int | i $ifname"
 action 446   string first "$ifname" "$_cli_result"
 action 448  elseif $_string_result ne "-1"
 action 450   cli command "ip ospf cost $dlc"
 action 452  end
 action 454 end
! Adjust the current applet
 action 456 syslog msg "The EEM script executed"
 action 458 cli command "event manager applet ACM62"
 action 460 cli command "event tag event_sd ethernet microwave sd interface
```

```
GigabitEthernet0/10 threshold $nb"
 action 462 if $ppmap eq 0
 action 464  if $_eem_mode le 1
 action 466   cli command "action 116 set ppmap $pmap"
 action 468  end
 action 470 end
! End of the script
```

Example: Configuring Event Handler

The following is a sample configuration of Event Handler.

```
event manager applet mw_ring_sd1
 event ethernet microwave sd interface gigabitethernet 0/0/0 threshold 400
 action 1 switch ring g8032 ringA instance 1
interface gigabitethernet 0/0/0
 ethernet event microwave hold-off 30
 ethernet event microwave loss-threshold 100
 ethernet event microwave wtr 45
```

Additional References

The following sections provide references related to Microwave ACM Signaling and EEM Integration feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
G.8032 and CFM Support for Microwave Adaptive Bandwidth	Carrier Ethernet Configuration Guide

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
IMA-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Microwave ACM Signaling and EEM Integration

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 34: Feature Information for Microwave ACM Signaling and EEM Integration

Feature Name	Releases	Feature Information
Microwave ACM Signaling and EEM Integration	15.3(2)S	This feature was introduced on the Cisco ASR 901 routers.

CHAPTER 32

IPv6 Support on the Cisco ASR 901 Router

This document provides implementation and command reference information for IPv6 features supported on the Cisco ASR 901 router. We strongly recommend that you read this entire document before reading other documents on IPv6 for Cisco IOS software.

Detailed conceptual information about the features supported on the Cisco ASR 901 router, is documented outside of this feature in the Cisco IOS software documentation. For information about the location of this related documentation, see the Feature Information for IPv6 Support on the Cisco ASR 901 Router, on page 600.

Complete configuration information of ASR 901-specific IPv6 features is provided in this document. This information can be found in the How to Configure IPv6 Support on the Cisco ASR 901 Router, on page 566.

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 table at the end of this module.

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 IPv6 Support on the Cisco ASR 901 Router

- Cisco IOS Release 15.2(2)SNG or a later IPv6-supporting release must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- To forward IPv6 traffic using Cisco Express Forwarding (CEF) or distributed CEF, you must configure forwarding of IPv6 unicast datagrams globally on the router by using the ipv6 unicast-routing command, and you must configure an IPv6 address on an interface by using the ipv6 address command.
- You must enable CEF for IPv4 globally on the router by using the ip cef command before enabling Cisco Express Forwarding for IPv6 globally on the router by using the ipv6 cef command.

Restrictions for IPv6 Support on the Cisco ASR 901 Router

- Switch port configuration is not supported.
- The fastethernet interface does not expect more than one IPv6 address.
- The following features are not supported:
    - Tunneling protocols such as IPv4-to-IPv6 or IPv6-to-IPv4
    - IPv6 Policy-Based Routing
    - Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) for IPv6
    - Quality of service (QoS) based on IPv6 addresses
    - IPv6 support of IEEE 1588v2
    - IPv6 support over slower links like time-division multiplexing (TDM) interfaces, Multilink Point-to-Point Protocol (MLPPP), etc
    - IPv6 Access Control Lists (ACLs) was not supported prior to Cisco IOS Release 15.4(2)S.
    - IPv6 over IP and Multiprotocol Label Switching (MPLS)
    - Bidirectional Forwarding Detection for IPv6 (BFDv6) for Intermediate System-to-Intermediate System (IS-IS)
    - IPv6 Virtual Routing and Forwarding (VRF) Lite

Information About IPv6 Support on the Cisco ASR 901 Router

Benefits

IPv6 Support on the Cisco ASR 901 router provides the following benefits:

- Supports state-less auto-configuration of IPv6 addresses.
- Supports the following routing protocols:
    - Static routing
    - Open Shortest Path First (OSPF) version 3
    - Border Gateway Protocol
    - Intermediate System-to-Intermediate System (IS-IS)

Overview of IPv6

IPv6 is the latest version of the Internet Protocol that has a much larger address space and improvements such as a simplified main header and extension headers. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses.

The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. IPv6 supports widely deployed routing protocols such as Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF) for IPv6, and multiprotocol Border Gateway Protocol (BGP). Other available features include stateless autoconfiguration and enhanced support for Mobile IPv6.

IPv6 is being introduced on the Cisco ASR 901 router to support Long Term Evolution (LTE) rollouts that provides high-bandwidth data connection for mobile wireless devices. The IPv6 transport utilizes Switch Virtual Interface (SVI) and Ethernet interfaces. The Cisco ASR 901 router also supports IPv6 addressing on Loopback interfaces.

IPv6 Address Formats

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

```
2001:DB8:7654:3210:FEDC:BA98:7654:3210
2001:DB8:0:0:8:800:200C:417A
```

It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less complicated, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). Table 35: Compressed IPv6 Address Formats , on page 561 lists compressed IPv6 address formats.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interface, but only one link-local address.

Note Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. The hexadecimal letters in IPv6 addresses are not case-sensitive.

Table 35: Compressed IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The loopback address listed in Table 35: Compressed IPv6 Address Formats , on page 561 are used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).

Note The IPv6 loopback address cannot be assigned to a physical interface. A packet that has the IPv6 loopback address as its source or destination address must remain within the node that created the packet. IPv6 routers do not forward packets that have the IPv6 loopback address as their source or destination address.

The unspecified address listed in Table 35: Compressed IPv6 Address Formats , on page 561 indicates the absence of an IPv6 address. For example, a newly initialized node on an IPv6 network may use the unspecified address as the source address in its packets until it receives its IPv6 address.

Note The IPv6 unspecified address cannot be assigned to an interface. The unspecified IPv6 addresses must not be used as destination addresses in IPv6 packets or the IPv6 routing header.

An IPv6 address prefix, in the format *ipv6-prefix*/*prefix-length*, can be used to represent bit-wise contiguous blocks of the entire address space. The *ipv6-prefix* must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:DB8:8086:6502::/32 is a valid IPv6 prefix.

For more information on IPv6 Addressing and Basic Connectivity, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv6 Addressing and Discovery

The IPv6 addressing and discover consists of static and autoconfiguration of addresses – both global and link local addresses. IPv6 differs from IPv4 in that same interface can have multiple IPv6 addresses assigned to it. The Cisco ASR 901 router supports both IPv4 and multiple IPv6 addresses on the same Loopback and SVI interface. The link-local addresses are automatically generated (if ipv6 enable command is configured) from the MAC-address of the interface as soon as the SVI comes up.

Static Configuration

Static configuration is the manual process of defining an explicit path between two networking devices. The administrator of the network manually enters the IPv6 addresses, subnet masks, gateways, and corresponding MAC addresses for each interface of each router into a table. Static configuration provides more control over the network but it requires more work to maintain the table. The table must be updated every time routes are added or changed. Moreover, the static routes must be manually reconfigured if there is a change in the network topology.

Static configuration provides security and resource efficiency. It uses less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. Static routes created by the static configuration can be redistributed into dynamic routing protocols. However, routes generated by dynamic routing protocols cannot be redistributed into the static routing table.

Static configuration is useful for smaller networks with only one path to an outside network and in providing security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.

Stateless Autoconfiguration

All interfaces on IPv6 nodes must have a link-local address, which is usually automatically configured from the identifier for an interface and the link-local prefix FE80::/10. A link-local address enables a node to communicate with other nodes on the link and can be used to further configure the node.

Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a Dynamic Host Configuration Protocol (DHCP) server.

With IPv6, a router on the link advertises in RA messages any global prefixes, and its willingness to function as a default router for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection (DAD) to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

For more information on IPv6 Addressing and Discovery, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

ICMPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages such as ICMP destination unreachable messages, and informational messages such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6.

For more information on ICMPv6, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv6 Duplicate Address Detection

During the stateless autoconfiguration process, duplicate address detection (DAD) verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). DAD is first performed first on the new link-local address. When the link local address is verified as unique, then DAD is performed on the remaining IPv6 unicast addresses on the interface.

When a duplicate address is identified, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is issued. If the duplicate address is a global address of the interface, the address is not used and an error message is issued. However, all configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and keep track of neighboring routers.

Neighbor solicitation messages (ICMPv6 Type 135) are sent on the local link by nodes attempting to discover the link-layer addresses of other nodes on the local link. The neighbor solicitation message is sent to the solicited-node multicast address.The source address in the neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The neighbor solicitation message also includes the link-layer address of the source node.

After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICPMv6 Type 136) on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node sending the neighbor advertisement message; the destination address is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node communicate with each other.

For more information on IPv6 Neighbor Discovery, see the Implementing IPv6 Addressing and Basic Connectivity chapter of IPv6 Configuration Guide, at the following location:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-addrg-bsc-con.html

IPv4 and IPv6 Dual-Stack on an Interface

A dual stack means that IPv4 and IPv6 addresses coexist on the same platform and support hosts of both types. This method is a way to transition from IPv4 to IPv6 with coexistence (IPv4 and IPv6) as a first step.

The Cisco ASR 901 router supports the configuration of both IPv6 and IPv4 on an interface. You do not need to enter any specific commands to do so; simply enter the IPv4 configuration commands and IPv6 configuration commands as you normally would. Make sure you configure the default route for both IPv4 and IPv6.

Routing Protocols

The Cisco ASR 901 router supports widely deployed routing protocols such as IS-IS, OSPFv3, and multiprotocol BGP.

IS-IS Enhancements for IPv6

IS-IS in IPv6 functions the same as in IPv4 and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. Extensions to the IS-IS command-line interface (CLI) allow configuration of IPv6-specific parameters. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

For more information on IS-IS Enhancements for IPv6, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-is-is.html

OSPFv3 for IPv6

OSPF is a routing protocol for IP. It is a link-state protocol. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. The state of a link is a description of that interface, and its relationship to its neighboring networking devices. The interface information includes the IPv6 prefix of the interface, the network mask, the type of network it is connected to, the devices connected to that network, and so on. This information is propagated in various type of link-state advertisements (LSAs).

For more information on OSPFv3 for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html

Multiprotocol BGP Extensions for IPv6

Multiprotocol BGP is the supported exterior gateway protocol (EGP) for IPv6. Multiprotocol BGP extensions for IPv6 support many of the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for an IPv6 address family and network layer reachability information (NLRI) and next hop (the next router in the path to the destination) attributes that use IPv6 addresses.

For more information on Multiprotocol BGP Extensions for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-mptcl-bgp.html

Bidirectional Forwarding Detection for IPv6

The BFDv6 is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. BFDv6 provides IPv6 support by accommodating IPv6 addresses and provides the ability to create BFDv6 sessions.

For more information on Bidirectional Forwarding Detection for IPv6, refer the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-bfd.html

QoS for IPv6

The Cisco ASR 901 router support of QoS features for IPv6 environments include ingress packet classification, policing, marking on Ethernet interfaces. It also supports egress packet classification, marking, scheduling, per interface and per qos-group shaping, Low Latency Queuing (LLQ), and weighted random early detection (WRED) on GigabitEthernet interfaces.

Note Queuing, shaping, scheduling and LLQ is not supported on the ingress path for the Ethernet interfaces. Policing is not supported on the egress path for GigabitEthernet interfaces.

The QoS implementation for IPv6 environment in the Cisco ASR router is the same as that of IPv4. For more information on Configuring QoS on the Cisco ASR 901 router, refer the following link:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/qos.html

For additional information on Implementing QoS for IPv6, refer the following link:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-qos.html

How to Configure IPv6 Support on the Cisco ASR 901 Router

Configuring IPv6 Addressing and Enabling IPv6 Routing

Perform this task to assign IPv6 addresses to individual router interfaces and enable IPv6 traffic forwarding globally on the router. By default, IPv6 addresses are not configured, and IPv6 routing is disabled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address/prefix-length* {**eui-64** | **link-local** | **anycast** } **Example:** `Router(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface. • **eui-64**—Specifies the global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. Only the 64-bit network prefix for the address needs to be specified; the last 64 bits are automatically computed from the interface ID. • **link-local**—Specifies the link-local address on the interface that is used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. • **anycast**—Specifies an IPv6 anycast address.
Step 5	**ipv6 enable** **Example:**	Enables IPv6 on the interface.

	Command or Action	Purpose
	`Router(config-if)# ipv6 enable`	
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.
Step 7	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 8	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables Cisco Express Forwarding (CEF) globally on the router.

Configuring a Static IPv6 Route

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 route** {*ipv6-prefix* | *prefix-length ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*] **Example:** `Router(config)# ipv6 route 2001::/64 5::5 100`	Configures a static default IPv6 route. • *ipv6-prefix*—The IPv6 network that is the destination of the static route. This could also be a host name when static host routes are configured. • *prefix-length*—The length of the IPv6 prefix. • *ipv6-address*—(Optional) The IPv6 address of the next hop that can be used to reach the specified network. • *interface-type*—Interface type. • *interface-number*—Interface number.

	Command or Action	Purpose
		• *administrative-distance*—(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes. • *administrative-multicast-distance*—(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF). • **unicast**—(Optional) Specifies a route that must not be used in multicast RPF selection. • **multicast**—(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB). • *tag*—(Optional) Tag value that is used as a "match" value for controlling redistribution via route maps.

Enabling Stateless Auto-Configuration

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface fastethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 address autoconfig** **Example:** `Router(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.

Implementing IPv6 on VLAN Interfaces

Perform the tasks given below to enable IPv6 on VLAN interfaces. By default, IPv6 is disabled on an interface.

Note For information on how to create a VLAN interface, see the Configuring Ethernet Virtual Connections document at the following location:
http://www.cisco.com/en/US/partner/docs/wireless/asr_901/Configuration/Guide/swevc.html

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface vlan 40`	Specifies an interface type and number, and places the router in interface configuration mode. farce

Step 4	Do one of the following:
	• **ipv6 enable**
	• **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
	Example:
	`Router(config-if)# ipv6 enable`
	`or`
	Example:
	`Router(config-if)# ipv6 address 2000::1/64`
		Configures IPv6 on the VLAN interface. Though both the commands automatically configure the link local address (LLA) on the interface, the **ipv6 address** command additionally configures an ipv6 address on the interface.
		• *ipv6-address*—The IPv6 address to be used.
		• *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
		• *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface.
		• *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the

	Command or Action	Purpose
		prefixes provided by the general prefix specified with the *prefix-name* argument.

Implementing IPv6 Addressing on Loopback Interfaces

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface loopback 0`	Specifies an interface type and number, and places the router in interface configuration mode.

Step 4	Do one of the following:
	• **ipv6 enable**
	• **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
	Example:
	`Router(config-if)# ipv6 enable`
	`or`
	Example:
	`Router(config-if)# ipv6 address 2000::1/64`
		Configures IPv6 on the Loopback interface. Though both the commands automatically configure the link local address (LLA) on the interface, the **ipv6 address** command additionally configures an ipv6 address on the interface.
		• *ipv6-address*—The IPv6 address to be used.
		• *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
		• *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface.
		• *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.

Configuring ICMPv6 Rate Limiting

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 icmp error-interval** *interval* **Example:** `Router(config)# ipv6 icmp error-interval 1200`	Configures the interval for IPv6 ICMP error messages. • *interval*—Specifies the interval between tokens, in milliseconds, being added to the bucket. The valid range is from 0 to 2147483647.

Configuring IPv6 Duplicate Address Detection

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# Interface Vlan 40`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 nd dad attempts** *value* **Example:**	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is

	Command or Action	Purpose
	`Router(config)ipv6 nd dad attempts 5`	performed on the unicast IPv6 addresses of the interface.

Configuring IPv6 Neighbor Discovery

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface type number** **Example:** `Router(config)# Interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 nd {advertisement-interval | autoconfig | cache | dad | managed-config-flag | na | ns-interval | nud | other-config-flag | prefix | ra | reachable-time | router-preference}** **Example:** `Router(config-if)# ipv6 nd autoconfig`	Configures a Neighbor Discovery on a specified interface on the router. • **advertisement-interval**—Sends an advertisement interval option in router advertisements (RAs). • **autoconfig**—Automatic configuration. • **cache**—Cache entry. • **dad**—Duplicate Address Detection. • **managed-config-flag**—Hosts should use DHCP for address config. • **na**—Neighbor advertisement control. Configures ND to extract an entry from an unsolicited NA. • **ns-interval**— Sets the advertised NS retransmission interval. • **nud** —Configures the number of times neighbor unreachability detection (NUD) resends neighbor solicitations (NSs). • **other-config-flag**—Hosts should use DHCP for non-address config.

	Command or Action	Purpose
		• **prefix**—Configures which IPv6 prefixes are included in IPv6 ND router advertisements. • **ra**—Router advertisement control. • **reachable-time**—Sets the advertised reachability time. • **router-preference**—Sets the default router preference value.

Configuring IPv6 and IPv4 Dual-Stack on the Same VLAN

Before you begin

You should enable IPv6 routing before proceeding with this task. See Configuring IPv6 Addressing and Enabling IPv6 Routing, on page 566.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface type number** **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config)# ip address 192.168.99.1 255.255.255.0`	Configures an IPv4 address on the interface.
Step 5	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:** `Router(config)# ipv6 address 2000::1/64`	Configures IPv6 address on the interface. • *ipv6-address*—The IPv6 address to be used. • *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how

	Command or Action	Purpose
		many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. • *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface. • *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.
Step 6	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 address on the interface.

Configuring OSPFv3 for IPv6

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface type number** **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 ospf** *process-id* **area** *area-id* **[instance** *instance-id***]** **Example:** `Router(config-if)# ipv6 ospf 1 area 0`	Enables OSPFv3 on an interface. • *process-id*—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process.

	Command or Action	Purpose
		• *area-id*—Area that is to be associated with the OSPFv3 interface. • *instance-id*—(Optional) Instance identifier.

Configuring IS-IS for IPv6

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode. • *area-tag*—Name for a routing process.
Step 4	**net** *network-entity-title* **Example:** `Router(config-router)# net 49.0001.0000.0000.000c.00`	Configures an IS-IS network entity title (NET) for the routing process. • *network-entity-title*—The network-entity-title argument defines the area addresses for the IS-IS area and the system ID of the router.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 7	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:**	Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface.

	Command or Action	Purpose
	`Router(config-if)# ipv6 address 2001:DB8::3/64`	• *ipv6-address*—The IPv6 address to be used. • *prefix-length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. • *prefix-name*—A general prefix, which specifies the leading bits of the network to be configured on the interface. • *sub-bits*—The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.
Step 8	**ipv6 router isis** *area-name* **Example:** `Router(config-if)# ipv6 router isis area2`	Enables the specified IPv6 IS-IS routing process on an interface. • *area-name*—Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a non-null area name to facilitate identification of the area. Optional for conventional IS-IS configuration.

Configuring Multiprotocol-BGP for IPv6

Perform this task to configure an IPv6 BGP routing process and an optional BGP router ID for a BGP-speaking router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 65000`	Configures a BGP routing process, and enters router configuration mode for the specified routing process. • *as-number*—Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. The range is from 1 to 65535.
Step 4	**no bgp default ipv4-unicast** **Example:** `Router(config-router)# no bgp default ipv4-unicast`	Disables the IPv4 unicast address family for the BGP routing process specified in the previous step.
Step 5	**bgp router-id** *ip-address* **Example:** `Router(config-router)# bgp router-id 192.168.99.70`	(Optional) Configures a fixed 32-bit router ID as the identifier of the local router running BGP.

Configuring BFD for IPv6

Perform the tasks given below to configure Bidirectional Forwarding Detection (BFD) for IPv6:

Specifying a Static BFDv6 Neighbor

Procedure

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

	Command or Action	Purpose
Step 3	**ipv6 route static bfd [vrf** *vrf-name***]** *interface-type interface-number ipv6-address* **[unassociated]** **Example:** `Router(config)# ipv6 route static bfd vlan 4000 2001::1`	Specifies static route IPv6 BFDv6 neighbors. • *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *interface-type*—Interface type. • *interface-number*—SVI name. • *ipv6-address*—IPv6 address of the neighbor. • **unassociated**—(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Associating an IPv6 Static Route with a BFDv6 Neighbor

IPv6 static routes are automatically associated with a static BFDv6 neighbor. A static neighbor is associated with a BFDv6 neighbor if the static next-hop explicitly matches the BFDv6 neighbor.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **Example:** `Router(config)# ipv6 route static bfd vlan 4000 2001::1`	Specifies static route IPv6 BFDv6 neighbors. • *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *interface-type*—Interface type. • *interface-number*—SVI name. • *ipv6-address*—IPv6 address of the neighbor. • **unassociated**—(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.
Step 4	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address* |	Establishes static IPv6 routes.

	Command or Action	Purpose
	interface-type [*interface-number ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance*] [**unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **Example:** `Router(config)# ipv6 route 2001:DB8::/64 vlan 4000 2001::1`	• *vrf-name*—(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes are specified. • *ipv6-prefix*—The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured. • *ipv6-address*—The IPv6 address of the next hop that can be used to reach the specified network. • *interface-type*—Interface type. • *interface-number*—SVI name. • **nexthop-vrf**—(Optional) Indicator that the next hop is a VRF. • *vrf-name1*—(Optional) Name of the next-hop VRF. • **default**—(Optional) Indicator that the next hop is the default. • *administrative-distance*—(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes. • *administrative-multicast-distance*—(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF). • **unicast**—(Optional) Specifies a route that must not be used in multicast RPF selection. • **multicast**—(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB). • *next-hop-address*—(Optional) Address of the next hop that can be used to reach the specified network. • **tag** *tag*—(Optional) Tag value that is used as a "match" value for controlling redistribution via route maps.

Configuring BFDv6 and OSPFv3

This section describes the procedures for configuring BFD support for OSPFv3, so that OSPFv3 is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.

There are two methods for enabling BFD support for OSPFv3:

- You can enable BFD for all of the interfaces for which OSPFv3 is routing by using the **bfd all-interfaces** command in router configuration mode.
- You can enable BFD for a subset of the interfaces for which OSPFv3 is routing by using the **ipv6 ospf bfd** command in interface configuration mode.

Before you begin

- OSPFv3 must be running on all participating routers.
- The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router ospf** *process-id* **Example:** `Router(config)# ipv6 router ospf 2`	Configures an OSPFv3 routing process. • *process-id*—Internal identification. It is locally assigned and can be a positive integer from 1 to 65535. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.
Step 4	**bfd all-interfaces** **Example:** `Router(config-rtr)# bfd all-interfaces`	Enables BFD for all interfaces participating in the routing process
Step 5	**end** **Example:** `Router(config-rtr)# end`	Enter this command twice to go to privileged EXEC mode.

Configuring BFDv6 for BGP

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-tag* **Example:** `Router(config)# router bgp 4500`	Specifies a BGP process and enter router configuration mode. • *as-tag*—Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. The range is from 1 to 65535.
Step 4	**neighbor** *ip-address* **fall-over bfd** **Example:** `Router(config-router)# neighbor 10.0.0.1 fall-over bfd`	Enables support for BFD failover. • *ip-address*—IPv4 or IPv6 address of a BGP neighbor. • **bfd**—Enables BFD protocol support for fallover.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Implementing QoS for IPv6

The QoS implementation for IPv6 environment in the Cisco ASR router is the same as that of IPv4. For configuration information on Configuring QoS on the Cisco ASR 901 router, refer the following link:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/qos.html

For additional information on Implementing QoS for IPv6, refer the following link: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-qos.html

Verifying the Configuration of IPv6 Support on the Cisco ASR 901 Router

This section describes how to use the **show** commands to verify the configuration and operation of the IPv6 Support feature on the Cisco ASR 901 router, and it contains the following topics:

Verifying IPv6 Addressing Routing

To verify the IPv6 Addressing Routing information, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying a Static IPv6 Route

To verify the static IPv6 route information, use the **show ipv6 route** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   22::/64 [0/0]
     via Vlan111, directly connected
L   22::22/128 [0/0]
     via Vlan111, receive
C   33::/64 [0/0]
     via Vlan111, directly connected
L   33::33/128 [0/0]
     via Vlan111, receive
I1  454::/96 [115/20]
     via FE80::4255:39FF:FE89:3F71, Vlan2020
```

Verifying a Stateless Auto-Configuration

To verify the autoconfigured IPv6 address and its state, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface loopback 0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Implementation on VLAN Interfaces

To verify the IPv6 implementation on VLAN interfaces, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface vlan40
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
```

```
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Implementation on Loopback Interfaces

To verify the IPv6 implementation on loopback interfaces, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface loopback0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying ICMPv6 Configuration

To verify the ICMPv6 configuration information, use the **show ipv6 interface** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
```

```
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

To verify the ICMPv6 statistics, use the **show ipv6 traffic** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 traffic
IPv6 statistics:
        Rcvd:  8 total, 0 local destination
               0 source-routed, 0 truncated
               0 format errors, 0 hop count exceeded
               0 bad header, 0 unknown option, 0 bad source
               0 unknown protocol, 0 not a router
               0 fragments, 0 total reassembled
               0 reassembly timeouts, 0 reassembly failures
        Sent:  870 generated, 0 forwarded
               0 fragmented into 0 fragments, 0 failed
               0 encapsulation failed, 0 no route, 0 too big
               0 RPF drops, 0 RPF suppressed drops
        Mcast: 8 received, 855 sent
ICMP statistics:
        Rcvd: 8 input, 0 checksum errors, 0 too short
              0 unknown info type, 0 unknown error type
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
                       0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 0 router advert, 0 redirects
              0 neighbor solicit, 0 neighbor advert
        Sent: 129 output, 0 rate-limited
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
```

```
                         0 sa policy, 0 reject route
              parameter: 0 error, 0 header, 0 option
              0 hopcount expired, 0 reassembly timeout,0 too big
              0 echo request, 0 echo reply
              0 group query, 0 group report, 0 group reduce
              0 router solicit, 50 router advert, 0 redirects
              8 neighbor solicit, 8 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Verifying IPv6 Duplicate Address Detection Configuration

To verify the IPv6 Duplicate Address Detection configuration information, use the **show running configuration** command or the **show ipv6 interface command** in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 interface
Vlan40 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    2011:8:8:3::4, subnet is 2011:8:8:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
```

```
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

Verifying IPv6 Neighbor Discovery Configuration

To verify the IPv6 neighbor discovery configuration, use the **show ipv6 neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 neighbors detail
IPv6 Address                              TRLV Age Link-layer Addr State Interface
2001:103::2                                 0    0 001e.4a97.05bb  REACH Vl103
2001:101::2                                 0    0 001e.4a97.05bb  REACH Vl101
2001:300::2                                 0   72 001e.4a97.05bb  STALE Vl300
2001:10::2                                  0    0 001e.4a97.05bb  REACH Vl10
FE80::200:1FF:FE97:41FE                     0   65 0000.0197.41fe  STALE Vl90
FE80::21E:4AFF:FE97:5BB                     0   25 001e.4a97.05bb  STALE Vl101
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  REACH Vl10
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  REACH Vl170
FE80::21E:4AFF:FE97:5BB                     0    0 001e.4a97.05bb  STALE Vl160
2001:170::2                                 0    0 001e.4a97.05bb  REACH Vl170
2001:180::2                                 0    0 001e.4a97.05bb  REACH Vl180
2001:190::2                                 0    0 001e.4a97.05bb  REACH Vl190
```

Verifying IPv6 and IPv4 Dual-Stack Configuration

To verify the IPv6 and IPv4 dual-stack configuration, use the **show ipv6 interface or show ip interface** commands in privileged EXEC mode, as shown in the examples.

```
Router# show ipv6 interface loopback0
Loopback0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::4255:39FF:FE89:4831
  No Virtual link-local address(es):
  Global unicast address(es):
    FE01:4::4, subnet is FE01:4::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FF00:4
    FF02::1:FF89:4831
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
Router# show ip interface
GigabitEthernet0/0 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/1 is administratively down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/2 is up, line protocol is up
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
```

```
GigabitEthernet0/3 is up, line protocol is up
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/4 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/5 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/6 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/7 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/8 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/9 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/10 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
GigabitEthernet0/11 is down, line protocol is down
  Inbound  access list is not set
  Outgoing access list is not set
  Internet protocol processing disabled
FastEthernet0/0 is administratively down, line protocol is down
  Internet protocol processing disabled
Vlan1 is down, line protocol is down
  Internet protocol processing disabled
Vlan40 is up, line protocol is up
  Internet protocol processing disabled
Loopback0 is up, line protocol is up
  Internet protocol processing disabled
```

Verifying OSPFv3 for IPv6 Configuration

To verify the OSPF for IPv6 configuration, use the **show ipv6 ospf** command in privileged EXEC mode, as shown in the example.

```
Router# show ipv6 ospf
 Routing Process "ospfv3 10" with ID 4.4.4.4
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
```

```
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
    Area 34
        Number of interfaces in this area is 2
        SPF algorithm executed 5 times
        Number of LSA 3. Checksum Sum 0x01F6C1
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Verifying IS-IS for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show isis ipv6 rib** command in privileged EXEC mode, as shown in the example.

```
Router# show isis ipv6 rib
IS-IS IPv6 process area2, local RIB
```

Verifying Multiprotocol-BGP for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show bgp ipv6** command in privileged EXEC mode, as shown in the examples.

```
Router# show bgp ipv6 unicast summary
BGP router identifier 9.9.9.9, local AS number 5500
BGP table version is 25, main routing table version 25
15 network entries using 2580 bytes of memory
53 path entries using 4664 bytes of memory
3/3 BGP path/bestpath attribute entries using 384 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7652 total bytes of memory
BGP activity 43/2 prefixes, 134/46 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:10::2      4         6500       0       0        1    0    0 00:22:30 Idle
2001:101::2     4         6500      87      84       25    0    0 01:09:28        8
2001:103::2     4         6500      84      83       25    0    0 01:09:34        8
2001:170::2     4         6500      88      82       25    0    0 01:09:33        8
2001:180::2     4         6500      87      84       25    0    0 01:09:29        8
2001:190::2     4         6500      89      83       25    0    0 01:09:34        8
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:300::2     4         6500       0       0        1    0    0 01:09:23 Idle
FE80::21E:4AFF:FE97:5BB%Vlan160
                4         6500      82      82       25    0    0 01:09:25        5
Router# show bgp ipv6 unicast neighbors 2001:101::2
BGP neighbor is 2001:101::2,  remote AS 6500, external link
 Fall over configured for session
 BFD is configured.  Using BFD to detect fast fallover
  BGP version 4, remote router ID 14.14.14.14
  BGP state = Established, up for 01:09:48
  Last read 00:00:10, last write 00:00:23, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
```

```
    Address family IPv6 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                8          9
    Keepalives:            75         76
    Route Refresh:          0          0
    Total:                 84         88
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  Session: 2001:101::2
  BGP table version 25, neighbor version 25/0
  Output queue size : 0
  Index 1, Advertise bit 0
  1 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:              15          8 (Consumes 704 bytes)
    Prefixes Total:                16         10
    Implicit Withdraw:              0          0
    Explicit Withdraw:              1          2
    Used as bestpath:             n/a          3
    Used as multipath:            n/a          0
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    AS_PATH loop:                       n/a          4
    Invalid Path:                         2        n/a
    Total:                                2          4
  Number of NLRIs in the update sent: max 7, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Refresh Epoch: 2
  Last Sent Refresh Start-of-rib: never
  Last Sent Refresh End-of-rib: never
  Last Received Refresh Start-of-rib: 01:09:48
  Last Received Refresh End-of-rib: 01:09:48
  Refresh-In took 0 seconds
                                       Sent       Rcvd
        Refresh activity:              ----       ----
          Refresh Start-of-RIB          0          1
          Refresh End-of-RIB            0          1
  Address tracking is disabled
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 1
Local host: 2001:101::1, Local port: 57438
Foreign host: 2001:101::2, Foreign port: 179
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x4853F8):
Timer          Starts    Wakeups            Next
Retrans            83          0             0x0
```

```
TimeWait            0          0             0x0
AckHold            83         81             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger        10940      10939        0x485427
DeadWait            0          0             0x0
Linger              0          0             0x0
iss:  338855921  snduna:  338858128  sndnxt:  338858128     sndwnd:  15636
irs:  816933509  rcvnxt:  816935775  rcvwnd:      15571  delrcvwnd:    813
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: none
Option Flags: higher precendence, nagle, path mtu capable
Datagrams (max data segment is 1440 bytes):
Rcvd: 163 (out of order: 0), with data: 86, total data bytes: 2265
Sent: 167 (retransmit: 0 fastretransmit: 0),with data: 167, total data bytes: 8894
```

Verifying BFD for IPv6 Configuration

To verify the IPv6 Addressing Routing information, use the **show bfd neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                               LD/RD         RH/RS     State     Int
101.101.101.2                            6/5          Up        Up        Vl101
103.103.103.2                            7/6          Up        Up        Vl103
150.150.150.2                            2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                               LD/RD         RH/RS     State     Int
2001:10::2                              16/14         Up        Up        Vl10
2001:101::2                             12/11         Up        Up        Vl101
2001:103::2                              3/2          Up        Up        Vl103
2001:170::2                              8/7          Up        Up        Vl170
2001:180::2                             11/10         Up        Up        Vl180
2001:190::2                              4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                 13/12         Up        Up        Vl160
CE1-2009#
```

Verifying BFDv6 and OSPFv3 Configuration

To verify the BFDv6 and OSPFv3 configuration, use the **show bfd neighbors or the show ipv6 ospf** command in privileged EXEC mode, as shown in the examples.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                               LD/RD         RH/RS     State     Int
101.101.101.2                            6/5          Up        Up        Vl101
103.103.103.2                            7/6          Up        Up        Vl103
150.150.150.2                            2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                               LD/RD         RH/RS     State     Int
2001:10::2                              16/14         Up        Up        Vl10
2001:101::2                             12/11         Up        Up        Vl101
2001:103::2                              3/2          Up        Up        Vl103
2001:170::2                              8/7          Up        Up        Vl170
2001:180::2                             11/10         Up        Up        Vl180
2001:190::2                              4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                 13/12         Up        Up        Vl160
Router# show ipv6 ospf
```

```
 Routing Process "ospfv3 10" with ID 4.4.4.4
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 RFC1583 compatibility enabled
    Area 34
        Number of interfaces in this area is 2
        SPF algorithm executed 11 times
        Number of LSA 3. Checksum Sum 0x01D6D1
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Verifying BFDv6 for BGP Configuration

To verify the BFDv6 for BGP configuration, use the **show bfd neighbors** command in privileged EXEC mode, as shown in the example.

```
Router# show bfd neighbors
IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
101.101.101.2                           6/5          Up        Up        Vl101
103.103.103.2                           7/6          Up        Up        Vl103
150.150.150.2                           2/1          Up        Up        Vl150
IPv6 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
2001:10::2                             16/14         Up        Up        Vl10
2001:101::2                            12/11         Up        Up        Vl101
2001:103::2                             3/2          Up        Up        Vl103
2001:170::2                             8/7          Up        Up        Vl170
2001:180::2                            11/10         Up        Up        Vl180
2001:190::2                             4/3          Up        Up        Vl190
FE80::21E:4AFF:FE97:5BB                13/12         Up        Up        Vl160
CE1-2009#
```

Configuration Examples for IPv6 Support on the Cisco ASR 901 Router

This section provides sample configuration examples for IPv6 Support on the Cisco ASR 901 router feature.

Example: IPv6 Addressing on VLAN Interfaces

The following is a sample configuration of IPv6 addressing on VLAN interfaces.

```
!
interface Vlan2020
 ip address 4.5.6.7 255.255.255.0
 ipv6 address FE80::3 link-local
 ipv6 address 3333::3335/64
 ipv6 address 4400::/64 anycast
 ipv6 address autoconfig
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

Example: IPv6 Addressing on Loopback Interfaces

The following is a sample configuration of IPv6 addressing on Loopback interfaces.

```
!
interface Loopback100
 ip address 170.0.0.201 255.255.255.0
!
interface Loopback555
 no ip address
 ipv6 address 22::22/64
 ipv6 address 555::554/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

Example: Customizing ICMPv6

The following is a sample configuration of customizing ICMPv6.

!

```
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
!
```

Example: Configuring IPv6 Duplicate Address Detection

The following is a sample configuration of IPv6 duplicate address detection.

!

```
  ND DAD is enabled, number of DAD attempts: 1
!Duplicate address detection information is given above.
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
!
```

Example: Configuring IPv6 Neighborhood Discovery

The following is a sample configuration of IPv6 neighborhood discovery.

```
!
interface Vlan111
 no ip address
 ipv6 address 22::22/64
 ipv6 address 33::33/64
ipv6 address autoconfig
ipv6 nd autoconfig prefix
!Neighborhood discovery information is given above.
 ipv6 enable
```

Example: Enabling IPv6 Stateless Address Autoconfiguration

The following is a sample configuration of IPv6 stateless address autoconfiguration.

```
!
interface Vlan111
 no ip address
 ipv6 address 22::22/64
 ipv6 address 33::33/64
ipv6 address autoconfig
!IPv6 address autoconfiguration details are given above.
ipv6 nd autoconfig prefix
 ipv6 enable
!
```

Example: Configuring the IPv4 and IPv6 Dual-Stack

The following is a sample configuration of IPv4 and IPv6 dual-stack.

```
!
interface Vlan222
 ip address 22.22.22.22 255.255.255.0
 ipv6 address 99::99/64
!IPv4 and IPv6 dual-stack information is given above.
 ipv6 enable
!
```

Example: Configuring IPv6 Static Routing

The following is a sample configuration of IPv6 static routing between two Cisco ASR 901 routers.

Router-1

```
ipv6 route 555::/64 Vlan2020
```

Router-2

```
interface Loopback555
 no ip address
```

```
 ipv6 address 22::22/64
 ipv6 address 555::554/64
 ipv6 enable
 ipv6 ospf 1 area 0
```

Example: Configuring BFD and Static Routing for IPv6

The following is a sample configuration of bidirectional forwarding detection and static routing for IPv6.

```
!
ipv6 route static bfd vlan 4000 2001::1
ipv6 route 2001:DB8::/64 vlan 4000 2001::1
interface vlan 4000
ipv6 add 2001::2/64
bfd interval 50 min_rx 50 multiplier 3
```

Example: Configuring OSPFv3 for IPv6

The following is a sample configuration of OSPFv3 for IPv6.

Router-1

```
!
interface Loopback20202
 no ip address
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
 ipv6 router ospf 1
 router-id 1.1.1.1
 area 0 range 4444::/48
!
```

Router-2

```
!
interface Loopback30303
 no ip address
 ipv6 address 4444::4443/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
 ipv6 router ospf 1
 router-id 3.3.3.3
 area 0 range 4444::/48
!
```

Example: Configuring BFD and OSPFv3 for IPv6

The following is a sample configuration of bidirectional forwarding detection support for OSPFv3 on one or more OSPFv3 Interfaces:

```
!
!
```

```
ipv6 router ospf 1
router-id 1.1.1.1
interface vlan 4000
ipv6 add 2001::2/64
ipv6 ospf 1 area 0
 ipv6 ospf bfd
bfd interval 50 min_rx 50 multiplier 3
!
```

The following is a sample configuration of bidirectional forwarding detection support for OSPFv3 on all interfaces:

```
ipv6 router ospf 1
router-id 1.1.1.1
bfd all-interfaces
interface vlan 4000
ipv6 add 2001::2/64
ipv6 ospf 1 area 0
bfd interval 50 min_rx 50 multiplier 3
```

Example: Configuring IS-IS for IPv6

The following is a sample configuration of IS-IS for IPv6.

Router-1

```
!
interface Loopback20202
 no ip address
 ipv6 address 565::565/96
 ipv6 address 4444::4444/64
 ipv6 enable
 ipv6 router isis alpha
 !
router isis alpha
 net 49.1111.2222.3333.4444.00
!
```

Router-2

```
!
interface Loopback30303
 no ip address
 ipv6 address 454::454/96
 ipv6 address 4444::4443/64
 ipv6 enable
 ipv6 router isis alpha
!
router isis alpha
 net 49.1111.2220.3330.4440.00
!
```

Example: Configuring Multiprotocol-BGP for IPv6

The following is a sample configuration of multiprotocol-BGP for IPv6.

Router-1

```
--------
ipv6 unicast-routing
!Enables forwarding of IPv6 packets.
ipv6 cef
interface Loopback10
 no ip address
 ipv6 address 2010:AB8:2::/48
 ipv6 enable
!
interface Loopback20
 no ip address
 ipv6 address 2010:AB8:3::/48
 ipv6 enable
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:AB8:0:2::/64 eui-64
 ipv6 enable
!
router bgp 1
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
!Without configuring “no bgp default ipv4-unicast” only IPv4 will be advertised.
 bgp log-neighbor-changes
 neighbor 2010:AB8:0:2:C601:10FF:FE58:0 remote-as 2
 !
 address-family ipv6
  neighbor 2010:AB8:0:2:C601:10FF:FE58:0 activate
  network 2010:AB8:2::/48
  network 2010:AB8:3::/48
 exit-address-family
!
```

Router-2

```
ipv6 unicast-routing
ipv6 cef
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:AB8:0:2::/64 eui-64
 ipv6 enable
!
router bgp 2
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2010:AB8:0:2:C600:10FF:FE58:0 remote-as 1
 !
 address-family ipv6
  neighbor 2010:AB8:0:2:C600:10FF:FE58:0 activate
 exit-address-family
!i
```

Example: Configuring BFD and Multiprotocol-BGP for IPv6

The following is a sample configuration of bidirectional forwarding detection and multiprotocol-BGP for IPv6.

Router-1

```
interface Vlan10
ipv6 address 2001:10::1/64
bfd interval 250 min_rx 250 multiplier 3
router bgp 5500
bgp router-id 9.9.9.9
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:10::2 remote-as 6500
neighbor 2001:10::2 fall-over bfd
address-family ipv6
redistribute connected
neighbor 2001:10::2 activate
exit-address-family
```

Router-2

```
interface Vlan10
ipv6 address 2001:10::2/64
bfd interval 250 min_rx 250 multiplier 3
router bgp 6500
bgp router-id 10.10.10.10
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2001:10::1 remote-as 5500
neighbor 2001:10::1 fall-over bfd
address-family ipv6
redistribute connected
neighbor 2001:10::1 activate
exit-address-family
```

Troubleshooting Tips

Problems can occur in the IPv6 functionality due to misconfigurations. To enable IPv6 functionality, you should enable IPv6 configurations at several places.

Some of the sample troubleshooting scenarios are provided below:

Problem	Solution
IPv6 commands are not available.	IPv6 is not enabled by default. Enable IPv6 functionality using **ipv6 unicast-routing** command. Also, check to see if IPv6 is enabled on the virtual templates.
No route advertisement is sent to the MN when the IPv6 CP comes up.	The route advertisement is disabled on the virtual-templates. Configure the **no ipv6 nd suppress-ra** command to enable route advertisement messages. Also, define a valid prefix pool for IPv6.

The following **debug** and **show** commands allows you to troubleshoot the IPv6 configuration.

Debug Commands	Show Commands	Platform Hardware Commands
debug ipv6	**show ipv6**	**debug platform hardware cef adjacency**
debug ipv6 address	**show ipv6 interface**	**debug platform hardware cef backwalk**
debug ipv6 icmp	**show ipv6 interface brief**	**debug platform hardware cef deaggregate**
debug ipv6 interface	**show ipv6 route**	**debug platform hardware cef entry**
debug ipv6 nd	—	**debug platform hardware cef interface**
debug ipv6 packet	—	**debug platform hardware cef loadbalance**
debug ipv6 pool	—	**debug platform hardware cef special**
debug ipv6 routing	—	**debug platform hardware cef table**
—	—	**debug platform hardware ether idb**

Where to Go Next

For additional information on IPv6 Support on the Cisco ASR 901 router, see the documentation listed in the Additional References section.

Additional References

The following sections provide references related to LLDP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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

Feature Information for IPv6 Support on the Cisco ASR 901 Router

Table 36: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 601 lists the release history for this feature.

Table 36: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 601 lists the features in this module and provides links to specific configuration information.

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 Table 36: Feature Information for IPv6 Support on the Cisco ASR 901 Router , on page 601 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 36: Feature Information for IPv6 Support on the Cisco ASR 901 Router

Feature Name	Releases	Feature Information
IPv6 Support on the Cisco ASR 901 Router	15.2(2)SNG	This feature is introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
ICMPv6	15.2(2)SNG	The ICMP is used to generate error messages. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • ICMP for IPv6
IPv6 Neighbor Discovery	15.2(2)SNG	The IPv6 neighbor discovery determines the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • IPv6 Neighbor Discovery • IPv6 Duplicate Address Detection
IPv4 and IPv6 Dual-Stack	15.2(2)SNG	The dual IPv4 and IPv6 protocol stack technique is used to transition to IPv6. It enables gradual, one-by-one upgrades to applications running on nodes. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Dual IPv4 and IPv6 Protocol Stacks
RIP for IPv6	15.2(2)SNG	The IPv6 RIP Routing Information Database (RIB) contains a set of best-cost IPv6 RIP routes learned from all its neighboring networking devices. The RIB also stores any expired routes that the RIP process is advertising to its neighbors running RIP. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing RIP for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • RIP for IPv6

Feature Name	Releases	Feature Information
IS-IS for IPv6	15.2(2)SNG	The IPv6 RIP Routing Information Database (RIB) contains a set of best-cost IPv6 RIP routes learned from all its neighboring networking devices. The RIB also stores any expired routes that the RIP process is advertising to its neighbors running RIP. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IS-IS for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • IS-IS for IPv6
OSPFv3 for IPv6	15.2(2)SNG	OSPF is a link-state protocol. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing OSPFv3 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Information about OSPFv3
Multiprotocol BGP Extensions for IPv6	15.2(2)SNG	Multiprotocol BGP is the supported exterior gateway protocol (EGP) for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing Multiprotocol BGP for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Multiprotocol BGP Extensions for IPv6
Bidirectional Forwarding Detection for IPv6	15.2(2)SNG	BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing Bidirectional Forwarding Detection for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Implementing Bidirectional Forwarding Detection for IPv6

Feature Name	Releases	Feature Information
Implementing QoS for IPv6	15.2(2)SNG	QoS features for IPv6 include packet classification, policing, marking on ingress path of Ethernet interfaces and packet classification, policing, marking, scheduling, per interface and per qos-group shaping, LLQ, and WRED on egress path of GigabitEthernet interfaces. **Platform-dependent Cisco IOS Software Documentation** The " Configuring QoS " section of the Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide provide information about this feature: • Configuring QoS **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing QoS for IPv6 " chapter of the *IPv6 Configuration Guide* provide information about this feature: • Implementing QoS for IPv6

CHAPTER 33

Labeled BGP Support

This feature module describes how to add label mapping information to the Border Gateway Protocol (BGP) message that is used to distribute the route on the Cisco ASR 901 Series Aggregation Services Routers.

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 table at the end of this module.

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 Labeled BGP Support

- Cisco IOS Release 15.2(2)SNG or a later release that supports Labeled BGP must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.

Restrictions for Labeled BGP Support

- The Cisco ASR 901 router supports only the client functionality of RFC 3107 and not its area border router (ABR) functionality.

- The Cisco ASR 901 router does not support two label-pop (Label pop is the process of removing label header).
- Four label push is not supported. Due to this limitation, Labeled BGP access (RFC 3107) with Remote LFA-FRR/TE-FRR is not supported, if it exceeds three labels.

Overview of Labeled BGP Support

The Labeled BGP Support feature provides the option to use the BGP update message (that is used to distribute the route) to re-distribute Multiprotocol Label Switching (MPLS) label mapped to that route. The label mapping information is added (using send-label option of RFC 3107) to the same BGP message that is used to distribute the route. This process is useful in inter-domain routing, and the Cisco ASR 901 router supports this functionality as well as the virtual private network (VPN) and virtual routing and forwarding (VRF) over Labeled BGP functionality.

VPN/VRF over RFC 3107

The VPN/VRF over Labeled BGP is a 3-label imposition process (VRF Label, BGP label, interior gateway protocols [IGP] label). The innermost label is VRF, followed by BGP (for RFC 3107), and IGP. This functionality allows the Cisco ASR 901 router to support a VRF over labeled BGP session with an ABR.

How to Configure Labeled BGP Support

Note The TDM over Labeled BGP feature is supported effective with Cisco IOS Release 15.3(3)S. The configuration and restrictions for this feature are the same as that of Labeled BGP Support.

To configure Labeled BGP Support feature on the Cisco ASR 901 router, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**router bgp** *peer-group-name* **Example:**	Enters router configuration mode. • *peer-group-name*—Number of an autonomous system that identifies the

	Command or Action	Purpose
	`Router(config)# router bgp 100`	router to other BGP routers and tags the routing information that is passed along. The valid values range from 1 to 65535.
Step 4	**address family ipv4** **Example:** `Router(config-router)# address family ipv4`	Configures the address family as IPv4 using standard IPv4 address prefixes.
Step 5	**neighbor** *peer-group-name* **send-community** **Example:** `Router(config-router)# neighbor 172.16.70.23 send-community`	Specifies that the communities attribute be sent to the neighbor at this IP address. • *peer-group-name*—Name of a BGP peer group.
Step 6	**neighbor***peer-group-name peer-group-name* **Example:** `Router(config-router)# neighbor 172.16.70.23 send-label`	Configures the router to associate a BGP label to the prefix using the **neighbor***peer-group-name***activate** option.
Step 7	**neighbor***peer-group-name***activate** **Example:** `Router(config-router)# neighbor 172.16.70.23 activate`	Enables the exchange of information with a neighboring BGP router.

Configuration Example for Labeled Support

The following is a sample configuration of the Labeled BGP Support feature.

```
!
router bgp 1000
 bgp router-id 100.111.13.23
 neighbor pan peer-group
 neighbor pan remote-as 1000
 neighbor pan update-source Loopback0
 neighbor 100.111.14.3 peer-group pan
 !
 address-family ipv4
  neighbor pan send-community
  neighbor pan send-label
!The "send-label" option is used to associate a BGP label to the prefix.
  neighbor 100.111.14.3 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor pan send-community extended
  neighbor 100.111.14.3 activate
 exit-address-family
 !
```

```
 address-family ipv4 vrf LTE12
  redistribute connected
 exit-address-family
!
```

Verifying Labeled BGP Support

To verify the Labeled BGP Support on the Cisco ASR 901 router, use the **show** commands given below:

Router# show bgp ipv4 unicast labels

```
  Network          Next Hop      In label/Out label
  1.0.0.0          0.0.0.0         imp-null/nolabel
  10.13.22.2/31    0.0.0.0         imp-null/nolabel
  10.13.23.0/31    0.0.0.0         imp-null/nolabel
  10.70.1.0/30     0.0.0.0         imp-null/nolabel
  100.100.10.1/32  100.111.14.4    nolabel/558
                   100.111.14.3    nolabel/560
  100.100.13.23/32 0.0.0.0         imp-null/nolabel
  100.101.13.23/32 0.0.0.0         imp-null/nolabel
  100.111.13.23/32 0.0.0.0         imp-null/nolabel
  100.111.13.26/32 100.111.14.3    nolabel/534
                   100.111.14.4    nolabel/68
  100.111.15.1/32  100.111.14.3    nolabel/25
Router# show ip bgp labels
   Network          Next Hop      In label/Out label
   1.0.0.0          0.0.0.0         imp-null/nolabel
   10.13.22.2/31    0.0.0.0         imp-null/nolabel
   10.13.23.0/31    0.0.0.0         imp-null/nolabel
   10.70.1.0/30     0.0.0.0         imp-null/nolabel
   100.100.10.1/32  100.111.14.4    nolabel/563
                    100.111.14.3    nolabel/556
   100.100.13.23/32 0.0.0.0         imp-null/nolabel
   100.101.13.23/32 0.0.0.0         imp-null/nolabel
   100.111.13.23/32 0.0.0.0         imp-null/nolabel
   100.111.13.26/32 100.111.14.4    nolabel/561
                    100.111.14.3    nolabel/559
   100.111.15.1/32  100.111.14.4    nolabel/59
                    100.111.14.3    nolabel/57
   100.111.15.2/32  100.111.14.4    nolabel/62
                    100.111.14.3    nolabel/52
   100.112.1.1/32   100.111.14.4    nolabel/nolabel
                    100.111.14.3    nolabel/nolabel
   100.112.1.2/32   100.111.14.4    nolabel/nolabel
                    100.111.14.3    nolabel/nolabel
   100.112.1.3/32   100.111.14.4    nolabel/nolabel
                    100.111.14.3    nolabel/nolabel
Router# show ip bgp vpnv4 all label
   Network          Next Hop      In label/Out label
Route Distinguisher: 236:236
   154.154.236.4/30 100.154.1.1     nolabel/14002
                    100.154.1.1     nolabel/14002
   154.154.236.8/30 100.154.1.1     nolabel/14002
                    100.154.1.1     nolabel/14002
   154.154.236.12/30
                    100.154.1.1     nolabel/14002
                    100.154.1.1     nolabel/14002
   154.154.236.16/30
                    100.154.1.1     nolabel/14002
                    100.154.1.1     nolabel/14002
   154.154.236.20/30
                    100.154.1.1     nolabel/14002
```

```
                    100.154.1.1     nolabel/14002
   154.154.236.24/30
                    100.154.1.1     nolabel/14002
                    100.154.1.1     nolabel/14002
Router# show ip vrf interface
Interface              IP-Address      VRF                              Protocol
Vl100                  113.23.12.1     LTE12
Router# show ip bgp vpnv4 vrf LTE12 label
   Network          Next Hop      In label/Out label
Route Distinguisher: 6666:6666 (LTE12)
   113.22.12.0/24   100.111.13.22   nolabel/51
                    100.111.13.22   nolabel/51
   113.23.12.0/24   0.0.0.0         50/nolabel(LTE12)
   113.24.12.0/24   100.111.13.24   nolabel/32
                    100.111.13.24   nolabel/32
   115.1.12.0/24    100.111.15.1    nolabel/16024
                    100.111.15.1    nolabel/16024
   154.154.236.4/30 100.154.1.1     nolabel/14002
   154.154.236.8/30 100.154.1.1     nolabel/14002
   154.154.236.12/30
                    100.154.1.1     nolabel/14002
   154.154.236.16/30
                    100.154.1.1     nolabel/14002
   154.154.236.20/30
                    100.154.1.1     nolabel/14002
   154.154.236.24/30
                    100.154.1.1     nolabel/14002
```

To verify three Label Support, use the **show ip cef vrf** command as shown in the following example.

```
Router# show ip cef vrf LTE12 113.22.12.0 internal
113.22.12.0/24, epoch 0, flags rib defined all labels, RIB[B], refcount 5, per-destination
 sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   LFD: 113.22.12.0/24  0 local labels
        contains path extension list
  ifnums: (none)
  path 13E8A064, path list 13F49DC8, share 1/1, type recursive, for IPv4, flags
must-be-labelled, recursive-via-host
    MPLS short path extensions: MOI flags = 0x0 label 51
  recursive via 100.111.13.22[IPv4:Default] label 51, fib 141253D8, 1 terminal fib,
v4:Default:100.111.13.22/32
    path 12520C8C, path list 13F49C38, share 1/1, type attached nexthop, for IPv4
   MPLS short path extensions: MOI flags = 0x0 label 17
      nexthop 100.111.14.4 Vlan10 label 17, adjacency IP adj out of Vlan10, addr 10.13.23.1
 13734C80
  output chain: label 22 label 51 label 17 TAG adj out of Vlan10, addr 10.13.23.1 143EDCA0
!You can see three labels in the output chain; of which 22 is VRF label, 51 is BGP label
!and 17 is LDP label
```

Additional References

The following sections provide references related to Labeled BGP Support feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
BGP Commands	Cisco IOS IP Routing: BGP Command Reference
Configuring BGP	Cisco IOS IP Configuration Guide, Release 12.2

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC-3107	*Carrying Label Information in BGP-4*

Technical Assistance

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

Feature Information for Labeled BGP Support

Table 37: Feature Information for Labeled BGP Support, on page 611 lists the features in this module and provides links to specific configuration information.

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 Table 37: Feature Information for Labeled BGP Support, on page 611 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 37: Feature Information for Labeled BGP Support

Feature Name	Releases	Feature Information
Labeled BGP Support	15.2(2)SNG	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
TDM over Labeled BGP	15.3(3)S	Support for TDM over Labeled BGP was introduced on the Cisco ASR 901 routers.

CHAPTER 34

BGP Support for Next-Hop Address Tracking

The BGP Support for Next-Hop Address Tracking feature is enabled by default when a supporting Cisco software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a bestpath calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About BGP Support for Next-Hop Address Tracking

BGP Next-Hop Address Tracking

The BGP next-hop address tracking feature is enabled by default when a supporting Cisco software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a best-path calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.

BGP Next-Hop Dampening Penalties

The BGP next-hop address tracking feature monitors the BGP next-hop routes and adds a global penalty whenever there are route updates such as, addition, deletion, or modification in the next-hop route for a given next-hop address. The global penalty increases by 500 during any route update. If the penalty value is lower than the penalty threshold, which is 950, then the next-hop scan is performed after a configurable delay (the BGP next-hop trigger delay) since the BGP next-hop route update has occurred.

If the penalty threshold value is higher than 950, then the delay is calculated as the reuse time using the dampening calculations. The dampening calculations use the following parameters:

- Penalty
- Half-life time
- Reuse time
- max-suppress-time

The values for the dampening parameters used are a max-suppress-time of 60 seconds, the half-life of 8 seconds, and the reuse-limit of 100.

For example, if the original penalty of 1600 is added, then after 16 seconds it becomes 800, and after 40 seconds, the penalty becomes 100. Hence, for the route update penalty of 1600, a delay of 40 seconds is used to schedule the BGP scanner.

These parameters (penalty threshold and any of the dampening parameters) cannot be modified.

Default BGP Scanner Behavior

BGP monitors the next hop of installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner is used to poll the RIB for this information every 60 seconds. During the 60 second time period between scan cycles, Interior Gateway Protocol (IGP) instability or other network failures can cause null routes and routing loops to temporarily form.

BGP Next_Hop Attribute

The Next_Hop attribute identifies the next-hop IP address to be used as the BGP next hop to the destination. The device makes a recursive lookup to find the BGP next hop in the routing table. In external BGP (eBGP), the next hop is the IP address of the peer that sent the update. Internal BGP (iBGP) sets the next-hop address to the IP address of the peer that advertised the prefix for routes that originate internally. When any routes to iBGP that are learned from eBGP are advertised, the Next_Hop attribute is unchanged.

A BGP next-hop IP address must be reachable in order for the device to use a BGP route. Reachability information is usually provided by the IGP, and changes in the IGP can influence the forwarding of the next-hop address over a network backbone.

Selective BGP Next-Hop Route Filtering

BGP selective next-hop route filtering was implemented as part of the BGP Selective Address Tracking feature to support BGP next-hop address tracking. Selective next-hop route filtering uses a route map to selectively define routes to help resolve the BGP next hop.

The ability to use a route map with the **bgp nexthop** command allows the configuration of the length of a prefix that applies to the BGP Next_Hop attribute. The route map is used during the BGP bestpath calculation and is applied to the route in the routing table that covers the next-hop attribute for BGP prefixes. If the next-hop route fails the route map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

Note Use route map on ASR series devices to set the next hop as BGP peer for the route and apply that route map in outbound direction towards the peer.

Note Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

BGP Support for Fast Peering Session Deactivation

BGP Hold Timer

By default, the BGP hold timer is set to run every 180 seconds in Cisco software. This timer value is set as the default to protect the BGP routing process from instability that can be caused by peering sessions with other routing protocols. BGP devices typically carry large routing tables, so frequent session resets are not desirable.

BGP Fast Peering Session Deactivation

BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. This feature is event driven and configured on a per-neighbor basis. When this feature is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

Selective Address Tracking for BGP Fast Session Deactivation

In Cisco IOS XE Release 2.1 and later releases, the BGP Selective Address Tracking feature introduced the use of a route map with BGP fast session deactivation. The **route-map** keyword and *map-name* argument are used with the **neighbor fall-over** BGP neighbor session command to determine if a peering session with a BGP neighbor should be reset when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset. The route map is not used for session establishment.

Note Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

How to Configure BGP Support for Next-Hop Address Tracking

Configuring BGP Next-Hop Address Tracking

The tasks in this section show how configure BGP next-hop address tracking. BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP. For more details about configuring route dampening, see “Configuring BGP Route Dampening.”

Configuring BGP Selective Next-Hop Route Filtering

Perform this task to configure selective next-hop route filtering using a route map to filter potential next-hop routes. This task uses prefix lists and route maps to match IP addresses or source protocols and can be used to avoid aggregate addresses and BGP prefixes being considered as next-hop routes. Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

For more examples of how to use the **bgp nexthop** command, see the “Examples: Configuring BGP Selective Next-Hop Route Filtering” section in this module.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 45000`	Enters router configuration mode and creates a BGP routing process.
Step 4	**address-family ipv4** [**unicast** | **multicast**] **Example:** `Device(config-router)# address-family ipv4 unicast`	Specifies the IPv4 address family and enters address family configuration mode. • The **unicast** keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the **unicast** keyword is

	Command or Action	Purpose
		not specified with the **address-family ipv4** command. • The **multicast** keyword specifies IPv4 multicast address prefixes.
Step 5	**bgp nexthop route-map** *map-name* **Example:** `Device(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP`	Permits a route map to selectively define routes to help resolve the BGP next hop. • In this example the route map named CHECK-NEXTHOP is created.
Step 6	**exit** **Example:** `Device(config-router-af)# exit`	Exits address family configuration mode and enters router configuration mode.
Step 7	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 8	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] **Example:** `Device(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25`	Creates a prefix list for BGP next-hop route filtering. • Selective next-hop route filtering supports prefix length matching or source protocol matching on a per address-family basis. • The example creates a prefix list named FILTER25 that permits routes only if the mask length is more than 25; this will avoid aggregate routes being considered as the next-hop route.
Step 9	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map CHECK-NEXTHOP deny 10`	Configures a route map and enters route map configuration mode. • In this example, a route map named CHECK-NEXTHOP is created. If there is an IP address match in the following **match** command, the IP address will be denied.
Step 10	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] **Example:** `Device(config-route-map)# match ip address prefix-list FILTER25`	Matches the IP addresses in the specified prefix list. • Use the *prefix-list-name* argument to specify the name of a prefix list. The ellipsis means that more than one prefix list can be specified.

	Command or Action	Purpose
		Note Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.
Step 11	**exit** **Example:** `Device(config-route-map)# exit`	Exits route map configuration mode and enters global configuration mode.
Step 12	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map CHECK-NEXTHOP permit 20`	Configures a route map and enters route map configuration mode. • In this example, all other IP addresses are permitted by route map CHECK-NEXTHOP.
Step 13	**end** **Example:** `Device(config-route-map)# end`	Exits route map configuration mode and enters privileged EXEC mode.
Step 14	**show ip bgp** [*network*] [*network-mask*] **Example:** `Device# show ip bgp`	Displays the entries in the BGP routing table. • Enter this command to view the next-hop addresses for each route. **Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.

Example

The following example from the **show ip bgp** command shows the next-hop addresses for each route:

```
BGP table version is 7, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.1.0/24      192.168.1.2              0             0 40000 i
*  10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
*> 172.17.1.0/24    0.0.0.0                  0         32768
```

Adjusting the Delay Interval for BGP Next-Hop Address Tracking

Perform this task to adjust the delay interval between routing table walks for BGP next-hop address tracking.

You can increase the performance of this feature by tuning the delay interval between full routing table walks to match the tuning parameters for the Interior Gateway protocol (IGP). The default delay interval is 5 seconds. This value is optimal for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 64512`	Enters router configuration mode to create or configure a BGP routing process.
Step 4	**address-family ipv4** [[**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]] **Example:** `Device(config-router)# address-family ipv4 unicast`	Enter address family configuration mode to configure BGP peers to accept address family-specific configurations. • The example creates an IPv4 unicast address family session.
Step 5	**bgp nexthop trigger delay** *delay-timer* **Example:** `Device(config-router-af)# bgp nexthop trigger delay 20`	Configures the delay interval between routing table walks for next-hop address tracking. • The time period determines how long BGP will wait before starting a full routing table walk after notification is received. • The value for the *delay-timer* argument is a number from 1 to 100 seconds. The default value is 5 seconds.

	Command or Action	Purpose
		• The example configures a delay interval of 20 seconds.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address-family configuration mode, and enters privileged EXEC mode.

Disabling BGP Next-Hop Address Tracking

Perform this task to disable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default under the IPv4 and VPNv4 address families. Beginning with Cisco IOS Release 12.2(33)SB6, BGP next-hop address tracking is also enabled by default under the VPNv6 address family whenever the next hop is an IPv4 address mapped to an IPv6 next-hop address.

Disabling next hop address tracking may be useful if you the network has unstable IGP peers and route dampening is not resolving the stability issues. To reenable BGP next-hop address tracking, use the **bgp nexthop**command with the **trigger** and **enable** keywords.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 64512`	Enters router configuration mod to create or configure a BGP routing process.
Step 4	**address-family ipv4** [[**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**] | **vpnv6** [**unicast**]] **Example:** `Device(config-router)# address-family ipv4 unicast`	Enter address family configuration mode to configure BGP peers to accept address family-specific configurations. • The example creates an IPv4 unicast address family session.
Step 5	**no bgp nexthop trigger enable** **Example:**	Disables BGP next-hop address tracking.

	Command or Action	Purpose
	`Device(config-router-af)# no bgp nexthop trigger enable`	• Next-hop address tracking is enabled by default for IPv4 and VPNv4 address family sessions. • The example disables next-hop address tracking.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address-family configuration mode, and enters Privileged EXEC mode.

Configuring Fast Session Deactivation

The tasks in this section show how to configure BGP next-hop address tracking. BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP. For more details about route dampening, see the "Configuring Internal BGP Features" module.

Configuring Fast Session Deactivation for a BGP Neighbor

Perform this task to establish a peering session with a BGP neighbor and then configure the peering session for fast session deactivation to improve the network convergence time if the peering session is deactivated.

Enabling fast session deactivation for a BGP neighbor can significantly improve BGP convergence time. However, unstable IGP peers can still introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 50000`	Enters router configuration mode to create or configure a BGP routing process.

	Command or Action	Purpose
Step 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv4 unicast`	Enters address family configuration mode to configure BGP peers to accept address family-specific configurations. • The example creates an IPv4 unicast address family session.
Step 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **Example:** `Device(config-router-af)# neighbor 10.0.0.1 remote-as 50000`	Establishes a peering session with a BGP neighbor.
Step 6	**neighbor** *ip-address* **fall-over** **Example:** `Device(config-router-af)# neighbor 10.0.0.1 fall-over`	Configures the BGP peering to use fast session deactivation. • BGP will remove all routes learned through this peer if the session is deactivated.
Step 7	**end** **Example:** `Device(config-router-af)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring Selective Address Tracking for Fast Session Deactivation

Perform this task to configure selective address tracking for fast session deactivation. The optional **route-map** keyword and *map-name* argument of the **neighbor fall-over** command are used to determine if a peering session with a BGP neighbor should be deactivated (reset) when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset.

> **Note** Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 45000`	Enters router configuration mode for the specified routing process.
Step 4	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* **Example:** `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 5	**neighbor** *ip-address* **fall-over** [**route-map** *map-name*] **Example:** `Device(config-router)# neighbor 192.168.1.2 fall-over route-map CHECK-NBR`	Applies a route map when a route to the BGP changes. • In this example, the route map named CHECK-NBR is applied when the route to neighbor 192.168.1.2 changes.
Step 6	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 7	**ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network* / *length* | **permit** *network* / *length*}[**ge** *ge-value*] [**le** *le-value*] **Example:** `Device(config)# ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28`	Creates a prefix list for BGP next-hop route filtering. • Selective next-hop route filtering supports prefix length matching or source protocol matching on a per-address-family basis. • The example creates a prefix list named FILTER28 that permits routes only if the mask length is greater than or equal to 28.
Step 8	**route-map** *map-name* [**permit** | **deny**][*sequence-number*] **Example:** `Device(config)# route-map CHECK-NBR permit 10`	Configures a route map and enters route-map configuration mode. • In this example, a route map named CHECK-NBR is created. If there is an IP address match in the following **match** command, the IP address will be permitted.

	Command or Action	Purpose
Step 9	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] **Example:** `Device(config-route-map)# match ip address prefix-list FILTER28`	Matches the IP addresses in the specified prefix list. • Use the *prefix-list-name* argument to specify the name of a prefix list. The ellipsis means that more than one prefix list can be specified. **Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.
Step 10	**end** **Example:** `Device(config-route-map)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for BGP Support for Next-Hop Address Tracking

Example: Enabling and Disabling BGP Next-Hop Address Tracking

In the following example, next-hop address tracking is disabled under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
 no bgp nexthop trigger enable
```

Example: Adjusting the Delay Interval for BGP Next-Hop Address Tracking

In the following example, the delay interval for next-hop tracking is configured to occur every 20 seconds under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
 bgp nexthop trigger delay 20
```

Examples: Configuring BGP Selective Next-Hop Route Filtering

The following example shows how to configure BGP selective next-hop route filtering to avoid using a BGP prefix as the next-hop route. If the most specific route that covers the next hop is a BGP route, then the BGP route will be marked as unreachable. The next hop must be an IGP or static route.

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP
 exit
 exit
route-map CHECK-BGP deny 10
 match source-protocol bgp 1
 exit
route-map CHECK-BGP permit 20
 end
```

The following example shows how to configure BGP selective next-hop route filtering to avoid using a BGP prefix as the next-hop route and to ensure that the prefix is more specific than /25.

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP25
 exit
 exit
ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25
route-map CHECK-BGP25 deny 10
 match ip address prefix-list FILTER25
 exit
route-map CHECK-BGP25 deny 20
 match source-protocol bgp 1
 exit
route-map CHECK-BGP25 permit 30
 end
```

Example: Configuring Fast Session Deactivation for a BGP Neighbor

In the following example, the BGP routing process is configured on device A and device B to monitor and use fast peering session deactivation for the neighbor session between the two devices. Although fast peering session deactivation is not required at both devices in the neighbor session, it will help the BGP networks in both autonomous systems to converge faster if the neighbor session is deactivated.

Device A

```
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 fall-over
 end
```

Device B

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

Example: Configuring Selective Address Tracking for Fast Session Deactivation

The following example shows how to configure the BGP peering session to be reset if a route with a prefix of /28 or a more specific route to a peer destination is no longer available:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
BGP commands	Cisco IOS IP Routing: BGP Command Reference

Technical Assistance

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

Feature Information for BGP Support for Next-Hop Address Tracking

Table 38: Feature Information for BGP Support for Next-Hop Address Tracking

Feature Name	Releases	Feature Information
BGP Support for Next-Hop Address Tracking		The BGP Support for Next-Hop Address Tracking feature is enabled by default when a supporting Cisco IOS software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a bestpath calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed. The following command was introduced in this feature: **bgp nexthop**.
BGP Selective Address Tracking		The BGP Selective Address Tracking feature introduces the use of a route map for next-hop route filtering and fast session deactivation. Selective next-hop filtering uses a route map to selectively define routes to help resolve the BGP next hop, or a route map can be used to determine if a peering session with a BGP neighbor should be reset when a route to the BGP peer changes. The following commands were modified by this feature: **bgp nexthop**, **neighbor fall-over**.

Feature Name	Releases	Feature Information
BGP Support for Fast Peering Session Deactivation		The BGP Support for Fast Peering Session Deactivation feature introduced an event-driven notification system that allows a Border Gateway Protocol (BGP) process to monitor BGP peering sessions on a per-neighbor basis. This feature improves the response time of BGP to adjacency changes by allowing BGP to detect an adjacency change and deactivate the terminated session in between standard BGP scanning intervals. Enabling this feature improves overall BGP convergence. The following command was modified by this feature: **neighbor fall-over**.

CHAPTER 35

MPLS Traffic Engineering - Fast Reroute Link Protection

This feature module describes the Fast Reroute (FRR) link protection and Bidirectional Forwarding Detection (BFD)-triggered FRR feature of Multiprotocol Label Switching (MPLS) traffic engineering (TE).

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 table at the end of this module.

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 MPLS Traffic Engineering - Fast Reroute Link Protection

- Cisco IOS Release 15.2(2)SNG or a later release that supports the MPLS TE-FRR link protection feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You should enable the asr901-platf-frr command at the global configuration before using TE-FRR.

- Your network must support both the following Cisco IOS features before you can enable Fast Reroute link protection:
  - IP Cisco Express Forwarding (CEF)
  - Multiprotocol Label Switching (MPLS)
- Your network must also support at least one of the following protocols:
  - Intermediate System-to-Intermediate System (IS-IS)
  - Open Shortest Path First (OSPF)

Restrictions for MPLS Traffic Engineering - Fast Reroute Link Protection

- MPLS TE works only on the Switch Virtual Interface (SVI).
- MPLS TE-FRR feature is used only for link protection and not for node protection.
- MPLS deployments that allows 4-label push is not supported.
- When the TE-FRR deployments are in ring topology, hair-pinning can occur while trying to reach the destination during cutover.
- MPLS TE-FRR is not supported on layer 3 over layer 2 deployments.
- You cannot configure BFD and RSVP on the same interface.
- You should use the no l3-over-l2 flush buffers command before configuring MPLS TE-FRR feature.
- Path protection is not supported.
- Time-division multiplexing (TDM) psuedowire over TE-FRR is not supported.
- QoS is not supported on the MPLS TE tunnels.
- You cannot enable FRR hello messages on a router that also has Resource Reservation Protocol (RSVP) Graceful Restart enabled.
- Psuedowire redundancy over TE-FRR is not supported.
- CFM over Xconnect over TE-FRR is not supported.
- The imposition statistics will not work for EOMPLS after the FRR event or layer 3 cutover.

MPLS TE-FRR Link Protection Overview

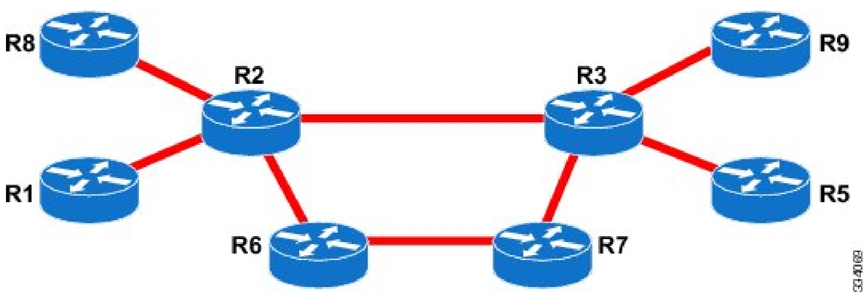
The MPLS TE is supported on the Cisco ASR 901 router to enable only the FRR. The traffic engineering aspects of MPLS TE is currently not supported. The MPLS TE is the process of establishing and maintaining label-switched paths (LSPs) across the backbone using Resource Reservation Protocol (RSVP). The path used by a given LSP at any point in time is based upon the LSP resource requirements and available network resources.

The MPLS TE-FRR feature is useful for time critical applications like voice calls that require minimal loss of data during link failures. This feature is used to overcome the issue of convergence speed experienced by the Interior Gateway Protocol (IGP) fast timers.

In the MPLS TE-FRR feature, backup tunnels are used to minimize the impact of link breakages. The point of failure can either be a head-end tunnel or a mid-point. In both the cases, the scope of recovery is local. The reroute decision is completely controlled locally by the router interfacing the failed link. The recovery is done by the node that listens to the failure. The node that detects the failure switches the traffic to the backup link with the least amount of delay.

The following figure illustrates the FRR link protection.

Figure 37: FRR Link Protection



R2	Head-end of the tunnel	**R2-R6-R7-R3**	Backup link
R2-R3	Protected link	**R3**	Tail-end of tunnel
R2-R3	Primary link		

The MPLS TE-FRR feature supports the following:

- IP, L3VPN, and EoMPLS.
- Supports BFD sessions with 50ms interval.
- Single hop tunnel and multi-hop tunnel deployments.
- Auto-tunnel feature in primary and backup nodes.
- Targeted LDP sessions on tunnels.

BFD-triggered Fast Reroute

The MPLS Traffic Engineering: BFD-triggered Fast Reroute feature allows you to obtain link protection by using the BFD protocol.

BFD

BFD is a detection protocol designed to provide fast forwarding link failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding link failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding link failures at a uniform rate, rather than the variable rates for different routing protocol Hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

Fast Reroute

Fast Reroute is a mechanism for protecting MPLS TE LSPs from link failures by locally repairing the LSPs at the point of failure. This allows the data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links.

Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure.

How to Configure Traffic Engineering - Fast Reroute Link Protection

This section describes how to configure MPLS TE-FRR Link Protection feature:

Enabling MPLS TE-FRR on an SVI Interface

To enable MPLS TE-FRR on an SVI interface, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**mpls traffic-engg tunnels** **Example:** `Router(config-if)# mpls traffic-engg tunnels`	Enables MPLS TE tunnel signaling on the specified interface.

	Command or Action	Purpose
	Example:	

Enabling MPLS TE-FRR for EoMPLS on a Global Interface

To enable MPLS TE-FRR for EoMPLS on a global interface, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**no l3-over-l2 flush buffers** **Example:** `Router(config)# no l3-over-l2 flush buffers`	Disables layer 3 over layer 2 deployments.
Step 4	**asr901-platf-frr enable** **Example:** `Router(config)# asr901-platf-frr enable`	Enables TE-FRR link protection.
Step 5	**mpls ldp discovery targeted-hello accept** **Example:** `Router(config)# mpls ldp discovery targeted-hello accept`	Configures the neighbors from which requests for targeted hello messages may be honored.
Step 6	**pseudowire-class** *pw-class-name* **Example:** `Router(config)# pseudowire-class T41`	Specifies the name of a layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 7	**encapsulation** *encapsulation-type* **Example:**	Specifies the encapsulation method used by the interface.

	Command or Action	Purpose
	`Router(config-pw-class)# encapsulation mpls`	
Step 8	**preferred-path {[interface] tunnel** *tunnel-number*| **peer** *host-ip-address***} [disable-fallback]** **Example:** `Router(config-pw-class)# preferred-path interface Tunnel41 disable-fallback`	Specifies the MPLS TE tunnel that traffic uses. • **interface**—Specifies the preferred path using an output interface. • **tunnel**—Specifies an MPLS TE tunnel interface that is the core-facing output interface. • *tunnel-number*—Tunnel interface number. • **peer**—Specifies a destination IP address or DNS name configured on the peer provider edge (PE) router, which is reachable through a label switched path (LSP). • *host-ip-address*—Peer host name or IP address.
Step 9	**exit** **Example:** `Router(config-pw-class)# exit`	Exits the pseudowire class configuration mode and enters the global configuration mode.
Step 10	**mpls label protocol ldp** **Example:** `Router(config)# mpls label protocol ldp`	Specifies the label distribution protocol for an interface. Here LDP protocol is used.
Step 11	**mpls ldp igp sync holddown** *milli-seconds* **Example:** `Router(config)# mpls ldp igp sync holddown 1000`	Specifies how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) synchronization to be achieved.

Enabling MPLS TE-FRR for EoMPLS on an Interface

To enable MPLS TE-FRR for EoMPLS on an interface, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**pw-class** **Example:**	Enables the privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**auto terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**pseudowire-class** *pw-class-name* **Example:** `Router(config)# pseudowire-class T41`	Specifies the name of a layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 4	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables the automatic negotiation.
Step 5	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 100 ethernet`	Configures an Ethernet service instance on an interface. The *id* is an integer that uniquely identifies a service instance on an interface. The value varies by the platform. Range: 1 to 4294967295. The identifier need not map to a VLAN and is local in scope to the interface.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 101`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. The *vlan-id* is the Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 8	**xconnect** *peer-ip-address vc-id* **pw-class** *pw-class-name* **Example:** `Router(config-if-srv)# xconnect 10.0.0.4 4 pw-class T41`	Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers.

	Command or Action	Purpose
		• **pw-class**—Specifies the pseudowire class for advanced configuration. • *pw-class-name*—Pseudowire class name.

Enabling MPLS TE-FRR for IS-IS

To enable MPLS TE-FRR for IS-IS routing process, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**mpls-ldp** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis`	Activates the IS-IS routing process for IP and puts the device into router configuration mode.
Step 4	**mpls traffic-eng router-id** *interface-name* **Example:** `Router(config-router)# mpls traffic-eng router-id Loopback102`	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface. The *interface-name* is the interface whose primary IP address is the router's identifier
Step 5	**mpls traffic-eng {level-1 | level-2}** **Example:** `Router(config-router)# mpls traffic-eng level-1`	Configures a router running IS-IS so that it floods MPLS TE link information into the indicated IS-IS level. • **level-1** —Floods MPLS TE link information into IS-IS level 1. • **level-2** —Floods MPLS TE link information into IS-IS level 2.
Step 6	**router isis** **Example:** `Router(config)# router isis`	Enables the IS-IS routing protocol and enters the router configuration mode.

	Command or Action	Purpose
Step 7	**net** *net-1* **Example:** `Router(config)# net 49.0001.0000.0000.0001.00`	Configures an Intermediate System-to-Intermediate System (IS-IS) network entity table (NET) for the routing process. • *net-1*—NET network services access point (NSAP) name or address for the IS-IS routing process on the Mulltilayer Switch Feature Card (MSFC) in the primary slot.
Step 8	**is-type level-1** **Example:** `Router(config-router)# is-type level-1`	Configures the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process.
Step 9	**fast-reroute per-prefix level-1 all** **Example:** `Router(config-router)# fast-reroute per-prefix level-1 all`	Configures an FRR path that redirects traffic to a remote LFA tunnel for level-1 packets. • **level-1** —Enables per-prefix FRR of level 1 packets. • **all** —Enables FRR of all primary paths.
Step 10	**fast-reroute per-prefix level-2 all** **Example:** `Router(config-router)# fast-reroute per-prefix level-2 all`	Configures an FRR path that redirects traffic to a remote LFA tunnel for level-2 packets. • **level-2** —Enables per-prefix FRR of level 2 packets. • **all** —Enables FRR of all primary paths.
Step 11	**fast-reroute remote-lfa level-1 mpls-ldp** **Example:** `Router(config-router)# fast-reroute remote-lfa level-1 mpls-ldp`	Configures an FRR path that redirects traffic to a remote LFA tunnel. • **level-1** —Enables LFA-FRR of level-1 packets. • **mpls-ldp** —Specifies that the tunnel type is MPLS or LDP.
Step 12	**fast-reroute remote-lfa level-2 mpls-ldp** **Example:** `Router(config-router)# fast-reroute remote-lfa level-2 mpls-ldp`	Configures an FRR path that redirects traffic to a remote LFA tunnel. • **level-2**—Enables LFA-FRR of level-2 packets. • **mpls-ldp**—Specifies that the tunnel type is MPLS or LDP.
Step 13	**bfd all-interfaces** **Example:** `Router(config-router)# bfd all-interfaces`	Enables Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process.

	Command or Action	Purpose
Step 14	**mpls ldp sync** **Example:** `Router(config-router)# mpls ldp sync`	Enables MPLS LDP synchronization on interfaces for an IS-IS process.

Configuring Primary One-hop Auto-Tunnels

To configure primary one-hop auto-tunnels for MPLS TE-FRR, perform the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng auto-tunnel primary onehop** **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary onehop`	Creates primary tunnels to all the next hops automatically.

Step 4	**mpls traffic-eng auto-tunnel primary tunnel-num [min** *min-num***] [max** *max-num* **]**
	Example:
	`Router(config)# mpls traffic-eng auto-tunnel`
	`primary tunnel-num min 3 max 400`
		Configures the range of tunnel interface numbers for primary autotunnels.
		• *min-num*—(Optional) Minimum number of the primary tunnels. The range is 0 to 65535, with a default value of 65436.
		• *max-num*—(Optional) Maximum number of the primary tunnels. The max number is the minimum number plus 99. The range is from 0 to 65535.

Step 5	**mpls traffic-eng auto-tunnel primary config unnumbered** *interface*
	Example:
	`Router(config)# mpls traffic-eng auto-tunnel`
	`primary config unnumbered-interface Loopback102`
		Enables IP processing without an explicit address.
		• *interface*—Interface on which IP processing is enabled without an explicit address.

	Command or Action	Purpose
Step 6	**mpls traffic-eng auto-tunnel primary timers removal rerouted** *sec* **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 604800`	Configures the period after a failure to remove primary autotunnels. • *sec*—Number of seconds after a failure that primary autotunnels are removed. The range is from 30 to 604,800, with a default of 0.
Step 7	**mpls traffic-eng auto-tunnel primary config mpls ip** **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary config mpls ip`	Enables Label Distribution Protocol (LDP) on primary autotunnels.

Configuring Backup Auto-Tunnels

To configure backup auto-tunnels, perform the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng auto-tunnel backup** **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup`	Builds next-hop (NHOP) and next-next hop (NNHOP) backup tunnels automatically.
Step 4	**mpls traffic-eng auto-tunnel backup nhop-only** **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup nhop-only`	Builds next-hop (NHOP) backup tunnels automatically.

	Command or Action	Purpose
Step 5	**mpls traffic-eng auto-tunnel backup tunnel-num** [**min** *min-num*] [**max** *max-num*] **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 3 max 400`	Configures the range of tunnel interface numbers for backup autotunnels. • *min-num*—(Optional) Minimum number of the backup tunnels. The range is 0 to 65535, with a default value of 65436. • *max-num*—(Optional) Maximum number of the backup tunnels. The max number is the minimum number plus 99. The range is from 0 to 65535.
Step 6	**mpls traffic-eng auto-tunnel backup timers removal unused** *sec* **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 604800`	Configures how frequently a timer scans the backup autotunnels and remove tunnels that are not being used. • *sec*—Configures (in seconds) the timer scan interval. The range is 0 to 604,800.
Step 7	**mpls traffic-eng auto-tunnel backup config unnumbered-interface** *interface* **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface Loopback0`	Configures a specific unnumbered interface for all backup auto-tunnels. • *interface*—Interface for all backup auto-tunnels. Default interface is Loopback0.

Enabling Targeted LDP session over Primary one-hop Auto-Tunnels

An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS TE tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers. You establish non-directly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

The default behavior of an LSR is to ignore requests from other LSRs that send targeted Hello messages. You can configure an LSR to respond to requests for targeted Hello messages by using the mpls ldp discovery targeted-hello accept command.

The active LSR mandates the protocol that is used for a targeted session. The passive LSR uses the protocol of the received targeted Hello messages.

To enable targeted LDP sessions over primary one-hop auto-tunnels, perform the steps given below:

Note For targeted mpls session, the head end tunnel should have “mpls ip” configuration.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**mpls ldp discovery targeted-hello accept** **Example:** `Router(config)# mpls ldp discovery targeted-hello accept`	Configures the router to respond to requests for targeted Hello messages from all neighbors.

Enabling BFD Triggered FRR on an SVI Interface

To enable BFD triggered FRR on an SVI interface, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip rsvp signalling hello bfd** **Example:** `Router(config-if)# ip rsvp signalling hello bfd`	Enables BFD protocol on an interface for FRR link protection.

Enabling BFD Triggered FRR on a Router

To enable BFD triggered FRR on a router, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip rsvp signalling hello bfd** **Example:** `Router(config-if)# ip rsvp signalling hello bfd`	Enables BFD protocol on an interface for FRR link protection.

What to do next

Verification Examples

Verifying MPLS TE-FRR Configuration

To verify the MPLS TE-FRR configuration, use the **show** commands given below:

- **show mpls traffic-eng tunnels brief**
- **show ip rsvp sender detail**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng tunnels backup**
- **show ip rsvp reservation detail**

Note For more information on the above show commands, see: http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-frr-node-prot.html

Use the following command to verify whether the backup tunnels are up.

```
Router# show mpls traffic-eng tunnels brief
Signalling Summary:
```

```
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Use the following command to verify whether the LSPs are protected by the appropriate backup tunnels.

```
Router# show ip rsvp sender detail
PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

Use the following command to verify whether the LSPs are protected.

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel      In-label   intf/label       FRR intf/label     Status
Tunnel10              Tun        pos5/0:Untagged  Tu0:12304          ready
Prefix item frr information:
Prefix        Tunnel  In-label   Out intf/label   FRR intf/label     Status
10.0.0.11/32  Tu110   Tun hd     pos5/0:Untagged  Tu0:12304          ready
LSP midpoint frr information:
LSP identifier        In-label   Out intf/label   FRR intf/label     Status
10.0.0.12 1 [459]     16         pos0/1:17        Tu2000:19          ready
```

Use the following command to verify the backup tunnel information.

```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
```

```
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin up, Oper: up
  Src 10.55.55.55,, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

Use the following command to verify the reservation detail.

```
Router# show ip rsvp reservation detail
Reservation:
  Tun Dest: 10.1.1.1  Tun ID: 1  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 104
  Next Hop: 172.17.1.2 on POS1/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    172.18.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    172.19.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    172.19.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

Verifying Primary One-hop Auto-Tunnels

To verify the configuration of primary one-hop auto-tunnels, use the **show** commands as shown in the following examples.

```
Router# show ip rsvp fast-reroute
Primary                  Protect BW         Backup
Tunnel                   I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                   ------- --------   ------------- ------ -----   ------
R3-PRP_t0                PO3/1   0:G        Tu1000:24     Ready  any-unl Nhop
Router# show ip interface brief
Interface            IP-Address    OK?  Method  Status                 Protocol
POS2/0               10.0.0.14     YES  NVRAM   down                   down
POS2/1               10.0.0.49     YES  NVRAM   up                     up
POS2/2               10.0.0.45     YES  NVRAM   up                     up
POS2/3               10.0.0.57     YES  NVRAM   administratively down  down
POS3/0               10.0.0.18     YES  NVRAM   down                   down
POS3/1               10.0.0.33     YES  NVRAM   up                     up
POS3/2               unassigned    YES  NVRAM   administratively down  down
POS3/3               unassigned    YES  NVRAM   administratively down  down
GigabitEthernet4/0   10.0.0.37     YES  NVRAM   up                     up
GigabitEthernet4/1   unassigned    YES  NVRAM   administratively down  down
GigabitEthernet4/2   unassigned    YES  NVRAM   administratively down  down
Loopback0            10.0.3.1      YES  NVRAM   up                     up
Tunnel0              10.0.3.1      YES  unset   up                     up
```

```
Tunnel65436          10.0.3.1      YES  unset   up                      up
Ethernet0            10.3.38.3     YES  NVRAM   up                      up
Ethernet1            unassigned    YES  NVRAM   administratively down   down
```

Verifying Backup Auto-Tunnels

To verify the configuration of backup auto-tunnels, use the **show** commands as shown in the following examples.

```
Router# show ip rsvp fast-reroute
Primary     Protect   BW         Backup
Tunnel      I/F       BPS:Type   Tunnel:Label  State  Level   Type
------      -------   -------    ------------  ------ -----   ----
R3-PRP_t0   PO3/1     0:G        None          None   None
Router# show ip interface brief
Interface               IP-Address      OK? Method Status                  Protocol
POS2/0                  10.0.0.14       YES NVRAM  down                    down
POS2/1                  10.0.0.49       YES NVRAM  up                      up
POS2/2                  10.0.0.45       YES NVRAM  up                      up
POS2/3                  10.0.0.57       YES NVRAM  administratively down   down
POS3/0                  10.0.0.18       YES NVRAM  down                    down
POS3/1                  10.0.0.33       YES NVRAM  up                      up
POS3/2                  unassigned      YES NVRAM  administratively down   down
POS3/3                  unassigned      YES NVRAM  administratively down   down
GigabitEthernet4/0      10.0.0.37       YES NVRAM  up                      up
GigabitEthernet4/1      unassigned      YES NVRAM  administratively down   down
GigabitEthernet4/2      unassigned      YES NVRAM  administratively down   down
Loopback0               10.0.3.1        YES NVRAM  up                      up
Tunnel0                 10.0.3.1        YES unset  up                      up
Tunnel65436             10.0.3.1        YES unset  up                      up
Tunnel65437             10.0.3.1        YES unset  up                      up
Ethernet0               10.3.38.3       YES NVRAM  up                      up
Ethernet1               unassigned      YES NVRAM  administratively down   down
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin up, Oper: up
  Src 10.55.55.55,, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

Verifying BFD Triggered FRR Configuration

To verify the configuration of BFD triggered FRR, use the **show** commands as shown in the following examples.

- **show mpls traffic-eng tunnels brief**
- **show ip rsvp sender detail**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng tunnels backup**
- **show ip rsvp reservation detail**
- **show ip rsvp hello**
- **show ip rsvp interface detail**
- **show ip rsvp hello bfd nbr**
- **show ip rsvp hello bfd nbr detail**
- **show ip rsvp hello bfd nbr summary**

Note For more information on the above show commands, see: http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-bfd-frr.html

Use the following command to verify whether or not the backup tunnels are up:

```
Router# show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         Gi4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         Gi4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Use the following command to verify whether the LSPs are protected by the appropriate backup tunnels.

```
Router# show ip rsvp sender detail
PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
```

```
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

Use the following command to verify whether the LSPs are protected:

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel              In-label Out intf/label   FRR intf/label   Status
Tunnel500                     Tun hd   AT4/0.100:Untagg Tu501:20         ready
Prefix item frr information:
Prefix             Tunnel     In-label Out intf/label    FRR intf/label  Status
10.0.0.8/32        Tu500      18       AT4/0.100:Pop ta  Tu501:20        ready
10.0.8.8/32        Tu500      19       AT4/0.100:Untagg  Tu501:20        ready
10.8.9.0/24        Tu500      22       AT4/0.100:Untagg  Tu501:20        ready
LSP midpoint item frr information:
LSP identifier     In-label Out     intf/label     FRR intf/label     Status
```

Use the following command to verify the backup tunnel information.

```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

Use the following command to verify detailed RSVP-related receiver information currently in the database.

```
Router# show ip rsvp reservation detail
Reservation:
  Tun Dest:   10.1.1.1  Tun ID: 1  Ext Tun ID: 10.1.1.1
  Tun Sender: 10.1.1.1  LSP ID: 104
  Next Hop: 10.1.1.2 on Gi1/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    10.1.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

Use this command to display hello status and statistics for FRR, reroute (hello state timer), and graceful restart.

```
Router# show ip rsvp hello
Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

Use this command to display the interface configuration for Hello.

```
Router# show ip rsvp interface detail
Gi9/47:
 RSVP: Enabled
 Interface State: Up
 Bandwidth:
  Curr allocated: 0 bits/sec
  Max. allowed (total): 0 bits/sec
  Max. allowed (per flow): 0 bits/sec
  Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
  Set aside by policy (total): 0 bits/sec
 Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
 Authentication: disabled
  Key chain: <none>
  Type:  md5
  Window size: 1
  Challenge:  disabled
 FRR Extension:
  Backup Path: Configured (or "Not Configured")
 BFD Extension:
  State: Disabled
  Interval: Not Configured
 RSVP Hello Extension:
  State: Disabled
  Refresh Interval: FRR: 200  , Reroute: 2000
  Missed Acks:      FRR: 4    , Reroute: 4
  DSCP in HELLOs:   FRR: 0x30 , Reroute: 0x30
```

Use this command to display information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol.

```
Router# show ip rsvp hello bfd nbr
Client  Neighbor    I/F     State   LostCnt   LSPs
FRR     10.0.0.6    Gi9/47  Up      0         1
```

Use this command to display detailed information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol:

```
Router# show ip rsvp hello bfd nbr detail
 Hello Client Neighbors
 Remote addr 10.0.0.6, Local addr  10.0.0.7
  Type: Active
  I/F: Gi9/47
  State: Up (for 00:09:41)
  Clients: FRR
  LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
  Communication with neighbor lost: 0
```

Use this command to display summarized information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol.

```
Router# show ip rsvp hello bfd nbr summary
Client  Neighbor    I/F     State  LostCnt  LSPs
FRR     10.0.0.6   Gi9/47  Up     0        1
```

Configuration Examples

This section provides sample configuration examples for IPv6 over MPLS: 6PE and 6VPE feature on the Cisco ASR 901 router.

Example: Configuring MPLS TE-FRR

For a sample configuration of MPLS TE-FRR, see:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-frr-node-prot.html

Example: Configuring Primary One-hop Auto-Tunnels

For a sample configuration of primary one-hop auto-tunnels, see:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-autotunnel.html

Example: Configuring Backup Auto-Tunnels

For a sample configuration of backup auto-tunnels, see:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-autotunnel.html

Example: Configuring BFD Triggered FRR

For a sample configuration of BFD triggered FRR, see:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-bfd-frr.html

Additional References

The following sections provide references related to IPv6 Multicast feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference

Standards and RFCs

Standards/RFCs	Title
RFC 2710	Multicast Listener Discovery (MLD) for IPv6

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for MPLS Traffic Engineering - Fast Reroute Link Protection

Table 39: Feature Information for MPLS Traffic Engineering - Fast Reroute Link Protection, on page 650 lists the features in this module and provides links to specific configuration information.

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 Table 39: Feature Information for MPLS Traffic Engineering - Fast Reroute Link Protection, on page 650 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 39: Feature Information for MPLS Traffic Engineering - Fast Reroute Link Protection

Feature Name	Releases	Feature Information
MPLS Traffic Engineering	15.2(2)SNG	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:

Feature Name	Releases	Feature Information
BFD-triggered Fast Reroute	15.2(2)SNG	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
TE-FRR for EoMPLS	15.3(2)S	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:

CHAPTER 36

Layer 2 Control Protocol Peering, Forwarding, and Tunneling

This feature module describes how to configure Layer 2 (L2) Control Protocol Peering, Forwarding, and Tunneling feature on the Cisco ASR 901 Series Aggregation Services Routers.

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 Layer 2 Control Protocol Peering, Forwarding, and Tunneling, on page 666.

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 Layer 2 Control Protocol Peering, Forwarding, and Tunneling

- A Cisco IOS software that supports Layer 2 Control Protocol Peering, Forwarding, and Tunneling must be installed previously on the Cisco ASR 901 Series Aggregation Services Router. For supported software releases, see Release Notes for Cisco ASR 901 Series Aggregation Services Router.

Restrictions for Layer 2 Control Protocol Peering, Forwarding, and Tunneling

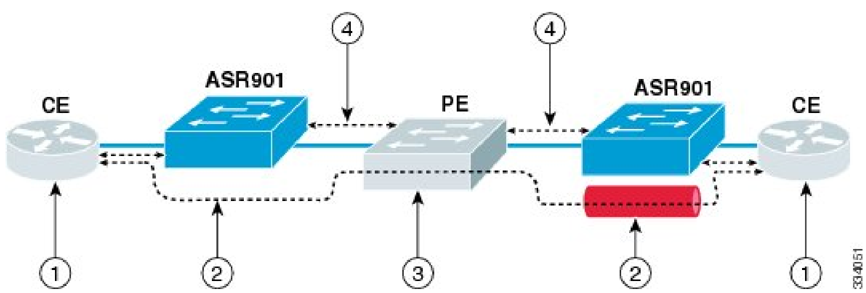
- If you want to peer Operation, Administration, and Maintenance (OAM) packets when **l2proto-forward tagged** command is configured at the interface level, you should also configure the **l2protocol peer lacp** command.
- Received L2CP Control Packets (like STP, CDP, and others) are not mirrored to the destination port.
- Forwarding L2CP tunneled packets over x-connect is not supported.

Layer 2 Control Protocol Forwarding

The ASR 901 forwards Layer 2 Control Protocol (L2CP) packets between customer-edge (CE) devices. Cisco ASR 901 router supports L2CP forwarding on Bridge-domain EVCs and on Cross-connect EVCs.

The following figure depicts an end-to-end layer 2 forwarding. The layer 2 traffic is sent through the S-network, and the S-network switches the traffic from end to end. The Cisco ASR 901 router forwards frames from the user network interface (UNI) to the network-to-network Interface (NNI) after appending S-tag. The third party provider edge (PE) router forwards the S-tagged frames. The PE peers the untagged Link Layer Discovery Protocol (LLDP) and Link Aggregation Control Protocol (LACP) frames. On the reverse path (from NNI to UNI), the S-tag is removed.

Figure 38: Layer 2 Forwarding



1	L2CP packets are forwarded between CE devices.	3	Third party PE forwards S-tagged frames and peers untagged frames.
2	Frames are forwarded from UNI to NNI after appending the S-tag. On the reverse path (NNI to UNI), S-tag is removed.	4	Untagged LLDP and LACP is peered.

Layer 2 Control Protocol Tunneling

Layer 2 Control Protocol Tunneling (L2PT) is a Cisco proprietary protocol for tunneling Ethernet protocol frames across layer 2 switching domains. The following tunnel protocols are supported:

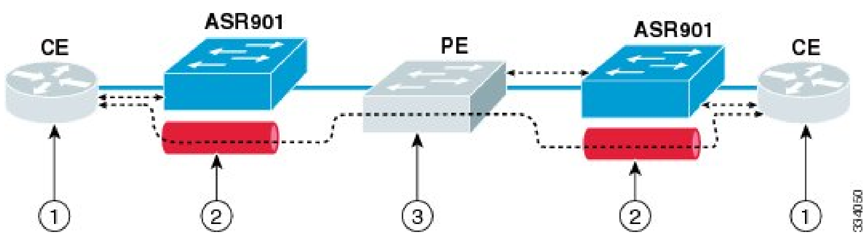
- Cisco Discovery Protocol (CDP)

- Dynamic Trunking Protocol (DTP)
- Link Aggregation Control Protocol (LACP)
- Link Layer Discovery Protocol (LLDP)
- Spanning Tree Protocol (STP)—including Multiservice Transport Platform (MSTP) and Per VLAN Spanning Tree (PVST)
- Virtual Trunking Protocol (VTP)

The ASR 901 router allows to tunnel layer 2 packets between CEs. The Cisco proprietary multicast address (01-00-0c-cd-cd-d0) is used while tunneling the packet over the NNI interfaces.

The following figure depicts Layer 2 Protocol Tunneling. The layer 2 traffic is sent through the S-network, and the S-network switches the traffic from end to end. The Cisco multicast address is added to the frames and sent from UNI to NNI. On the reverse path (NNI to UNI), protocol specific multicast address is attached to the frames and sent to the UNI.

Figure 39: Layer 2 Protocol Tunneling



1	CE layer 2 control protocol tunnel (end-to-end).	3	Third party PE forwards S-tagged frames and peers untagged frames.
2	Cisco multicast address is added to the frames and sent from UNI to NNI. On the reverse path (NNI to UNI), a protocol specific multicast address is attached to the frames and sent to UNI.	4	—

How to Configure Layer 2 Control Protocol Peering, Forwarding, and Tunneling

This section describes how to configure layer 2 control protocol peering, forwarding and tunneling:

Note The configuration defined for LACP impacts all slow protocols, and is applicable to all the options like peering, forwarding, and tunneling.

Configuring Layer 2 Peering

The ASR 901 router supports layer 2 peering functionality on a per Ethernet Flow Point (EFP) basis. It supports a maximum packet rate of 10 packets ps (per interface) for a protocol, and 100 packets ps for all protocols (on all interfaces).

Table 40: Options Supported on the ASR 901 Router, on page 656 displays the supported defaults and configuration options for the Cisco ASR 901 router.

Table 40: Options Supported on the ASR 901 Router

Protocol	Packet Type	Default Action	Configuration Option
CDP	Untagged	Peer	Peer/Forward/Tunnel
DTP	Untagged	Peer	Peer/Forward/Tunnel
LACP	Untagged	Peer	Peer/Forward/Tunnel
LLDP	Untagged	Peer	Peer/Forward/Tunnel
STP	Untagged	Peer	Peer/Forward/Tunnel
VTP	Untagged	Peer	Peer/Forward/Tunnel
CDP	Tagged	Drop	Forward/Tunnel
DTP	Tagged	Drop	Forward/Tunnel
LACP	Tagged	Drop	Forward/Tunnel
LLDP	Tagged	Drop	Forward/Tunnel
STP	Tagged	Drop	Forward/Tunnel
VTP	Tagged	Drop	Forward/Tunnel

Complete the following steps to configure layer 2 peering:

Note

- If an EFP is configured with layer 2 peering, then L2CP packets coming on the EFP is sent to the CPU for local protocol processing.
- Layer2 protocol peering is not supported on port-xconnect.

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/6`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 20 ethernet`	Configures an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if-srv)# encapsulation untagged`	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.
Step 6	**l2protocol peer** [*protocol*] **Example:** `Router(config-if-srv)# l2protocol peer lacp`	Configures transparent Layer 2 protocol peering on the interface for a specified layer 2 protocol. • *protocol*—The protocol to be used. The options are: *cdp, dtp, lacp, lldp, stp,*and *vtp*. **Note** The peer option is not supported for DTP protocol.

Configuring Layer 2 Forwarding

Complete the following steps to configure layer 2 forwarding:

Note

- The layer 2 forwarding functionality is supported only on an untagged EFP (Only one untagged EFP exists per interface).
- Forwarding functionality is not supported with dot1q VLAN range encapsulation.
- If an interface is configured with layer 2 protocol forwarding, then L2CP packets on the interface are flooded on to the bridge domain. The flooding follows the translations specified in interface.
- Any manipulation of EXP bit is not supported while sending Bridge Protocol Data Units (BPDU) over xconnect.
- L2CP forwarding is supported only on xconnect interfaces/EFPs created over GigE/TenGig/Port-channel interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**l2proto-forward tagged** *protocol* **Example:** `Router(config-if)# l2proto-forward tagged cdp`	Configures a layer 2 control protocol forwarding on an interface. • *protocol*—Specifies the protocol to be forwarded.
Step 5	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 20 ethernet`	Configures an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface.
Step 6	**encapsulation untagged** **Example:** `Router(config-if-srv)# encapsulation untagged`	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.
Step 7	**l2protocol forward** [*protocol*] **Example:** `Router(config-if-srv)# l2protocol forward cdp`	Enables forwarding of untagged packets of specified protocol in a service instance. • *protocol*—The protocol to be used. The options are: *cdp, dtp, lacp, lldp, stp,*and *vtp*. Perform Step 8 if you want to bind a service instance to a bridge domain. Go to Step 9 if you want to bind an attachment to a xconnect.
Step 8	**bridge-domain** *bridge-id* **Example:**	Binds a service instance to a bridge domain instance.

	Command or Action	Purpose
	`Router(config-if-srv)# bridge-domain 200`	• *bridge-id*—Identifier for the bridge domain instance.
Step 9	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 1.1.1.1 100 encapsulation mpls`	Binds an attachment circuit to a pseudowire. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers. • **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire. • **mpls**—Specifies MPLS as the tunneling method.

Configuring Layer 2 Tunneling

The ASR 901 router supports layer 2 control protocol tunneling functionality on a per EFP basis. This functionality is supported for tagged and untagged packets based on CDP, DTP, LACP, LLDP, STP, and VTP protocols.

If an EFP is configured for layer 2 control protocol tunneling, then:

- Any L2CP packet coming on the EFP is forwarded to the bridge domain (BD) with Cisco proprietary multicast address (01-00-0c-cd-cd-d0).
- Any packet coming on the BD with Cisco proprietary multicast address (01-00-0c-cd-cd-d0) is stamped with well known L2CP MAC address (on EFP which has layer 2 protocol tunneling configured).
- A packet with Cisco proprietary multicast address is forwarded as is if l2protocol tunnel is not configured.

Complete the following steps to configure layer 2 tunneling:

Note

- Layer 2 protocol tunneling is not supported on xconnect EFPs.
- Tunneling functionality is not supported with dot1q VLAN range encapsulation.
- Layer 2 protocol tunneling supports a maximum packet rate of 10 packets ps (per interface) for a protocol, and 100 packets ps for all protocols (on all interfaces).
- Layer2 protocol tunneling is not supported on port-xconnect.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/4`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 9 ethernet`	Configure an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if-srv)# encapsulation untagged`	Sets the encapsulation method used by the interface. • *encapsulation type*—Type of encapsulation to be used.
Step 6	**l2protocol tunnel** [*protocol*] **Example:** `Router(config-if-srv)# l2protocol tunnel cdp`	Configures transparent Layer 2 protocol tunneling on the interface for the specified Layer 2 protocol. • *protocol*—(Optional) The protocol to be used. The options are: *cdp, dtp, lacp, lldp, stp*,and *vtp*.
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 9`	Binds a service instance to a bridge domain instance. • *bridge-id*—Identifier for the bridge domain instance.

Verifying Layer 2 Peering

To verify the layer 2 protocol peering functionality, use the **show ethernet service instance** command as shown below.

```
Router# show ethernet service instance id 99 interface gigabitEthernet0/4 detail
Service Instance ID: 99
Service Instance Type: static
Associated Interface: GigabitEthernet0/4
Associated EVC:
L2protocol peer cdp
CE-Vlans:
Encapsulation: untagged
Interface Dot1q Tunnel Ethertype: 0x8100
```

```
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 99
```

Verifying Layer 2 Forwarding

To verify the layer 2 protocol forwarding functionality, use the **show ethernet service instance** command as shown below.

```
Router# show ethernet service instance id 99 interface gigabitEthernet 0/0 detail
Service Instance ID: 99
Service Instance Type: static
Associated Interface: GigabitEthernet0/0
Associated EVC:
L2protocol forward cdp lldp
CE-Vlans:
Encapsulation: untagged
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
Pkts In Bytes In Pkts Out Bytes Out
0 0 0 0
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 99
```

Verifying Layer 2 Tunneling

To verify the layer 2 control protocol tunneling functionality, use the **show ethernet service instance** command as shown below.

```
Router# show ethernet service instance id 9 interface GigabitEthernet 0/4 detail
Service Instance ID: 9
Service Instance Type: static
Associated Interface: GigabitEthernet0/4
Associated EVC:
L2protocol tunnel
CE-Vlans:
Encapsulation: untagged
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
Pkts In Bytes In Pkts Out Bytes Out
0 0 0 0
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 9
```

Configuration Examples

This section provides sample configuration examples for Layer 2 Control Protocol Peering, Forwarding, and Tunneling feature on the Cisco ASR 901 routers.

Example: Configuring Layer 2 Peering

The following is a sample configuration of layer 2 peering.

```
!
interface GigabitEthernet0/0
negotiation auto
l2proto-forward tagged -- forwards all tagged frames, and drops untagged frames
cdp enable
service instance 9 ethernet
encapsulation dot1q 9
rewrite ingress tag pop 1 symmetric
bridge-domain 9
!
service instance 99 ethernet
encapsulation untagged
l2protocol peer cdp lldp -- peers lldp and cdp
bridge-domain 99
!
!
```

Example: Configuring Layer 2 Forwarding

The following is a sample configuration of layer 2 protocol forwarding at untagged EFP.

```
Building configuration...
Current configuration : 267 bytes
!
interface Port-channel1
 negotiation auto
!
 service instance 9 ethernet
  encapsulation untagged
  l2protocol forward cdp
  bridge-domain 9
 !
end
```

The following is a sample configuration of layer 2 protocol forwarding of tagged BPDUs at the port-channel interface level.

```
Current configuration : 270 bytes
!
interface Port-channel1
 no negotiation auto
 l2proto-forward tagged cdp
 service instance 9 ethernet
  encapsulation untagged
  bridge-domain 9
 !
 service instance 99 ethernet
```

```
  encapsulation dot1q 99
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
 !
end
```

Note By default, tagged and untagged BPDUs are forwarded on port-xconnect.

The following is a sample configuration for interface level forwarding.

```
interface GigabitEthernet0/3
 no ip address
 negotiation auto
 l2proto-forward tagged cdp lldp
service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  xconnect 55.55.55.55 123 encapsulation mpls
service instance 200 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  xconnect 66.66.66.66 124 encapsulation mpls
service instance 300 ethernet
  encapsulation untagged
  l2protocol peer cdp
l2protocol forward lacp
bridge-domain 300
```

The following is a sample configuration for Default Encapsulation EFP.

```
interface GigabitEthernet0/3
no ip address
 negotiation auto
service instance 200 ethernet
 encapsulation default
 l2protocol forward cdp stp
 l2protocol peer lldp
 xconnect 33.33.33.33 123 encapsulation mpls
```

Note No explicit L2CP related configuration needs to be done for port-xconnect.

The following is a sample configuration for port-xconnect.

```
interface GigabitEthernet 0/4
 xconnect 44.44.44.44 123 encapsulation mpls
```

Example: Configuring Layer 2 Tunneling

The following is a sample configuration of Layer 2 control protocol tunneling for untagged packets.

```
Building configuration...
Current configuration : 151 bytes
!
```

```
interface GigabitEthernet0/1
negotiation auto
service instance 10 ethernet
encapsulation untagged
l2protocol tunnel cdp
bridge-domain 10
!
Service instance 100 ethernet
encapsulation dot1q 100
l2protocol tunnel lldp
rewrinte ingress tag pop 1 symmetric
bridge-domain 100
!
interface GigabitEthernet0/7
negotiation auto
service instance 20 ethernet
encapsulation untagged
l2protocol tunnel
bridge-domain 20
!
end
```

The following is a sample configuration of Layer 2 control protocol tunneling for tagged packets.

Note The configuration given below applies to only one router. Similar configuration has to be applied on two Cisco ASR 901 routers.

```
Building configuration...
Current configuration : 153 bytes
!
interface GigabitEthernet0/11
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 100
  l2protocol tunnel
  bridge-domain 50
 !
!
interface GigabitEthernet0/1
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 100
  bridge-domain 50
 !
end
```

The following is a sample configuration of layer 2 protocol tunneling for receiving untagged LLDP packets from customer nodes and tunneling them tagged over provider network.

Router 1

```
Building configuration...
Current configuration : 151 bytes
!
interface GigabitEthernet0/1
 negotiation auto
 service instance 10 ethernet
  encapsulation untagged
  l2protocol tunnel lldp
```

```
  bridge-domain 20
 !
!
interface GigabitEthernet0/7
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
end
```

Router 2

```
Current configuration : 170 bytes
!
interface GigabitEthernet0/7
 negotiation auto
 service instance 20 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
 !
!
interface GigabitEthernet0/6
 negotiation auto
 service instance 20 ethernet
  encapsulation untagged
  l2protocol tunnel lldp
  bridge-domain 30
 !
end
```

Additional References

The following sections provide references related to the Layer 2 Control Protocol Peering, Forwarding, and Tunneling feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference
Cisco IOS LAN Switching Commands	Cisco IOS LAN Switching Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Layer 2 Control Protocol Peering, Forwarding, and Tunneling

Table 41: Feature Information for Layer 2 Control Protocol Peering, Forwarding, and Tunneling, on page 667 lists the features in this module and provides links to specific configuration information.

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 Table 41: Feature Information for Layer 2 Control Protocol Peering, Forwarding, and Tunneling, on page 667 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 41: Feature Information for Layer 2 Control Protocol Peering, Forwarding, and Tunneling

Feature Name	Releases	Feature Information
Layer 2 Control Protocol Peering and Forwarding	15.2(2)SNG	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature: The following command was introduced: l2proto-forward
Layer 2 Control Protocol Tunneling	15.2(2)SNH1	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
Layer 2 Control Protocol Forwarding over xconnect	15.4(1)S	This feature was introduced on the Cisco ASR 901 routers.

CHAPTER 37

Configuring Inverse Muliplexing over ATM

This feature module describes how to configure Inverse Multiplexing over ATM (IMA) to transport ATM traffic over a bundle of T1 or E1 cables. This feature enables the expansion of WAN bandwidth from T1 speeds, without DS3 or OC3 circuits.

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 Inverse Multiplexing over ATM, on page 690.

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

Before testing any IMA implementation, you should terminate the T1 circuits end-to-end.

Restrictions

The following features are not supported:

- Native ATM interfaces

- IP Routing
- VPI or VCI rewrite
- 1:1 and N:1 (where N > 1) VCC or VPP mode
- up and down traps
- ATM class of service (CBR, VBR-RT, VBR-nRT, UBR+, and UBR) for VPCs and port-mode
- Transmission of AIS on VCCs and VPCs to the customer-edge s, when the pseudowire goes down.
- Enabling atm cell payload scrambling for T1
- Disabling atm cell payload scrambling for E1

Information About Inverse Muliplexing over ATM

IMA involves inverse multiplexing and de-multiplexing of ATM cells in a cyclical fashion among physical links grouped to form a higher-bandwidth and logical link. Streams of cells are distributed in a round-robin manner across the multiple T1/E1 links and reassembled at the destination to form the original cell stream. Sequencing is provided using IMA Control Protocol (ICP) cells.

The following features are supported in this release:

- AAl0 and AAL5 encapsulation
- N:1 (where N == 1) VPC and VCC cell relay mode
- Cell packing and Maximum Cell Packing Timeout (MCPT) timers
- Port mode
- AAL5 SDU frame encapsulation

How to Configure IMA

This section describes how to configure IMA on E1/T1 interface and over MPLS:

Configuring ATM IMA on T1/E1 Interface

To configure the ATM IMA on an E1 or T1 interface, complete the following steps:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**card type** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# card type e1 0 0`	Configures IMA on an E1 or T1 interface.
Step 4	**controller** {**t1** | **e1**} *slot/port* **Example:** `Router(config)# controller E1 0/4`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 5	**ima-group** *ima-group-number* **Example:** `Router(config-controller)# ima-group 0`	Assigns the interface to an IMA group. This command creates the ATM0/IMAx interface by default.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the controller interface.
Step 7	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config-if)# interface ATM0/IMA0`	Specifies the slot location and port of IMA interface group. • *ATMslot*—Specifies the slot location of the ATM IMA port adapter. • *ATMgroup-number*—Specifies the group number of the IMA group.
Step 8	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 9	**atm bandwidth dynamic** **Example:** `Router(config-if)# atm bandwidth dynamic`	Specifies the ATM bandwidth as dynamic.
Step 10	**no atm ilmi-keepalive** **Example:** `Router(config-if)# no atm ilmi-keepalive`	Disables the Interim Local Management Interface (ILMI) keepalive parameters.

Configuring ATM IMA over MPLS

This service allows the Cisco ASR 901 router to deliver ATM services over an existing MPLS network. The following sections describe how to configure transportation of service using ATM over MPLS:

Configuring the T1/E1 Controller

Complete the following steps to configure an E1 or T1 controller:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**card type {t1 | e1}** *slot port* **Example:** `Router(config)# card type e1 0 0`	Configures the IMA on an E1 or T1 interface.
Step 4	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller E1 0/4`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 5	**clock source internal** **Example:** `Router(config-controller)# clock source internal`	Sets the clock source to internal.
Step 6	**ima-group group-number** **Example:** `Router(config-controller)# ima-group 0`	Specifies the group number for the controller.

Configuring an ATM IMA Interface

Complete the following steps to configure an ATM IMA interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller E1 0/4`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config-controller)# interface ATM0/IMA0`	Specifies the slot location and port of IMA interface group. • *ATMslot/*—Specifies the slot location of the ATM IMA port adapter. • */IMAgroup-number*—Specifies the group number of the IMA group.
Step 5	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 6	**atm bandwidth dynamic** **Example:** `Router(config-if)# atm bandwidth dynamic`	Specifies the ATM bandwidth as dynamic.
Step 7	**no atm ilmi-keepalive** **Example:** `Router(config-if)# no atm ilmi-keepalive`	Disables the ILMI keepalive parameters.

Configuring ATM over MPLS Pseudowire Interface

You can configure ATM over MPLS in the following modes:

Configuring a Port Mode Pseudowire

A port mode pseudowire allows you to map an entire ATM interface to a single pseudowire connection. To configure, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface atm0/ima0`	Specifies the slot location and port of IMA interface group and configures the ATM interface. • *ATMslot*—Specifies the slot location of the ATM IMA port adapter. • *IMAgroup-number*—Specifies the group number of the IMA group.
Step 4	**xconnect** *ip-address port-number* **encapsulation mpls** **Example:** `Router(config-if)# xconnect 10.10.10.10 20 encapsulation mpls`	Binds an attachment circuit to the ATM IMA interface to create a pseudowire.

Configuring an N-to-1 VCC Cell Mode

An N-to-1 Virtual Channel Connection (VCC) pseudowire allows you to map a ATM VCC to a pseudowire. You must use an ATM adaptation layer (AAL) encapsulation for this transport type. To configure, complete the following steps:

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface ATM0/IMA0`	Specifies the slot location and port of IMA interface group and configures the ATM interface. • *ATMslot*—Specifies the slot location of the ATM IMA port adapter. • *ATMgroup-number*—Specifies the group number of the IMA group.
Step 4	**pvc VPI/VCI l2transport** **Example:** `Router(config-if)# 100/12 l2transport`	Specifies the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the Permanent Virtual Circuit (PVC) and configures them in layer 2 transport mode.
Step 5	**encapsulation** *encapsulation-typ*e **Example:** `Router(config-if-atm-l2trans-)# encapsulation aal0`	Sets the encapsulation type to AAL0
Step 6	**xconnect ip-address port-number encapsulation mpls one-to-one** **Example:** `Router(config-if-atm-l2trans-)# xconnect 25.25.25.25 125 encapsulation mpls`	Binds an attachment circuit to the ATM IMA interface to create a pseudowire.

Configuring an N-to-1 vPC Cell Mode

An N-to-1 virtual port channel (vPC) pseudowire allows you to map one or more vPCs to a single pseudowire. You must use ATM Adaptation Layer (AAL) encapsulation for this transport type. To configure, complete the following steps:

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface ATM0/IMA0`	Specifies the slot location and port of IMA interface group and configures the ATM interface. • *ATMslot*—Specifies the slot location of the ATM IMA port adapter. • *IMAgroup-number*—Specifies the group number of the IMA group.
Step 4	**atm pvp VPI l2transport** **Example:** `Router(config-if)# atm pvp 10 l2transport`	Specifies the VPI of the PVP and configures the PVP in L2transport mode.
Step 5	**xconnect ip-address port-number encapsulation mpls one-to-one** **Example:** `Router(config-if-atm-l2trans-pvp)# xconnect 30.30.30.2 305 encapsulation mpls`	Binds an attachment circuit to the ATM IMA interface to create a pseudowire.

ATM AAL5 SDU VCC Transport

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM to another ATM. You must use AAL5 encapsulation for this transport type. Complete the following steps to configure an ATM AAL5 SDU VCC transport pseudowire:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface ATM0/IMA0`	Specifies the slot location and port of IMA interface group. • *slot*—Specifies the slot location of the ATM IMA port adapter. • *group-number*—Specifies the group number of the IMA group.

	Command or Action	Purpose
Step 4	**VPI/VCI l2transport** **Example:** `Router(config-if)# 100/12 l2transport`	Specifies the VPI and VCI and configures them in layer 2 transport mode.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if-atm-l2trans-)# encapsulation aal5`	Sets the encapsulation type to AAL5. AAL5 is the default l2transport encapsulation for the VCC mode.
Step 6	**xconnect ip-address port-number encapsulation mpls** **Example:** `Router(config-if-atm-l2trans-)# xconnect 25.25.25.25 125 encapsulation mpls`	Binds an attachment circuit to the ATM IMA interface to create a pseudowire.

Verifying IMA Configurations

To verify the IMA configurations, use the **show ima interface** command.

```
Router# show ima interface ATM0/IMA3
ATM0/IMA3 is up, ACTIVATION COMPLETE
Slot 0 Slot Unit 0 unit 3, CTRL VC -1, Vir -1, VC -1
IMA Configured BW 3022, Active BW 3022
IMA version 1.0, Frame length 64
Link Test: Disabled
Auto-Restart: Disabled
ImaGroupState: NearEnd = operational, FarEnd = operational
ImaGroupFailureStatus = noFailure
IMA Group Current Configuration:
ImaGroupMinNumTxLinks = 1 ImaGroupMinNumRxLinks = 1
ImaGroupDiffDelayMax = 200 ImaGroupNeTxClkMode = independent(itc)
ImaGroupFrameLength = 64 ImaTestProcStatus = disabled
ImaGroupTestLink = None ImaGroupTestPattern = 0xFF
ImaGroupConfLink = 2 ImaGroupActiveLink = 2
IMA Link Information:
ID Link Link State - Ctlr/Chan/Prot Test Status Scrambling
---- -------------- ------------------------------ --------------- ------------
0 T1 0/0 Up Up Up Up disabled Off
1 T1 0/1 Up Up Up Up disabled Off
```

How to Configure ATM Class of Service

This section describes how to configure ATM class of services:

Configuring Constant Bit Rate

Complete the following steps to configure Constant Bit Rate (CBR) QoS class for an ATM PVC and to specify the bandwidth on the Cisco ASR 901 series router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface ATM1/IMA0`	Configures an ATM interface and enters the interface configuration mode.
Step 4	**pvc** *VPI/VCI* **l2transport** **Example:** `Router(config-if)# 100/12 l2transport`	Specifies the VPI and VCI of the PVC and configures the PVC in Layer 2 transport mode. • **l2transport** is an optional keyword.
Step 5	**cbr** *rate* **Example:** `Router(config-if-atm-vc)# cbr 16000`	Configures the constant bit rate (CBR) QoS class for an ATM permanent virtual circuit () and specifies the bandwidth. • *rate*—Peak cell rate in Kbps.

Configuring Unspecified Bit Rate

Complete the following steps to configure Unspecified Bit Rate (UBR) QoS class for an ATM permanent virtual circuit () and to specify the bandwidth on the Cisco ASR 901 series Router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface ATMslot/IMAgroup-number** **Example:** `Router(config)# interface ATM1/IMA0`	Configures an ATM interface and enters the interface configuration mode.
Step 4	**pvc VPI/VCI l2transport** **Example:** `Router(config-if)# pvc 100/12 l2transport`	Specifies the VPI and VCI of the PVC and configures the PVC in layer 2 transport mode. • l2transport is an optional field.
Step 5	**ubr rate** **Example:** `Router(config-if-atm-vc)# ubr 16000`	Configures the UBR QoS class for an ATM permanent virtual circuit (PVC) and specifies the bandwidth. By default a value is set to UBR ATM class of service with the rate equal to the bandwidth of the IMA interface, which in turn is a product of the number of active IMA links and the bandwidth of each link. • *rate*—Peak cell rate in Kbps.

Configuring Unspecified Bit Rate Plus

Complete the following steps to configure Unspecified Bit Rate Plus (UBR+) QoS class for an ATM permanent virtual circuit () and to specify the bandwidth on the Cisco ASR 901 series Router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface ATMslot/IMAgroup-number** **Example:**	Configures an ATM interface and enters the interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface ATM1/IMA0`	
Step 4	**pvc VPI/VCI l2transport** **Example:** `Router(config-if)# pvc 100/12 l2transport`	Specifies the VPI and VCI of the PVC and configures the PVC in layer 2 transport mode. • l2transport is an optional field.
Step 5	**ubr+ pcr-rate mcr-rate** **Example:** `Router(config-if-atm-vc)# ubr+ 16000 2000`	Configures the UBR+ QoS class for an ATM permanent virtual circuit () and specifies the bandwidth. • *pcr-rate*—Peak cell rate in Kbps. • mcr-rate—Peak cell rate in Mbps

Configuring Variable Bit Rate for Real/Non-Real Time Traffic

Complete the following steps to configure the real/non-real time Variable Bit Rate for VoATM voice connections for an ATM on the Cisco ASR901 series Router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface ATMslot/IMAgroup-number** **Example:** `Router(config)# interface ATM1/IMA0`	Configures an ATM interface and enters the interface configuration mode.
Step 4	**pvc VPI/VCI l2transport** **Example:** `Router(config-if)# pvc 100/12 l2transport`	Specifies the VPI and VCI of the PVC and configures the PVC in layer 2 transport mode. • l2transport is an optional field.
Step 5	Do one of the following: • **vbr-rt peak-rate average-rate burst** •	Configures the real-time VBR for VoATM voice connections for an ATM in virtual circuit configuration mode.

	Command or Action	Purpose

	•
	•
	•
	• **vbr-nrt peak-rate average-rate burst**
	Example:
	`Router(config-if-atm-vc)# vbr-rt 600 300 37`
	Example:
	Example:
	`Router(config-if-atm-vc)# vbr-nrt 600 300 37`
		Configures the non-real time VBR for VoATM voice connections for an ATM in virtual circuit configuration mode.
		• *peak-rate*—Peak cell rate in Kbps.
		• average-rate—Average cell rate in Kbps.
		• burst—Burst cell size in number of cells. Minimum cell size is 37.

Configuration Examples

This section provides sample configuration examples for IMA on the Cisco ASR 901 Router:

Example: Creating an IMA Interface

The following is a sample configuration to create an IMA interface with T1 controller.

```
!
controller t1 0/0
 ima-group 0
exit
!
```

The following is a sample configuration to create an IMA interface with E1 controller.

```
controller e1 0/0
 ima-group 0
exit
!
```

Example: Configuring a Port Mode Pseudowire

```
The following is a sample configuration of a port mode pseudowire.
!
interface ATM0/IMA2
 no ip address
 xconnect 10.10.10.10 20 encapsulation mpls
!
```

Example: Configuring an N-to-1 VCC Cell Mode

```
The following is a sample configuration of N-to-1 VCC cell mode:
!
interface ATM0/IMA0
 no ip address
```

```
 atm mcpt-timers 500 600 700
 no atm enable-ilmi-trap
  100/100 l2transport
  cell-packing 10 mcpt-timer 2
  encapsulation aal0
  xconnect 25.25.25.25 125 encapsulation mpls
!
```

The following is a sample configuration for AAL5 SDU mode:

```
!
interface ATM0/IMA0
 no ip address
 no atm enable-ilmi-trap
  100/100 l2transport
  encapsulation aal5
  xconnect 25.25.25.25 125 encapsulation mpls
!
```

Example: Configuring an N-to-1 VPC Cell Mode

```
The following is a sample configuration of N-to-1 Permanent Virtual Circuit (VPC) cell mode.
!
interface ATM0/IMA0
 no ip address
 atm pvp 12 l2transport
 xconnect 30.30.30.30 30 encapsulation mpls
!
```

Example: Configuring CBR

The following is a sample configuration of constant bit rate.

```
!
interface atm0/ima0
  1/200 l2transport
  cbr 16000
!
```

Example: Configuring UBR

The following is a sample configuration of constant bit rate.

```
!
interface atm0/ima0
  1/200 l2transport
  ubr 16000
!
```

Example: Configuring UBR Plus

```
!
interface atm0/ima0
  1/200 l2transport
  ubr+ 16000 2000
!
```

Example: Configuring VBR for Real Time Traffic

```
!
interface atm0/ima0
  1/200 l2transport
  vbr-rt 10000 5000 37
!
```

Example: Configuring VBR for Non-Real Time Traffic

```
!
interface atm0/ima0
  1/200 l2transport
  vbr-nrt 10000 5000 50
!
```

Configuring Marking MPLS Experimental Bits

You can configure MPLS through the following procedures:

Creating a Policy-map for PVP/PVC/ATM IMA Interface

To configure a policy map, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**policy-map policy-map-name** **Example:** `Router(config)# policy-map mark_qosgroup`	Specifies a name for the policy map.
Step 4	**class class-name** **Example:** `Router(config-if)# class class-default`	Specifies a name for the class associated with the policy map.

	Command or Action	Purpose
Step 5	set qos-group qos-group-number **Example:** `Router(config-if)# set qos-group 2`	Sets a group to the policy map.

Applying the Policy-map

You can apply a policy map on the following interfaces:

Applying a Policy map on PVC and PVP

To apply a policy map on PVC and PVP, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface atm0/ima0`	Specifies the slot location and port of IMA interface group and configures the ATM interface. • *slot*—Specifies the slot location of the ATM IMA port adapter. • *group-number*—Specifies the group number of the IMA group.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 5	**no atm enable-ilmi-trap** **Example:** `Router(config-if)# no atm enable-ilmi-trap`	Disables the ILMI trap parameters.

	Command or Action	Purpose
Step 6	**pvc VPI/VCI l2transport** **Example:** `Router(config-if)# pvc 100/100 l2transport`	Specifies the VPI and VCI of the PVC and configures the PVC in layer 2 transport mode.
Step 7	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation aal0`	Sets the PVC encapsulation type to AAL0.
Step 8	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input mark_qosgroup`	Attaches a policy map to the input interface.
Step 9	**xconnect ip-address port-number encapsulation mpls** **Example:** `Router(config-if)# xconnect 25.25.25.25 125 encapsulation mpls`	Binds an attachment circuit to the ATM IMA PVC to create a pseudowire.
Step 10	**atm pvp VPI l2transport** **Example:** `Router(config-if)# atm pvp 200 l2transport`	Specifies the VPI of the PVP and configures the PVP in layer 2 transport mode.
Step 11	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input mark_qosgroup`	Attaches a policy map to the input interface.
Step 12	**xconnect ip-address port-number encapsulation mpls** **Example:** `Router(config-if)# xconnect 25.25.25.25 126 encapsulation mpls`	Binds an attachment circuit to the ATM IMA PVP to create a pseudowire.

Applying a Policy map on ATM IMA Interface

To apply a policy map on ATM IMA interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ATMslot/IMAgroup-number* **Example:** `Router(config)# interface atm0/ima0`	Specifies the slot location and port of IMA interface group and configures the ATM interface. • *slot*—Specifies the slot location of the ATM IMA port adapter. • *group-number*—Specifies the group number of the IMA group.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables the IP address configuration for the physical layer interface.
Step 5	**no atm enable-ilmi-trap** **Example:** `Router(config-if)# no atm enable-ilmi-trap`	Disables the ILMI trap parameters.
Step 6	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input mark_qosgroup`	Attaches a policy map to the input interface.
Step 7	**xconnect ip-address port-number encapsulation mpls** **Example:** `Router(config-if)# xconnect 25.25.25.25 125 encapsulation mpls`	Binds an attachment circuit to the ATM IMA interface to create a pseudowire.

Creating a Table-map

To create a table map for mapping QoS group to MPLS experimental bit, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**table-map table-name** **Example:** `Router(config)# table-map qos_exp_table`	Creates a table map with the specified name.
Step 4	**map from from-value to to-value** **Example:** `Router(config-if)# map from 1 to 2`	Maps the values associated with the policy map.

Creating a Policy-map for SVI Interface

To create a policy-map, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**policy-map map-name** **Example:**	Specifies the name of the existing policy map.

	Command or Action	Purpose
	`Router(config)# policy-map pmap_qos_exp`	
Step 4	**class class-default** **Example:** `Router(config)# class class-default`	Specifies the name of the class associated with the policy map.
Step 5	set mpls experimental topmost qos-group table table-map-name **Example:** `Router(config-if)# set mpls experimental topmost qos-group table qos_exp_table`	Copies the MPLS EXP value in the incoming MPLS traffic to the Qos group table.

Applying a Service Policy on SVI Interface

To apply a service policy on SVI interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-type* **Example:** `Router(config)# interface vlan10`	Specifies the interface type and enters the interface configuration mode.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 9216`	Configures the IP maximum transmission unit (MTU) size for the tunnel. • *bytes*—The range is from 1500 to 9216. The default is 1500.
Step 5	**ip address** *ip-address subnet-mask* **Example:**	Configures an IP address and subnet mask on the interface.

	Command or Action	Purpose
	`Router(config-if)# ip address 9.0.54.9 255.255.255.0`	
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for the interface.
Step 7	**service-policy output policy-map-name** **Example:** `Router(config-if)# service-policy output pmap_qos_exp`	Attaches the specified policy map to the output interface.

Additional References

The following sections provide references related to inverse multiplexing over ATM.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
IMA-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Inverse Multiplexing over ATM

Table 42: Feature Information for Inverse Multiplexing over ATM, on page 690 lists the features in this module and provides links to specific configuration information.

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 Table 42: Feature Information for Inverse Multiplexing over ATM, on page 690 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 42: Feature Information for Inverse Multiplexing over ATM

Feature Name	Releases	Feature Information
Inverse Multiplexing over ATM	15.2(2)SNH1	This feature was introduced. See the following links for more information about this feature: • How to Configure IMA, on page 670 • Configuring ATM IMA on T1/E1 Interface, on page 670 • Configuring ATM IMA over MPLS, on page 672 • How to Configure ATM Class of Service, on page 677 • Configuring Marking MPLS Experimental Bits, on page 683

CHAPTER 38

IPv6 over MPLS: 6PE and 6VPE

This feature module describes how to implement IPv6 VPN Provider Edge Transport over MPLS (IPv6 on Provider Edge Routers [6PE] and IPv6 on VPN Provider Edge Routers [6VPE]) on the Cisco ASR 901 Series Aggregation Services Routers.

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 table at the end of this module.

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

- Cisco IOS Release 15.2(2)SNI or a later release that supports the IPv6 over MPLS: 6PE and 6VPE feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- Multiprotocol Label Switching (MPLS) in provider backbone devices.
- MPLS with Virtual Private Network (VPN) code in provider devices with VPN provider edge (PE) devices.
- Border Gateway Protocol (BGP) in all devices providing a VPN service.

- Cisco Express Forwarding switching in every MPLS-enabled device.

Restrictions

The following restrictions are applicable for the IPv6 over MPLS: 6PE and 6VPE feature on the Cisco IOS Release 15.2(2)SNI.

- All the existing MPLS and IPv6 restrictions are applicable, as the base infrastructure of IPv6 and IPv4 MPLS remains the same.
- 6PE and 6VPE is supported only on the SVI interfaces.
- The number of global VRFs supported is the same as that of IPv4, as both the IPv4 and IPv6 VPN Routing and Forwarding (VRF) share the resources from the global VRF pool.
- The number of IPv6 VRFs supported is restricted to 113, though the maximum number of configurable VRFs are 127.
- For the single label per prefix mode allocation, the 6PE and 6VPE scale is limited by the number of labels available in the box (4000 labels).
- Supports only static routes and BGP for IPv6 in VRF context.

Feature Overview

The IPv6 over MPLS: 6PE and 6VPE feature enables the service providers running an MPLS/IPv4 infrastructure to offer IPv6 services without any major changes in the infrastructure. This feature offers the following options to the service providers:

- Connect to other IPv6 networks accessible across the MPLS core
- Provide access to IPv6 services and resources that service provider provides
- Provide IPv6 VPN services without going for complete overhaul of existing MPLS/IPv4 core

6PE and 6VPE uses the existing MPLS/IPv4 core infrastructure for IPv6 transport. It enables IPv6 sites to communicate with each other over an MPLS/IPv4 core network using MPLS label switched paths (LSPs).

This feature relies heavily on multiprotocol Border Gateway Protocol (BGP) extensions in the IPv4 network configuration on the provider edge (PE) router to exchange IPv6 reachability information (in addition to an MPLS label) for each IPv6 address prefix. Edge routers are configured as dual-stack, running both IPv4 and IPv6, and use the IPv4 mapped IPv6 address for IPv6 prefix reachability exchange.

Benefits of 6PE and 6VPE

6PE and 6VPE offers the following benefits to service providers:

- Minimal operational cost and risk—No impact on existing IPv4 and MPLS services.
- Only provider edge routers require upgrade—A 6PE and 6VPE router can be an existing PE router or a new one dedicated to IPv6 traffic.
- No impact on IPv6 customer edge (CE) routers—The ISP can connect to any CE router running Static, IGP or EGP.
- Production services ready—An ISP can delegate IPv6 prefixes.
- IPv6 introduction into an existing MPLS service—6PE and 6VPE routers can be added at any time.

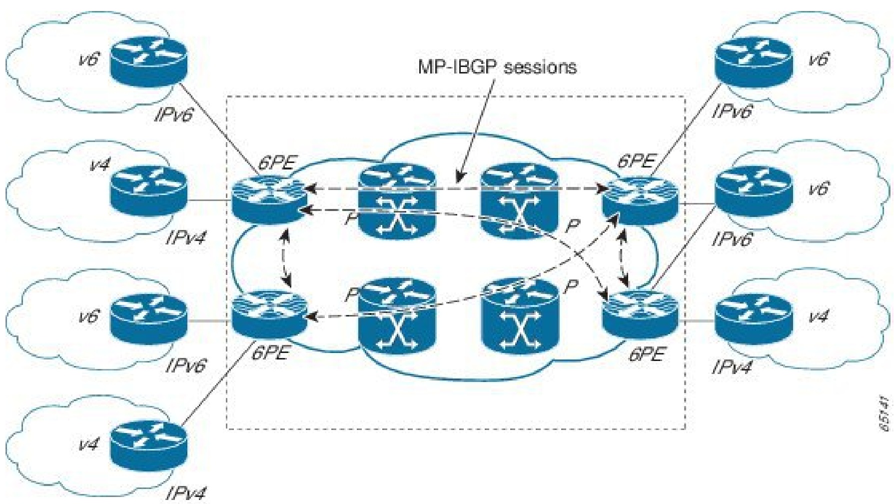
IPv6 on Provider Edge Routers

6PE is a technique that provides global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices. 6PE allows IPv6 domains to communicate with one another over the IPv4 without an explicit tunnel setup, requiring only one IPv4 address per IPv6 domain.

While implementing 6PE, the provider edge routers are upgraded to support 6PE, while the rest of the core network is not touched (IPv6 unaware). This implementation requires no reconfiguration of core routers because forwarding is based on labels rather than on the IP header itself. This provides a cost-effective strategy for deploying IPv6.The IPv6 reachability information is exchanged by PE routers using multiprotocol Border Gateway Protocol (mp-iBGP) extensions.

6PE relies on mp-iBGP extensions in the IPv4 network configuration on the PE router to exchange IPv6 reachability information in addition to an MPLS label for each IPv6 address prefix to be advertised. PE routers are configured as dual stacks, running both IPv4 and IPv6, and use the IPv4 mapped IPv6 address for IPv6 prefix reachability exchange. The next hop advertised by the PE router for 6PE and 6VPE prefixes is still the IPv4 address that is used for IPv4 L3 VPN routes. A value of ::FFFF: is prepended to the IPv4 next hop, which is an IPv4-mapped IPv6 address.

The following figure illustrates the 6PE topology.



V6	IPv6 router on the customer premises	6PE	PE equipment, connected to CEs and entry points to the MPLS clouds, running a dual stack IPv6/IPv4 (IPv6 to communicate with CEs)
V4	IPv4 router on the customer premises	P	Provider routers, core of the MPLS backbone running MPLS and IPv4 stack

IPv6 on VPN Provider Edge Routers

6VPE is a mechanism to use the IPv4 backbone to provide VPN IPv6 services. It takes advantage of operational IPv4 MPLS backbones, eliminating the need for dual-stacking within the MPLS core. This translates to savings in operational costs and addresses the security limitations of the 6PE approach. 6VPE is more like a regular IPv4 MPLS-VPN provider edge, with an addition of IPv6 support within VRF. It provides logically separate routing table entries for VPN member devices.

Components of MPLS-based 6VPE Network

- VPN route target communities – A list of all other members of a VPN community.
- Multiprotocol BGP (MP-BGP) peering of VPN community PE routers – Propagates VRF reachability information to all members of a VPN community.
- MPLS forwarding – Transports all traffic between all VPN community members across a VPN service-provider network.

In the MPLS-VPN model a VPN is defined as a collection of sites sharing a common routing table. A customer site is connected to the service provider network by one or more interfaces, where the service provider associates each interface with a VPN routing table–known as the VRF table.

For more conceptual information on 6PE and 6VPE, see the IPv6 VPN over MPLS guide in the MPLS: Layer 3 VPNs Configuration Guide.

Supported Features

The following 6PE and 6VPE features are supported on the Cisco ASR 901 router effective with Cisco IOS Release 15.2(2) SNI:

- IPv6 VRF support – Enabled for supporting 6VPE
- MPLS VPN 6VPE and 6PE – Provides IPV6 reachability for IPv6 edge routers across an MPLS network backbone running an IPv4 control plane, without making changes to the software on the MPLS P routers.
- 6VPE and 6PE with QoS – Supports QoS provisioning in 6PE and 6VPE networks by using existing QoS infrastructure and configuration.
- MPLS VPN - VRF command for IPv4 and IPv6 VPN – Supports commands that allows users to enable IPv4 and IPv6 in the same VRF.

Note All the above features are built upon existing IPv4, IPv6, MPLS and BGP infrastructure in the IOS and Cisco ASR 901 data plane support.

Scalability Numbers

Table 43: Scalability Numbers for 6PE and 6VPE , on page 694 shows the scalability numbers for the 6PE and 6VPE feature.

Table 43: Scalability Numbers for 6PE and 6VPE

Interface	Numbers
Number of VRFs	113
Number of VPNv6 prefixes per VRF	About 4000 [3]
Number of VPNv6 prefixes	About 4000 Table 43: Scalability Numbers for 6PE and 6VPE , on page 694

Interface	Numbers
Number of global IPv6 prefixes	About 4000 Table 43: Scalability Numbers for 6PE and 6VPE , on page 694

[3] This number is limited by the MPLS label usage on the PE router. The maximum number of label space shared between IPv4 and IPv6 is 4000.

How to Configure IPv6 over MPLS: 6PE and 6VPE

This section describes how to configure IPv6 over MPLS: 6PE and 6VPE feature:

Configuring 6PE

Ensure that you configure 6PE on PE routers participating in both the IPv4 cloud and IPv6 clouds. To learn routes from both clouds, you can use any routing protocol supported on IOS (BGP, OSPF, IS-IS, EIGRP, Static).

BGP running on a PE router should establish (IPv4) neighborhood with BGP running on other PEs. Subsequently, it should advertise the IPv6 prefixes learnt from the IPv6 table to the neighbors. The IPv6 prefixes advertised by BGP would automatically have IPv4-encoded-IPv6 addresses as the nexthop-address in the advertisement.

To configure 6PE, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding on the router.
Step 4	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables Cisco Express Forwarding for IPv6.

	Command or Action	Purpose
Step 5	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 6	**router bgp** *as-number* **Example:** `Router(config)# router bgp 100`	Enters the number that identifies the autonomous system (AS) in which the router resides. • *as-number*—Autonomous system number. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.
Step 7	**no synchronization** **Example:** `Router(config-router)# no synchronization`	Advertises a network route without waiting for IGP.
Step 8	**no bgp default ipv4-unicast** **Example:** `Router(config-router)# no bgp default ipv4-unicast`	Disables the default IPv4 unicast address family for peering session establishment.
Step 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **Example:** `Router(config-router)# neighbor 10.108.1.2 remote-as 65200`	Adds an entry to the BGP or multiprotocol BGP neighbor table. • *ip-address*—IP address of a peer router with which routing information will be exchanged. • *ipv6-address*—IPv6 address of a peer router with which routing information will be exchanged. • *peer-group-name*—Name of the BGP peer group. • **remote-as**—Specifies a remote autonomous system. • *as-number*—Number of an autonomous system to which the neighbor belongs, ranging from 1 to 65535.
Step 10	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **Example:** `Router(config-router)# neighbor`	Configures BGP sessions to use any operational interface for TCP connections.

	Command or Action	Purpose
	`172.16.2.3` `update-source Loopback0`	
Step 11	**address-family ipv6** **Example:** `Router(config-router)# address-family ipv6`	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
Step 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.44 activate`	Enables the exchange of information with a BGP neighbor.
Step 13	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **Example:** `Router(config-router-af)# neighbor 10.0.0.44 send-label`	Sends MPLS labels with BGP routes to a neighboring BGP router.
Step 14	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits BGP address-family submode.

Configuring 6VPE

6VPE requires setting up of IPv6 connectivity from PE to CE routers, MP-BGP peering to the neighboring PE and MPLS/IPv4 connectivity to the core network using supported routing protocols (like OSPF, IS-IS, EIGRP, Static) as done in 6PE. In addition, IPv6 VRFs have to be created on the PE routers and attached to the interfaces connecting to CE routers. IPv6-only or dual-stack(multi-protocol) VRFs support IPv6 VRF definitions.

To configure 6VPE, perform the tasks given below:

Setting up IPv6 Connectivity from PE to CE Routers

To configure IPv6 connectivity from PE to CE routers, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables the privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**router bgp** **Example:** `Router(config)# router bgp 100`	Enters the number that identifies the autonomous system (AS) in which the router resides. Autonomous system number: Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.

Step 4	**address-family ipv6 [vrf** *vrf-name***]**
	
	Example:
	
	`Router(config-router)# address-family ipv6`
	`labeled-unicast`
		Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
		
		• **vrf**—(Optional) Specifies all VRF instance tables or a specific VRF table for an IPv6 address.
		• *vrf-name*—(Optional) A specific VRF table for an IPv6 address.

Step 5	**neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
	
	Example:
	
	`Router(config-router-af)# neighbor 10.108.1.2`
	`remote-as 65200`
		Adds an entry to the BGP or multiprotocol BGP neighbor table.
		
		• *ip-address* —IP address of a peer router with which routing information will be exchanged.
		• *ipv6-address* —IPv6 address of a peer router with which routing information will be exchanged.
		• *peer-group-name* —Name of the BGP peer group.
		• **remote-as** —Specifies a remote autonomous system.
		• *as-number*—Number of an autonomous system to which the neighbor belongs, ranging from 1 to 65535.

Step 6	**neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
	
	Example:
	
	`Router(config-router-af)# neighbor 10.0.0.44`
	`activate`
		Enables the exchange of information with a BGP neighbor.

	Command or Action	Purpose
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits the BGP address-family submode.

Setting up MP-BGP Peering to the Neighboring PE

To configure MP-BGP peering to the neighboring PE routers, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Router(config)# router bgp 100`	Enters the number that identifies the autonomous system (AS) in which the router resides. Autonomous system number. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535.
Step 4	**address-family vpnv6** **Example:** `Router(config-router)# address-family vpnv6`	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
Step 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** **Example:** `Router(config-router-af)# neighbor 10.0.0.44 activate`	Enable the exchange of information with a BGP neighbor.
Step 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community extended** **Example:**	Adds an entry to the BGP or multiprotocol BGP neighbor table.

	Command or Action	Purpose
	`Router(config-router-af)# neighbor 10.108.1.2 send-community extended`	
Step 7	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits the BGP address-family submode.

Setting up MPLS/IPv4 Connectivity with LDP

To configure MPLS and IPv4 connectivity with LDP, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *ip-address* **Example:** `Router(config)# interface vlan 100`	Configures an interface type and to enter interface configuration mode. • interface-name—Interface name.
Step 4	**ip address***ip-address* **Example:** `Router(config-if)# ip address 1.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IP packets along normally routed paths for a particular interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.

Creating IPv6 VRFs on PE Routers

To configure IPv6 VRFs on the PE routers, complete the following tasks:

Configuring IPv6-only VRF

To configure IPv6-only VRF, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition red`	Configures a VRF routing table instance and enters VRF configuration mode. • *vrf-name*—Name assigned to a VRF.
Step 4	**address-family ipv6** **Example:** `Router(config-vrf)# address-family ipv6`	Enters address family configuration mode for configuring routing sessions that use standard IPv6 address prefixes.
Step 5	**exit-address-family** **Example:** `Router(config-vrf-af)# exit-address-family`	Exits address-family submode.

Configuring Dual-stack VRF

To configure dual-stack VRF, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition red`	Configures a VRF routing table instance and enters VRF configuration mode. • *vrf-name*—Name assigned to a VRF.
Step 4	**address-family ipv4** **Example:** `Router(config-vrf)# address-family ipv4`	Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes.
Step 5	**exit-address-family** **Example:** `Router(config-vrf-af)# exit-address-family`	Exits address-family submode.
Step 6	**address-family ipv6** **Example:** `Router(config-vrf)# address-family ipv6`	Enters address family configuration mode for configuring routing sessions that use standard IPv6 address prefixes.
Step 7	**exit-address-family** **Example:** `Router(config-vrf-af)# exit-address-family`	Exits address-family submode.

Verifying IPv6 over MPLS: 6PE and 6VPE Configuration

To verify the IPv6 over MPLS: 6PE and 6VPE configuration, use the show commands shown in the following examples.

To display BGP entries from all of the customer-specific IPv6 routing tables, use the following show command.

```
Router# show bgp vpnv6 unicast all

Network                   Next Hop              Metric LocPrf    Weight Path
Route Distinguisher: 100:1
*  2001:100:1:1000::/56   2001:100:1:1000::72a    0               0     200 ?
*                         ::                0                      32768 ?
```

```
*  i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
*  2001:100:2:1000::/56   ::               0                       32768 ?
*  2001:100:2:2000::/56   ::FFFF:200.10.10.1      0                 32768 ?
```

To display the parameters and the current state of the active IPv6 routing protocol processes, use the following show command:

```
Router# show ipv6 protocols vrf vpe_1

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 100"
  IGP synchronization is disabled
  Redistribution:
    None
  Neighbor(s):
    Address                  FiltIn FiltOut Weight RoutemapIn RoutemapOut
    100::2
```

To display IPv6 router advertisement (RA) information received from on-link devices, use the following show command:

```
Router# show ipv6 route vrf vpe_1

IPv6 Routing Table - vpe_1 - 29 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   72::/64 [20/0]
     via 100::2
B   72:0:0:1::/64 [20/0]
     via 100::2
B   72:0:0:2::/64 [20/0]
     via 100::2
B   72:0:0:4::/64 [20/0]
     via 100::2
B   72:0:0:5::/64 [20/0]
     via 100::2
B   72:0:0:6::/64 [20/0]
     via 100::2
B   72:0:0:7::/64 [20/0]
     via 100::2
B   72:0:0:8::/64 [20/0]
     via 100::2
B   72:0:0:9::/64 [20/0]
     via 100::2
B   72:0:0:A::/64 [20/0]
     via 100::2
B   72:0:0:B::/64 [20/0]
     via 100::2
B   72:0:0:C::/64 [20/0]
     via 100::2
B   72:0:0:D::/64 [20/0]
     via 100::2
B   72:0:0:E::/64 [20/0]
     via 100::2
B   72:0:0:F::/64 [20/0]
     via 100::2
B   72:0:0:10::/64 [20/0]
```

```
     via 100::2
B   72:0:0:11::/64 [20/0]
     via 100::2
B   72:0:0:12::/64 [20/0]
     via 100::2
```

To display the Cisco Express Forwarding Forwarding Information Base (FIB) associated with an IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the following show command.

```
Router# show ipv6 cef vrf cisco1

2001:8::/64
  attached to GigabitEthernet0/0/1
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 GigabitEthernet0/1/0 label 22 19
 2010::/64
  nexthop 2001:8::1 GigabitEthernet0/0/1
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

To display IPv6 routing table information associated with a VPN routing and forwarding (VRF) instance, use the following show command.

```
Router# show ipv6 route vrf

IPv6 Routing Table cisco1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:8::/64 [0/0]
     via ::, GigabitEthernet0/0/1
L   2001:8::3/128 [0/0]
     via ::, GigabitEthernet0/0/1
B   2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B   2010::/64 [20/1]
     via 2001:8::1,
C   2012::/64 [0/0]
     via ::, Loopback1
L   2012::1/128 [0/0]
     via ::, Loopback1
```

To display label forwarding information for advertised Virtual Private Network (VPN) routing and forwarding (VRF) instance routes, use the following show command.

```
Router# show mpls forwarding-table vrf vpe_1

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
1760       No Label   72::/64[V]       0             Vl100      100::2
1761       No Label   72:0:0:1::/64[V] 0             Vl100      100::2
1762       No Label   72:0:0:2::/64[V] 0             Vl100      100::2
1764       No Label   72:0:0:3::/64[V] 0             Vl100      100::2
1765       No Label   72:0:0:4::/64[V] 0             Vl100      100::2
1768       No Label   72:0:0:7::/64[V] 0             Vl100      100::2
1769       No Label   72:0:0:8::/64[V] 0             Vl100      100::2
1770       No Label   72:0:0:9::/64[V] 0             Vl100      100::2
```

```
1771       No Label   72:0:0:A::/64[V] 0             Vl100      100::2
1772       No Label   72:0:0:B::/64[V] 0             Vl100      100::2
1773       No Label   72:0:0:C::/64[V] 0             Vl100      100::2
1774       No Label   72:0:0:D::/64[V] 0             Vl100      100::2
1775       No Label   72:0:0:E::/64[V] 0             Vl100      100::2
1776       No Label   72:0:0:F::/64[V] 0             Vl100      100::2
1777       No Label   72:0:0:10::/64[V]   \
                                   0             Vl100      100::2
1778       No Label   72:0:0:11::/64[V]   \
                                   0             Vl100      100::2
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
1779       No Label   72:0:0:12::/64[V]   \
                                   0             Vl100      100::2
1780       No Label   72:0:0:13::/64[V]   \
                                   0             Vl100      100::2
1781       No Label   72:0:0:14::/64[V]   \
                                   0             Vl100      100::2
1782       No Label   72:0:0:15::/64[V]   \
                                   0             Vl100      100::2
1783       No Label   72:0:0:16::/64[V]   \
                                   0             Vl100      100::2
1784       No Label   72:0:0:17::/64[V]   \
                                   0             Vl100      100::2
1785       No Label   72:0:0:18::/64[V]   \
                                   0             Vl100      100::2
```

To display output information linking the MPLS label with prefixes, use the following show command.

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes tag Outgoing       Next Hop
tag   tag or VC     or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop tag       192.168.99.64/30  0         GE0/0         point2point
20    Pop tag       192.168.99.70/32  0         GE0/0         point2point
21    Pop tag       192.168.99.200/32 0         GE0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

To display entries in the IPv6 BGP routing table, use the following show command:

```
Router# show bgp ipv6 2001:33::/64

BGP routing table entry for 2001:33::/64, version 3
Paths: (1 available, best #1, table Global-IPv6-Table)
 Not advertised to any peer
 Local
 ::FFFF:192.168.0.2 (metric 30) from 192.168.0.2 (192.168.0.2)
 Origin IGP, localpref 100, valid, internal, best
```

Configuration Examples

This section provides sample configuration examples for IPv6 over MPLS: 6PE and 6VPE feature on the Cisco ASR 901 router.

Example: Configuring 6PE

The following is a sample configuration of 6PE.

```
interface GigabitEthernet0/3/0/0
 ipv6 address 2001::1/64
!
router isis ipv6-cloud
 net 49.0000.0000.0001.00
 address-family ipv6 unicast
  single-topology
 interface GigabitEthernet0/3/0/0
  address-family ipv6 unicast
  !
!
router bgp 55400
 bgp router-id 54.6.1.1
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
  network 55:5::/64
  redistribute connected
  redistribute isis ipv6-cloud
   allocate-label all
 !
 neighbor 34.4.3.3
  remote-as 55400
  address-family ipv4 unicast
  !
  address-family ipv6 labeled-unicast
```

Example: Configuring 6VPE

The following is a sample configuration of 6VPE.

```
vrf vpn1
 address-family ipv6 unicast
  import route-target
   200:2
  !
  export route-target
   200:2
interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255
interface GigabitEthernet0/0/0/1
 vrf  vpn1
 ipv6 address 2001:c003:a::2/64
router bgp 1
 bgp router-id 10.0.0.1
 bgp redistribute-internal
 bgp graceful-restart
 address-family ipv4 unicast
!
address-family vpnv6 unicast
 !
 neighbor 10.0.0.2                >>>> Remote peer loopback address.
  remote-as 1
  update-source Loopback0
  address-family ipv4 unicast
  !
```

```
 address-family vpnv6 unicast
  route-policy pass-all in
  route-policy pass-all out
!
 vrf vpn1
  rd 100:2
  bgp router-id 140.140.140.140
  address-family ipv6 unicast
  redistribute connected
!
neighbor 2001:c003:a::1
  remote-as 6502
  address-family ipv6 unicast
  route-policy pass-all in
  route-policy pass-all out
```

Additional References

The following sections provide references related to IPv6 over MPLS: 6PE and 6VPE feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
IPv6 Provider Edge Router over MPLS	Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS
IPv6 VPN over MPLS	MPLS: Layer 3 VPNs Configuration Guide

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for IPv6 over MPLS: 6PE and 6VPE

Table 44: Feature Information for IPv6 over MPLS: 6PE and 6VPE, on page 708 lists the features in this module and provides links to specific configuration information.

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 Table 44: Feature Information for IPv6 over MPLS: 6PE and 6VPE, on page 708 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 44: Feature Information for IPv6 over MPLS: 6PE and 6VPE

Feature Name	Releases	Feature Information
IPv6 over MPLS: 6PE and 6VPE	15.2(2)SNI	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:

CHAPTER 39

Storm Control

This feature module describes the Storm Control feature that helps to monitor the incoming broadcast, multicast, and unknown unicast packets and prevent them from flooding the LAN ports.

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 table at the end of this module.

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 Storm Control

- Cisco IOS Release 15.3(3)S or a later release that supports the Storm Control feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.

Restrictions for Storm Control

- The storm-control command is not recommended on an interface that is part of a port channel.

- Storm-control counters are not supported on port channel as the counters are based on physical ports.
- Discarded counters are not displayed for port channel. You should check the port channel member-ports for discarded counters.
- The current rate field is not supported for show commands in hardware based storm control.
- Supports only drop counters. Total broadcast received in storm control is not supported.

Information About Storm Control

A traffic storm occurs when huge amount of broadcast, multicast, or unknown unicast packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can also cause a storm. The mechanism to prevent and control such events is known as storm control or broadcast suppression.

The Storm Control feature prevents switchports on a LAN from being disrupted by a broadcast, multicast, or unknown unicast storm on one of the interfaces. This feature monitors incoming traffic statistics over a time period and compares the measurement with a predefined suppression level threshold. The threshold represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, the system takes the appropriate storm control action until the incoming traffic falls below the threshold level.

Storm control also acts as a policer, and it drops only the storms that breaches the configured storm level.

This feature supports the following:

- Ethernet port: per port configuration for broadcast, multicast, and unknown unicast traffic.
- 10 GigabitEthernet interfaces.
- SNMP trap and SYSLOG messages: indicating storm control detection.
- Individual dropped packet counters: for broadcast, multicast, and unknown unicast flows.
- Error disable recovery feature with storm control shutdown action.

Configuring Storm Control

To configure Storm Control feature, complete the following steps:

Note This feature is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**storm-control {action {shutdown | trap}| {broadcast | multicast | unicast} {level {level | bps bps-level| pps pps-level}}** **Example:** `Router(config-if)# storm-control broadcast level 70`	Configures broadcast, multicast, or unknown unicast storm control. • **action**—Specifies the action to take when a storm occurs on a port. • **shutdown**—Disables the port during a storm. • **trap**—Sends an SNMP trap. • **broadcast**—Configures broadcast storm control. • **multicast**—Configures multicast storm control. • **unicast**—Configures unknown unicast storm control. • **level**—Specifies the rising threshold level for broadcast, multicast, or unicast traffic as a percentage of the bandwidth. • *level*—Threshold level. The valid range is from 1 to 100 percent. There can also be a fractional part in the level ranging from 0 to 99, which is expressed in percentage. So a level of 49.99 on a GigabitEthernet interface means that once the number of broadcast (or configured type) packets on the interface exceeds 499.90Mbps, all the exceeding packets are dropped. • **bps**—Specifies the suppression level in bits per second. • *bps-level*—Threshold level. • **pps**—Specifies the suppression level in packets per second. • *pps-level*—Threshold level.
Step 5	**end** **Example:**	Exits the interface configuration mode and enters the privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-if)# end`	

What to do next

> **Note** To disable Storm Control feature, use the no storm-control command.

Verifying Storm Control

To verify the Storm Control feature configuration, use the show command described in the following example.

```
Router# show storm-control broadcast
Interface   Type    Filter State  Level         Current
---------  ------  -------------  -----------  ----------
Gi0/1       Bcast   Forwarding     200 pps      0 pps
Gi0/1       Mcast   Forwarding     300 pps      0 pps
! The "current" field is not supported for storm control.
```

To verify the dropped counters, use the show command described in the following example.

```
Router# show interface gigabitethernet 0/1 counters storm-control
Port   UcastSupp UcastSuppDiscards McastSupp McastSuppDiscards BcastSupp BcastSuppDiscards
         %/ps                        %/ps                        %/ps
Gi0/1   100.00%   0                 20000p   1065163           100.00%   0
```

Configuring Error Disable Recovery

The Cisco ASR 901 router supports error disable recovery for traffic storm control. When a storm is detected, the interfaces configured with the shutdown action of the storm control command are brought down. By default, the error recovery is disabled. You can configure automatic recovery by enabling the error disable recovery at the global configuration level and by setting a time-interval for error recovery.

To configure error disable recovery, complete the following steps:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**errdisable recovery cause storm-control** **Example:** `Router(config)# errdisable recovery cause storm-control`	Configure recovery mechanism and recovery from a specific cause.
Step 4	**errdisable recovery interval** *seconds* **Example:** `Router(config)# errdisable recovery interval 30`	Configures the period to recover from a specified error-disable cause. • *seconds*—Specifies the time to recover from a specified error-disable cause.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters the privileged EXEC mode.

Monitoring Error Disable Recovery

To display the information about the error-disable recovery timer, use the show command described in the following example.

```
Router# show errdisable recovery

ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
lsgroup              Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
mac-limit            Disabled
unicast-flood        Disabled
storm-control        Enabled
arp-inspection       Disabled
loopback             Disabled
link-monitor-fail    Disabled
oam-remote-failur    Disabled
oam-remote-failur    Disabled
oam-remote-failur    Disabled
dot1ad-incomp-ety    Disabled
dot1ad-incomp-tun    Disabled
mlacp-minlink        Disabled
```

```
Timer interval: 30 seconds
Interfaces that will be enabled at the next timeout:
Interface       Erdisable reason      Time left(sec)
----------    ---------------------    --------------
   Gi0/3            storm-control            4
```

Configuration Example for Storm Control

The following is a sample configuration of Storm Control feature on the Cisco ASR 901 router.

```
!
interface GigabitEthernet0/1
no ip address
negotiation auto
storm-control broadcast level pps 200
storm-control multicast level pps 300
storm-control action trap
end
!
```

Troubleshooting Tips for Storm Control

Use the following debug command to enable the debug feature to help in troubleshooting the storm control feature.

```
Router# debug platform hardware ether SC
```

Additional References

The following sections provide references related to Storm Control feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Storm Control

Table 45: Feature Information for Storm Control, on page 715 lists the features in this module and provides links to specific configuration information.

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 Table 45: Feature Information for Storm Control, on page 715 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 45: Feature Information for Storm Control

Feature Name	Releases	Feature Information
Storm Control	15.3(3)S	This feature was introduced on the Cisco ASR 901 routers. The following section provides information about this feature:

CHAPTER 40

Remote Loop-Free Alternate - Fast Reroute

This feature module describes the Remote Loop-free Alternate (LFA) - Fast Reroute (FRR) feature that uses a backup route, computed using dynamic routing protocol during a node failure, to avoid traffic loss.

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 table at the end of this module.

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 Remote Loop-Free Alternate - Fast Reroute

- Cisco IOS Release 15.2(2)SNI or a later release that supports the Remote LFA-FRR feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You should enable the following commands at the global configuration mode before configuring the Remote LFA-FRR feature.
    - asr901-platf-frr enable
    - mpls label protocol ldp
    - mpls ldp router-id *loopback-id* force
    - mpls ldp discovery targeted-hello accept

  - no l3-over-l2 flush buffers

- Your network must support the following Cisco IOS features before you can enable fast reroute link protection:
  - IP Cisco Express Forwarding (CEF)
  - Multiprotocol Label Switching (MPLS)
- Your network must also support at least one of the following protocols:
  - Intermediate System-to-Intermediate System (IS-IS)
  - Open Shortest Path First (OSPF)
- You should use throttle interior gateway protocol (IGP) timers for IS-IS and OSPF protocols.

Restrictions for Remote Loop-Free Alternate - Fast Reroute

- 4-label push is not supported. Due to this limitation, Labeled BGP access (RFC 3107) with Remote LFA-FRR/TE-FRR is not supported, if it exceeds three labels. Four label push is observed on L2VPN and L3VPN scenarios where multihop tunnel terminates before the destination. The four labels are given below:
  - Backup-Repair Label
  - Tunnel Label
  - MPLS LDP Label
  - VC or VRF Label
- Since FRR is a software based solution on the Cisco ASR 901 router, you should keep the number of prefixes, label-entries, and pseudowires to a minimum to obtain good convergence numbers.
- Remote LFA-FRR is not supported on layer 3 over layer 2 deployments. Disable this configuration using the no l3-over-l2 flush buffers command before configuring Remote LFA-FRR.
- Ethernet over Multiprotocol Label Switching (EoMPLS) redundancy is not useful unless you have dual home pseudowire and a protecting backup pseudowire egress link with FRR.
- Psuedowire redundancy over RLFA is supported effective with Cisco IOS Realease 15.4(1)S.
- TDM psuedowires over RLFA is supported effective with Cisco IOS Realease 15.3(3)S.
- CFM over Xconnect over TE-FRR is not supported.
- The imposition statistics do not work for EoMPLS after the FRR event or layer 3 cutover.
- The Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) edge is not supported. Specifically, the bgp additional-paths install command is not supported.
- If the network port is an LAG interface (etherchannel), you must use BFD over SVI to achieve FRR convergence numbers.
- If the LAG interface is used either on access side or towards the core, you should shutdown the interface before removing it.

Feature Overview

The LFA-FRR is a mechanism that provides local protection for unicast traffic in IP, MPLS, EoMPLS, Inverse Multiplexing over ATM (IMA) over MPLS, Circuit Emulation Service over Packet Switched Network (CESoPSN) over MPLS, and Structure-Agnostic Time Division Multiplexing over Packet (SAToP) over MPLS networks. However, some topologies (such as the ring topology) require protection that is not afforded by LFA-FRR alone. The Remote LFA-FRR feature is useful in such situations.

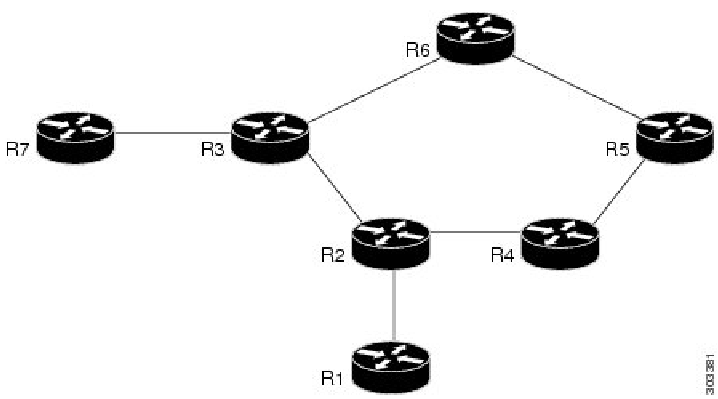
The Remote LFA-FRR extends the basic behavior of LFA-FRR to any topology. It forwards the traffic around a failed node to a remote LFA that is more than one hop away.

In Remote LFA-FRR, a node dynamically computes its LFA node. After determining the alternate node (which is non-directly connected), the node automatically establishes a directed Label Distribution Protocol (LDP) session to the alternate node. The directed LDP session exchanges labels for the particular forward error correction (FEC).

When the link fails, the node uses label stacking to tunnel the traffic to the remote LFA node, to forward the traffic to the destination. All the label exchanges and tunneling to remote LFA node are dynamic in nature and pre-provisioning is not required.

The following figure shows the repair path that is automatically created by the Remote LFA-FRR feature to bypass looping. In this figure, the traffic is flowing between CE nodes (R1 to R7) through the PE nodes (protected link - R2 and R3). When the PE node fails, the repair path (R2 - R4- R5 - R6 - R3) is used to route the traffic between CE nodes.

Figure 40: Remote LFA-FRR Link Protection



R1 and R7	CE nodes	R6 - R5 - R4	P nodes
R2 and R3	PE nodes (protected link)	R2 - R4- R5 - R6 - R3	Fast Reroute Repair Path

Benefits of Remote LFA-FRR

- Simplifies operation with minimum configuration
- Eliminates additional traffic engineering (TE) protocols.
- Computes PQ node dynamically without any manual provisioning (PQ node is a member of both the extended P-space and the Q-space. P-space is the set of routers reachable from a specific router without any path (including equal cost path splits) transiting the protected link. Q-space is the set of routers from

which a specific router can be reached without any path, including equal cost path splits, transiting the protected link.)

- Prevents hair pinning that occurs in TE-FRR
- Remote LFA-FRR supports the following:
  - Basic LFA-FRR (supported for OSPF and IS-IS protocols)
  - IP, L2VPN, and L3VPN
  - BFD triggered MPLS TE-FRR. Supports BFD sessions with 50ms interval.

Avoiding Traffic Drops

Traffic drops can occur due to congestion as a result of formation of micro loops during link recovery. To avoid traffic drops, the tunnel-buffer port command is introduced to set the hardware buffer values on the port. For more details on this command, see the Cisco ASR 901 Series Aggregation Services Router Command Reference guide.

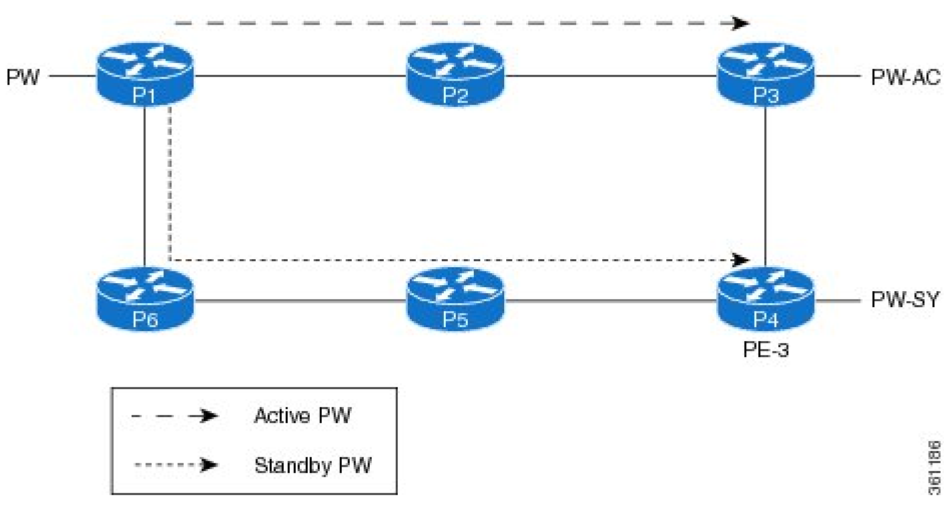
Pseudowire Redundancy over FRR

Pseudowire redundancy enables you to configure a pseudowire as a backup for the primary pseudowire. When the primary pseudowire fails, the services are switched to the backup pseudowire. Effective with Cisco IOS Release 15.4(1)S, Pseudowire Redundancy over FRR feature is supported.

You can enable FRR (TE-FRR and RLFA) in the network for both active and standby pseudowires separately. The primary and backup paths for these virtual circuits (VCs) may or may not overlap. This feature supports link failures through FRR and node failures through PW redundancy. It supports up to 500 primary and backup pseudowires.

The following figure shows the pseudowire redundancy over FRR implementation.

Figure 41: Pseudowire Redundancy Over FRR



Conditions for Switchover

- If the primary path to the peer node goes down for active VC, the FRR changes to backup and the VC remains active.

- A VC switchover does not occur unless both primary and backup paths are down for active VC.
- The standby VC does not go down until both primary and backup paths to the standby peer are down.
- A VC switchover occurs when the peer node of the active VC reboots or when the access circuit goes down.
- If the peer node of active VC reboots when the standby VC is in backup state, the VC switchover occurs immediately and the standby VC becomes active.

How to Configure Remote Loop-Free Alternate - Fast Reroute

Note Effective with Cisco IOS Release 15.3(3)S, the Remote LFA-FRR feature is supported on CESoPSN, SAToP, and ATM/IMA.

- Effective with Cisco IOS Release 15.4(1)S, the Pseudowire Redundancy over FRR feature is supported.

This section describes how to configure Remote LFA-FRR feature:

Configuring Remote LFA-FRR for IS-IS

To configure Remote LFA-FRR for the IS-IS routing process, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables automatic negotiation.

	Command or Action	Purpose
Step 5	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 7 ethernet`	Configures an Ethernet service instance on an interface. • *id* —Integer that uniquely identifies a service instance on an interface.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if)# encapsulation dot1q 7`	Enables IEEE 802.1Q encapsulation of traffic on a specified interface in a VLAN. • *vlan-id*—Virtual LAN identifier.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. • **pop**—Removes a tag from a packet. • **1** —Specifies the outermost tag for removal from a packet. • **symmetric**—Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
Step 8	**bridge-domain** *bridge-domain-id* **Example:** `Router(config-if)# bridge-domain 7`	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). • *bridge-domain-id*—Bridge domain identifier.
Step 9	**interface vlan** *bridge-domain-id* **Example:** `Router(config-if)# interface vlan 7`	Configures an Ethernet interface to create or access a dynamic Switch Virtual Interface (SVI).
Step 10	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 7.7.7.1 255.255.255.0`	Specifies an IP address for the specified interface.
Step 11	**ip router isis** **Example:** `Router(config-if)# ip router isis`	Configures an IS-IS routing process for an IP on an interface.

	Command or Action	Purpose
Step 12	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
Step 13	**isis network point-to-point** **Example:** `Router(config-if)# isis network point-to-point`	Configures a network of two networking devices that use the integrated IS-IS routing protocol to function as a point-to-point link.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode and enters the global configuration mode.
Step 15	**router isis** **Example:** `Router(config)# router isis`	Enables the IS-IS routing protocol and enters the router configuration mode.
Step 16	**fast-reroute per-prefix {level-1 | level-2} {all | route-map** *route-map-name***}** **Example:** `Router(config-router)# fast-reroute per-prefix level-1 all`	Configures an FRR path that redirects traffic to a remote LFA tunnel for either level 1 or level 2 packets. • **level-1**—Enables per-prefix FRR of level 1 packets. • **level-2**—Enables per-prefix FRR of level 2 packets. • **all**—Enables FRR of all primary paths. • **route-map**—Specifies the route map for selecting primary paths for protection. • *route-map-name*—Route map name.
Step 17	**fast-reroute remote-lfa {level-1 | level-2} mpls-ldp [maximum-metric** *metric-value***]** **Example:** `Router(config-router)# fast-reroute remote-lfa level-1 mpls-ldp`	Configures an FRR path that redirects traffic to a remote LFA tunnel. • **level-1**—Enables LFA-FRR of level 1 packets. • **level-2**—Enables LFA-FRR of level 2 packets. • **mpls-ldp**—Specifies that the tunnel type is MPLS or LDP. • **maximum-metric**—Specifies the route map for selecting primary paths for protection. • *metric-value*—Metric value.

	Command or Action	Purpose
Step 18	**mpls ldp sync** **Example:** `Router(config-router)# mpls ldp sync`	Enables MPLS LDP synchronization on interfaces for an IS-IS process.
Step 19	**mpls ldp igp sync holddown** *milliseconds* **Example:** `Router(config)# mpls ldp igp sync holddown 1000`	Specifies how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) synchronization to be achieved. • *milliseconds*—Peer host name or IP address.

Configuring Remote LFA-FRR for OSPF

To configure Remote LFA-FRR for the OSPF routing process, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables automatic negotiation.
Step 5	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 7 ethernet`	Configures an Ethernet service instance on an interface. • *id* —Integer that uniquely identifies a service instance on an interface.

	Command or Action	Purpose
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if)# encapsulation dot1q 7`	Enables IEEE 802.1Q encapsulation of traffic on a specified interface in a VLAN. • *vlan-id*—Virtual LAN identifier.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. • **pop**—Removes a tag from a packet. • **1** —Specifies the outermost tag for removal from a packet. • **symmetric**—Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
Step 8	**bridge-domain** *bridge-domain-id* **Example:** `Router(config-if)# bridge-domain 7`	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). • *bridge-domain-id*—Bridge domain identifier.
Step 9	**interface vlan** *bridge-domain-id* **Example:** `Router(config-if)# interface vlan 7`	Configures an Ethernet interface to create or access a dynamic SVI.
Step 10	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 7.7.7.1 255.255.255.0`	Specifies an IP address for the specified interface.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode and enters the global configuration mode.
Step 12	**router ospf** **Example:** `Router(config)# router ospf`	Enables the OSPF routing protocol and enters the router configuration mode.

	Command or Action	Purpose
Step 13	**fast-reroute per-prefix enable** [**area** *area-id*] **Example:** `Router(config-router)# fast-reroute per-prefix enable area 1`	Configures a per-prefix loop-free alternate (LFA) Fast Reroute (FRR) path that redirects traffic to an alternative next hop other than the primary neighbor. • **area**—Specifies the area in which to enable LFA-FRR. • *area-id*—OSPF area ID expressed as a decimal value or in IP address format.
Step 14	**fast-reroute per-prefix remote-lfa** [**area** *area-id*] **Example:** `Router(config-router)# fast-reroute per-prefix remote-lfa area 1`	Configures a per-prefix LFA FRR path that redirects traffic to a remote LFA area.
Step 15	**mpls ldp sync** **Example:** `Router(config-router)# mpls ldp sync`	Enables MPLS LDP synchronization on interfaces for an OSPF process.

Configuring Remote LFA-FRR for Ethernet and TDM Pseudowires

Note The Remote LFA-FRR feature is supported on the TDM pseudowires from Cisco IOS Realease 15.3(3)S onwards. The configuration and restrictions for EoMPLS are also applicable to the TDM pseudowires.

Note During packet loss, SAToP requires one second for convergence and two seconds for recovery.

- Configuring Remote LFA-FRR on a Global Interface, on page 726
- Configuring Remote LFA-FRR on a GigabitEthernet Interface, on page 727
- Configuring Remote LFA-FRR on an SVI Interface, on page 729
- Configuring Remote LFA-FRR on IS-IS , on page 730
- Configuring LFA-FRR for EoMPLS , on page 733
- Configuring LFA-FRR for ATM/IMA , on page 735
- Configuring LFA-FRR for CESoPSN , on page 737
- Configuring LFA-FRR for SAToP , on page 739

Configuring Remote LFA-FRR on a Global Interface

To configure Remote LFA-FRR on a global interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls label protocol ldp** **Example:** `Router(config)# mpls label protocol ldp`	Specifies that this LDP is the default distribution protocol.
Step 4	**no l3-over-l2 flush buffers** **Example:** `Router(config)# no l3-over-l2 flush buffers`	Disables Layer 3 over Layer 2 deployments.
Step 5	**asr901-platf-frr enable** **Example:** `Router(config)# asr901-platf-frr enable`	Enables TE-FRR link protection.
Step 6	**mpls ldp discovery targeted-hello accept** **Example:** `Router(config)# mpls ldp discovery targeted-hello accept`	Configures the neighbors from which requests for targeted hello messages may be honored. • **targeted-hello** —Configures the intervals and hold times for neighbors that are not directly connected. • **accept**—Configures the router to respond to requests for targeted hello messages from all neighbors.

Configuring Remote LFA-FRR on a GigabitEthernet Interface

To configure Remote LFA-FRR on a GigabitEthernet interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables automatic negotiation.
Step 5	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 7 ethernet`	Configures an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 7`	Enables IEEE 802.1Q encapsulation of traffic on a specified interface in a VLAN. • *vlan-id*—Virtual LAN identifier.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. • **pop** —Removes a tag from a packet. • **1**—Specifies the outermost tag for removal from a packet. • **symmetric** —Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
Step 8	**bridge-domain** *bridge-domain-id* **Example:** `Router(config-if-srv)# bridge-domain 7`	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI).

	Command or Action	Purpose
		• *bridge-domain-id*—Bridge domain identifier.

Configuring Remote LFA-FRR on an SVI Interface

To configure Remote LFA-FRR on an SVI interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 7.7.7.1 255.255.255.0`	Specifies an IP address for the specified interface.
Step 5	**ip router isis** **Example:** `Router(config-if)# ip router isis`	Configures an IS-IS routing process for an IP on an interface.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
Step 7	**isis network point-to-point** **Example:** `Router(config-if)# isis network point-to-point`	Configures a network of two networking devices that use the integrated IS-IS routing protocol to function as a point-to-point link.

Configuring Remote LFA-FRR on IS-IS

To configure Remote LFA-FRR for the IS-IS routing process, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis`	Enables the IS-IS routing protocol and enters the router configuration mode.
Step 4	**net** *net* **Example:** `Router(config-router)# net 49.0001.0002.0001.0001.00`	Configures an IS-IS network entity table (NET) for the routing process.
Step 5	**is-type level-1** **Example:** `Router(config-router)# is-type level-1`	Configures the routing level for an instance of the IS-IS routing process. • **level-1** —Router performs only Level 1 (intra-area) routing. This router learns only about destinations inside its area.
Step 6	**advertise-passive-only** **Example:** `Router(config-router)# advertise-passive-only`	Configures IS-IS to advertise only prefixes that belong to passive interfaces.
Step 7	**ispf level-1** **Example:** `Router(config-router)# ispf level-1`	Enables incremental shortest path first (SPF). • **level-1** —Enables incremental SPF for Level 1 packets only. The level-1 keyword applies only after enabling IS-IS. **Note** When IS-IS incremental SPF is configured on a ring topology, high convergence numbers

	Command or Action	Purpose
		are observed for random global prefixes. See CSCue11410 for details.
Step 8	**fast-flood** **Example:** `Router(config-router)# fast-flood`	Fills IS-IS link-state packets (LSPs).
Step 9	**max-lsp-lifetime** *seconds* **Example:** `Router(config-router)# max-lsp-lifetime 65535`	Configures the maximum link-state packets (LSPs) lifetime. • *seconds*—Maximum LSP lifetime in seconds. The range is from 1 to 65535.
Step 10	**lsp-refresh-interval** *seconds* **Example:** `Router(config-router)# lsp-refresh-interval 900`	Sets the link-state packet (LSP) refresh interval. • seconds—Interval (in seconds) at which LSPs are refreshed.The range is 1 to 65535 seconds. The default value is 900 seconds (15 minutes).
Step 11	**spf-interval [level-1 | level-2]** *spf-max-wait* [*spf-initial-wait spf-second-wait*] **Example:** `Router(config-router)# spf-interval 5 50 200`	Customizes IS-IS throttling of shortest path first (SPF) calculations. • **level-1**—(Optional) Apply intervals to Level-1 areas only. • **level-2**—(Optional) Apply intervals to Level-2 areas only. • *spf-max-wait*—Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds. • *spf-initial-wait*—(Optional) Indicates the initial SPF calculation delay (in milliseconds) after a topology change. The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds). • *spf-second-wait*—(Optional) Indicates the hold time between the first and second SPF calculation (in milliseconds). The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).
Step 12	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] **Example:**	Customizes IS-IS throttling of partial route calculations (PRC).

	Command or Action	Purpose
	`Router(config-router)# prc-interval 5 50 200`	• *prc-max-wait*—Indicates the maximum interval (in seconds) between two consecutive PRC calculations. Value range is 1 to 120 seconds. The default is 5 seconds. • *prc-initial-wait* —(Optional) Indicates the initial PRC calculation delay (in milliseconds) after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds. • *prc-second-wait*—(Optional) Indicates the hold time between the first and second PRC calculation (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).
Step 13	**lsp-gen-interval [level-1 | level-2]** *lsp-max-wait* **[***lsp-initial-wait lsp-second-wait***]** **Example:** `Router(config-router)# lsp-gen-interval 5 50 200`	Customizes IS-IS throttling of LSP generation. • **level-1**—(Optional) Apply intervals to Level-1 areas only. • **level-2**—(Optional) Apply intervals to Level-2 areas only. • *lsp-max-wait*—Indicates the maximum interval (in seconds) between two consecutive occurrences of an LSP being generated. The range is 1 to 120 seconds. The default is 5 seconds. • *lsp-initial-wait* —(Optional) Indicates the initial LSP generation delay (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 50 milliseconds. • *lsp-second-wait*—(Optional) Indicates the hold time between the first and second LSP generation (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).
Step 14	**no hello padding** **Example:** `Router(config-router)# no hello padding`	Reenables IS-IS hello padding at the router level.
Step 15	**log-adjacency-changes** **Example:** `Router(config-router)# log-adjacency-changes`	Configures the router to send a syslog message when an OSPF neighbor goes up or down.

	Command or Action	Purpose
Step 16	**fast-reroute per-prefix {level-1 | level-2} {all | route-map** *route-map-name***}** **Example:** `Router(config-router)# fast-reroute per-prefix level-1 all`	Configures an FRR path that redirects traffic to a remote LFA tunnel for either level 1 or level 2 packets. • **level-1**—Enables per-prefix FRR of level 1 packets. • **level-2**—Enables per-prefix FRR of level 2 packets. • **all**—Enables FRR of all primary paths. • **route-map**—Specifies the route map for selecting primary paths for protection. • *route-map-name*—Route map name.
Step 17	**fast-reroute remote-lfa {level-1 | level-2} mpls-ldp [maximum-metric** *metric-value***]** **Example:** `Router(config-router)# fast-reroute remote-lfa level-1 mpls-ldp`	Configures an FRR path that redirects traffic to a remote LFA tunnel. • **level-1**—Enables LFA-FRR of level 1 packets. • **level-2**—Enables LFA-FRR of level 2 packets. • **mpls-ldp**—Specifies that the tunnel type is MPLS or LDP. • **maximum-metric**—(Optional)Specifies the maximum metric value required to reach the release node. • *metric-value*—Metric value.
Step 18	**passive-interface** *interface-type interface-number* **Example:** `Router(config-router)# passive-interface Loopback0`	Disables sending routing updates on an interface. • *interface-type*—Interface type. • *interface-number*—Interface number.
Step 19	**mpls ldp sync** **Example:** `Router(config-router)# mpls ldp sync`	Enables MPLS LDP synchronization on interfaces for an IS-IS process.

Configuring LFA-FRR for EoMPLS

To configure LFA-FRR for EoMPLS, complete the following steps:

Note Effective with Cisco IOS release 15.4(1)S, the EoMPLS Pseudowire Redundancy over FRR feature is supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 5	**negotiation auto** **Example:** `Router(config-if)# negotiation auto`	Enables automatic negotiation.
Step 6	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 100 ethernet`	Configures an Ethernet service instance on an interface. • *id*—Integer that uniquely identifies a service instance on an interface. The value varies by the platform. Range: 1 to 4294967295. The identifier need not map to a VLAN and is local in scope to the interface.
Step 7	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 101`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. • *vlan-id*—Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.

	Command or Action	Purpose
Step 8	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 9	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 10.0.0.4 4 encapsulation mpls`	Binds an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire. • *peer-ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—The 32-bit identifier of the virtual circuit (VC) between the PE routers. • **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.
Step 10	**backup peer** *peer-ip-address vc-id* **Example:** `Router(config-if-ether-vc-xconn)# backup peer 10.0.0.5 4`	Specifies a redundant peer for a pseudowire VC. • *peer-ip-address*—IP address of the remote peer.

Configuring LFA-FRR for ATM/IMA

To configure LFA-FRR for ATM/IMA, complete the following steps:

Note Effective with Cisco IOS release 15.4(1)S, the TDM Pseudowire Redundancy over FRR feature is supported.

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller e1 0/0`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**ima-group** *ima-group-number* **Example:** `Router(config-controller)# ima-group 2`	Assigns the interface to an IMA group. • *ima-group-number*—IMA group number.
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode and enters global configuration mode.
Step 6	**interface ATM** *slot* **/IMA** *group-number* **Example:** `Router(config)# interface ATM0/IMA2`	Configures inverse multiplexing over ATM (IMA) group. • *slot*—Specifies the slot location of the ATM IMA port adapter. • *group-number*—Specifies the group number of the IMA group.
Step 7	**no ip address** **Example:** `Router(config-if)# no ip address`	Disables IP address configuration for the physical layer interface.
Step 8	**no atm ilmi-keepalive** **Example:** `Router(config-if)# no atm ilmi-keepalive`	Disables the Interim Local Management Interface (ILMI) keepalive parameters.
Step 9	**pvc** *vpi/vci* **l2transport** **Example:** `Router(config-if)# pvc 90/90 l2transport`	Create or assigns a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC. • *vpi*—ATM network virtual path identifier (VPI) for this PVC. • *vci*—ATM network virtual channel identifier (VCI) for this PVC.
Step 10	**xconnect** *ip-address* **encapsulation mpls** **Example:** `Router(config-if-cem)# xconnect 2.2.2.2 111 encapsulation mpls`	Binds an attachment circuit to a pseudowire, to configure an Any Transport over MPLS (AToM) static pseudowire. • *ip-address*—IP address of the remote provider edge (PE) peer. The remote

	Command or Action	Purpose
		router ID can be any IP address, as long as it is reachable. • **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.
Step 11	**backup peer** *peer-ip-address* **Example:** `Router(config-if-xconn)# backup peer 2.2.2.3 111`	Specifies a redundant peer for a pseudowire VC. • *peer-ip-address*—IP address of the remote peer.

Configuring LFA-FRR for CESoPSN

To configure LFA-FRR for CESoPSN, complete the following steps:

Note Effective with Cisco IOS release 15.4(1)S, the TDM Pseudowire Redundancy over FRR feature is supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller e1 0/0`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**clock source internal** **Example:** `Router(config-controller)# clock source internal`	Sets clocking for individual links.

	Command or Action	Purpose
Step 5	**cem-group** *group-number* **timeslots** *timeslot-range* **Example:** `Router(config-controller)# cem-group 0 timeslots 1-31`	Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel and specific timeslots to the CEM channel. • *group-number*—Channel number to be used for this group of time slots. • **timeslot**—Specifies that a list of time slots is to be used as specified by the timeslot-range argument. • *timeslot-range*—List of the time slots to be included in the CEM channel. The list may include commas and hyphens with no spaces between the numbers.
Step 6	**description** *descriptive-name* **Example:** `Router(config-controller)# description E1 CESoPSN example`	Specifies a descriptive name for the controller.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 8	**interface cem** *slot/port* **Example:** `Router(config)# interface CEM 0/0`	Defines a CEM channel.
Step 9	**no ip address** **Example:** `Router(config-cem)# no ip address`	Removes an IP address or disables IP processing.
Step 10	**cem** *group-number* **Example:** `Router(config-cem)# cem 0`	Defines a CEM channel.
Step 11	**xconnect** *ip-address* **encapsulation mpls** **Example:** `Router(config-cem)# xconnect 2.2.2.2 111 encapsulation mpls`	Binds an attachment circuit to a pseudowire, to configure an Any Transport over MPLS (AToM) static pseudowire. • *ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.

	Command or Action	Purpose
		• **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.
Step 12	**backup peer** *peer-ip-address* **Example:** `Router(config-if-xconn)# backup peer 2.2.2.3 111`	Specifies a redundant peer for a pseudowire VC. • *peer-ip-address*—IP address of the remote peer.

Configuring LFA-FRR for SAToP

To configure LFA-FRR for SAToP, complete the following steps:

Note Effective with Cisco IOS release 15.4(1)S, the TDM Pseudowire Redundancy over FRR feature is supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller {t1 | e1}** *slot/port* **Example:** `Router(config)# controller e1 0/0`	Selects a T1 or E1 controller and enters controller configuration mode.
Step 4	**framing unframed** **Example:** `Router(config-controller)# framing unframed`	Specifies the framing format of a circuit emulation (CEM) T1 or E1 port.

	Command or Action	Purpose
Step 5	**clock source internal** **Example:** `Router(config-controller)# clock source internal`	Sets clocking for individual T1 or E1 links.
Step 6	**cem-group** *group-number* **unframed** **Example:** `Router(config-controller)# cem-group 0 unframed`	Assigns channels on the T1 or E1 circuit to the CEM channel. • *group-number*—Channel number to be used for this group of time slots. • **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.
Step 7	**description** *descriptive-name* **Example:** `Router(config-controller)# description E1 SAToP example`	Specifies a descriptive name for the controller
Step 8	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode.
Step 9	**interface cem** *slot/port* **Example:** `Router(config)# interface CEM 0/0`	Defines a CEM channel.
Step 10	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 11	**cem** *group-number* **Example:** `Router(config-if)# cem 0`	Defines a CEM channel.
Step 12	**xconnect** *ip-address* **encapsulation mpls** **Example:** `Router(config-if-cem)# xconnect 2.2.2.2 111 encapsulation mpls`	Binds an attachment circuit to a pseudowire, to configure an Any Transport over MPLS (AToM) static pseudowire. • *ip-address*—IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.

	Command or Action	Purpose
		• **encapsulation**—Specifies the tunneling method to encapsulate the data in the pseudowire. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.
Step 13	**backup peer** *peer-ip-address* **Example:** `Router(config-if-cem-xconn)# backup peer 2.2.2.3 111`	Specifies a redundant peer for a pseudowire VC. • *peer-ip-address*—IP address of the remote peer.

Verification Examples for Remote LFA-FRR

Verifying Remote LFA-FRR Configuration

To verify the remote LFA-FRR configuration, use the show commands described in the following examples.

To display information for an OSPF per-prefix LFA-FRR configuration, use the following show command.

```
Router# show ip ospf fast-reroute remote-lfa tunnels
            OSPF Router with ID (1.1.1.1) (Process ID 1)
                     Area with ID (0)
                    Base Topology (MTID 0)
Interface MPLS-Remote-Lfa5
  Tunnel type: MPLS-LDP
  Tailend router ID: 5.5.5.5
  Termination IP address: 5.5.5.5
  Outgoing interface: Vlan4004
  First hop gateway: 71.14.1.4
  Tunnel metric: 2
  Protects:
    71.17.1.7 Vlan4003, total metric 4
Interface MPLS-Remote-Lfa6
  Tunnel type: MPLS-LDP
  Tailend router ID: 6.6.6.6
  Termination IP address: 6.6.6.6
  Outgoing interface: Vlan4003
  First hop gateway: 71.17.1.7
  Tunnel metric: 2
  Protects:
    71.14.1.4 Vlan4004, total metric 4
```

To display entries in the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB), use the following show command.

```
Router# show ip cef 171.1.1.0 internal
171.1.1.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB, LTE
  feature space:
   IPRM: 0x00028000
   LFD: 171.1.1.0/24 1 local label
   local label info: global/542
```

```
        contains path extension list
        disposition chain 0x12E83850
        label switch chain 0x12E83850
  ifnums:
   Vlan4004(30): 71.14.1.4
   MPLS-Remote-Lfa6(37)
  path 12C70E98, path list 12D52154, share 1/1, type attached nexthop, for IPv4, flags
has-repair
    MPLS short path extensions: MOI flags = 0x20 label 31
  nexthop 71.14.1.4 Vlan4004 label [31|537], adjacency IP adj out of Vlan4004, addr 71.14.1.4
 12CD6A40
    repair: attached-nexthop 6.6.6.6 MPLS-Remote-Lfa6 (12C70FE8)
  path 12C70FE8, path list 12D52154, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 6.6.6.6 MPLS-Remote-Lfa6, repair, adjacency IP midchain out of MPLS-Remote-Lfa6
12CD7880
  output chain: label [31|537]
  FRR Primary (0x11139020)
  <primary:  TAG adj out of Vlan4004, addr 71.14.1.4 12D8A780>
  <repair:  TAG midchain out of MPLS-Remote-Lfa6 12CD6580 label 338 TAG adj out of Vlan4003,
 addr 71.17.1.7 12CD7160>
```

To display local Routing Information Base (RIB) or locally redistributed routes use the following show command.

```
Router# show ip ospf rib 171.1.1.0
            OSPF Router with ID (1.1.1.1) (Process ID 1)
                Base Topology (MTID 0)
OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator
*>  171.1.1.0/24, Intra, cost 2, area 0
     SPF Instance 130, age 00:03:52
     Flags: RIB, iSPF
      via 71.14.1.4, Vlan4004
       Flags: RIB, iSPF
       LSA: 1/2.0.0.2/2.0.0.2
      repair path via 6.6.6.6, MPLS-Remote-Lfa6, cost 4
       Flags: RIB, Repair, IntfDj, BcastDj, CostWon
       LSA: 1/2.0.0.2/2.0.0.2
```

To display information for an IS-IS per-prefix LFA-FRR configuration, use the following show command.

```
Router# show isis fast-reroute remote-lfa tunnels
Tag Null - Fast-Reroute Remote-LFA Tunnels:
  MPLS-Remote-Lfa1: use Vl4003, nexthop 71.17.1.7, end point 6.6.6.6
  MPLS-Remote-Lfa2: use Vl4004, nexthop 71.14.1.4, end point 5.5.5.5
```

To display entries in the CEF Forwarding Information Base (FIB) use the following show command.

```
Router# show ip cef 171.1.1.0 internal
171.1.1.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB, LTE
  feature space:
   IPRM: 0x00028000
   LFD: 171.1.1.0/24 1 local label
   local label info: global/18
        contains path extension list
        disposition chain 0x12B537C8
  ifnums:
   Vlan4004(30): 71.14.1.4
   MPLS-Remote-Lfa1(32)
  path 12C55CB4, path list 12C856E8, share 1/1, type attached nexthop, for IPv4, flags
```

```
has-repair
    MPLS short path extensions: MOI flags = 0x20 label none
  nexthop 71.14.1.4 Vlan4004 label [none|23], adjacency IP adj out of Vlan4004, addr 71.14.1.4
 1139FAA0
    repair: attached-nexthop 6.6.6.6 MPLS-Remote-Lfa1 (12C55D24)
  path 12C55D24, path list 12C856E8, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 6.6.6.6 MPLS-Remote-Lfa1, repair, adjacency IP midchain out of MPLS-Remote-Lfa1
12D512C0
  output chain: label [none|23]
  FRR Primary (0xA74F800)
  <primary:  IP adj out of Vlan4004, addr 71.14.1.4 1139FAA0>
  <repair:  TAG midchain out of MPLS-Remote-Lfa1 11180740 label 366 TAG adj out of Vlan4003,
 addr 71.17.1.7 12D51520>
```

To display information about IS-IS FRR configurations, use the following show command.

```
Router# show isis fast-reroute summary
Tag null:
IPv4 Fast-Reroute Protection Summary:
 Prefix Counts:          Total      Protected    Coverage
   High priority:        0          0            0%
   Normal priority:      10         8            80%
   Total:                10         8            80%
```

To display paths for a specific route or for all routes under a major network that are stored in the IP local Routing Information Base (RIB), use the following show command.

```
Router# show isis rib 171.1.1.0
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x0) =================
Repair path attributes:
    DS - Downstream, LC - Linecard-Disjoint, NP - Node-Protecting
    PP - Primary-Path, SR - SRLG-Disjoint
Routes under majornet 171.1.0.0/16:
171.1.1.0/24
  [115/L1/10] via 71.14.1.4(Vlan4004), from 71.14.1.4, tag 0, LSP[2/18]
             (installed)
     repair path: 6.6.6.6(MPLS-Remote-Lfa1) metric:20 (DS,SR) LSP[2]
```

Verifying Remote LFA-FRR Configuration for EoMPLS on a GigabitEthernet Interface

To verify the remote LFA-FRR configuration for EoMPLS on a GigabitEthernet interface, use the show commands described in the following examples.

```
Router# show mpls l2transport vc 1 detail
Local interface: Gi0/0 up, line protocol up, Ethernet up
  Destination address: 3.3.3.3, VC ID: 1, VC status: up
    Output interface: Vl4000, imposed label stack {18 16}
    Preferred path: not configured
    Default path: active
    Next hop: 71.12.1.2
  Create time: 00:00:06, last status change time: 00:00:06
    Last label FSM state change time: 00:00:06
  Signaling protocol: LDP, peer 3.3.3.3:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 3.3.3.3, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
```

```
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 323, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 4801/4799 (used), PWID: 1
  VC statistics:
    transit packet totals: receive 0, send 1009697
    transit byte totals:   receive 0, send 96933706
    transit packet drops:  receive 0, seq error 0, send 0
Local interface: Gi0/0 up, line protocol up, Ethernet up
  Destination address: 4.4.4.4, VC ID: 1, VC status: standby
    Output interface: Vl4000, imposed label stack {21 16}
    Preferred path: not configured
    Default path: active
    Next hop: 71.12.1.2
  Create time: 00:00:06, last status change time: 00:16:44
    Last label FSM state change time: 00:00:06
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 4.4.4.4, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LrdRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: DOWN(standby)
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: DOWN(standby)
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 324, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 8898/8896 (used), PWID: 2
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

Verifying Remote LFA-FRR Configuration for EoMPLS on an EVC Interface

To verify the remote LFA-FRR configuration for EoMPLS on an EVC interface, use the show commands described in the following examples.

```
Router# show mpls l2transport vc 3001 detail
Local interface: Gi0/0 up, line protocol up, Eth VLAN 200 up
  Interworking type is Ethernet
  Destination address: 3.3.3.3, VC ID: 1, VC status: up
    Output interface: Vl4000, imposed label stack {18 16}
    Preferred path: not configured
    Default path: active
    Next hop: 71.12.1.2
  Create time: 00:13:47, last status change time: 00:04:20
    Last label FSM state change time: 00:11:54
  Signaling protocol: LDP, peer 3.3.3.3:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 3.3.3.3, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 16, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent:1, received:0
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 1434251/4096 (used), PWID: 1
  VC statistics:
    transit packet totals: receive 0, send 260970
    transit byte totals:   receive 0, send 24009240
    transit packet drops:  receive 0, seq error 0, send 0
Local interface: Gi0/0 up, line protocol up, Eth VLAN 200 up
  Interworking type is Ethernet
  Destination address: 4.4.4.4, VC ID: 1, VC status: standby
    Output interface: Vl4000, imposed label stack {21 16}
    Preferred path: not configured
    Default path: active
    Next hop: 71.12.1.2
  Create time: 00:13:47, last status change time: 00:14:41
    Last label FSM state change time: 00:12:47
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 4.4.4.4, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LrdRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: DOWN(standby)
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: DOWN(standby)
      Last remote LDP TLV    status rcvd: No fault
```

```
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 17, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent:1, received:0
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 885253/8193 (used), PWID: 2
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

Verifying Remote LFA-FRR Configuration on IS-IS

To verify the remote LFA-FRR configuration on IS-IS, use the show commands described in the following examples.

```
Router# show isis fast-reroute remote-lfa tunnels
Tag aggg - Fast-Reroute Remote-LFA Tunnels:
  No Remote-LFA tunnel
Tag Null - Fast-Reroute Remote-LFA Tunnels:
  No Remote-LFA tunnel
Tag agg - Fast-Reroute Remote-LFA Tunnels:
  MPLS-Remote-Lfa5: use Vl27, nexthop 27.27.27.2, end point 192.168.1.2
  MPLS-Remote-Lfa6: use Vl50, nexthop 50.50.50.2, end point 192.168.1.2
```

Verifying Remote LFA-FRR Configuration on ATM/IMA

To verify the remote LFA-FRR configuration on ATM/IMA, use the show commands described in the following example.

```
Router# show mpls l2 vc 90 detail
Local interface: AT0/IMA2 up, line protocol up, ATM AAL5 90/90 Basic 1 up
  Destination address: 2.2.2.2, VC ID: 111, VC status: up
    Output interface: Vlan300, imposed label stack {29 32}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 17:54:25, last status change time: 17:54:25
    Last label FSM state change time: 17:54:25
  Signaling protocol: LDP, peer 2.2.2.2:0 up
    Targeted Hello: 170.0.0.201(LDP Id) -> 2.2.2.2, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 20, remote 32
    Group ID: local 0, remote 0
```

```
    MTU: local 0, remote 0
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
```

Verifying Remote LFA-FRR Configuration on CESoPSN

To verify the remote LFA-FRR configuration on CESoPSN, use the show commands described in the following example.

```
Router# show mpls l2 vc 111 detail
Local interface: CE0/0 up, line protocol up, CESoPSN Basic 1 up
  Destination address: 2.2.2.2, VC ID: 111, VC status: up
    Output interface: Vlan300, imposed label stack {29 32}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 17:54:25, last status change time: 17:54:25
    Last label FSM state change time: 17:54:25
  Signaling protocol: LDP, peer 2.2.2.2:0 up
    Targeted Hello: 170.0.0.201(LDP Id) -> 2.2.2.2, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 20, remote 32
    Group ID: local 0, remote 0
    MTU: local 0, remote 0
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 4124/8219 (used), PWID: 4
  VC statistics:
    transit packet totals: receive 64465447, send 64465519
    transit byte totals:   receive 15987430856, send 15987448712
    transit packet drops:  receive 0, seq error 0, send 0
```

Verifying Remote LFA-FRR Configuration on SAToP

To verify the remote LFA-FRR configuration on SAToP, use the show commands described in the following example.

Router# show mpls l2 vc 111 detail

```
Local interface: CE0/0 up, line protocol up, SATOP Basic 1 up
  Destination address: 2.2.2.2, VC ID: 111, VC status: up
    Output interface: Vlan300, imposed label stack {29 32}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
```

```
  Create time: 17:54:25, last status change time: 17:54:25
    Last label FSM state change time: 17:54:25
  Signaling protocol: LDP, peer 2.2.2.2:0 up
    Targeted Hello: 170.0.0.201(LDP Id) -> 2.2.2.2, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 20, remote 32
    Group ID: local 0, remote 0
    MTU: local 0, remote 0
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
```

Configuration Examples for Remote LFA-FRR

This section provides sample configuration examples for Remote LFA-FRR feature on the Cisco ASR 901 router.

Example: Configuring Remote LFA-FRR for IS-IS

The following is a sample configuration of Remote LFA-FRR for IS-IS on all nodes.

```
!
mpls label protocol ldp
mpls ldp router-id lo0 force
mpls ldp discovery targeted-hello accept
no l3-over-l2 flush buffers
asr901-platf-frr enable
router isis
metric-style wide
fast-flood
max-lsp-lifetime 65535
lsp-refresh-interval 65000
spf-interval 5 50 200
prc-interval 5 50 200
lsp-gen-interval 5 50 200
no hello padding
log-adjacency-changes all
fast-reroute per-prefix level-1 all
fast-reroute remote-lfa level-1 mpls-ldp
mpls ldp sync
!
```

Example: Configuring Remote LFA-FRR for OSPF

The following is a sample configuration of Remote LFA-FRR for OSPF on all nodes.

```
!
mpls label protocol ldp
mpls ldp router-id lo0 force
mpls ldp discovery targeted-hello accept
no l3-over-l2 flush buffers
asr901-platf-frr enable
router ospf 1
router-id 5.5.5.5
fast-reroute per-prefix enable area 0 prefix-priority low
fast-reroute per-prefix remote-lfa tunnel mpls-ldp
timers throttle spf 50 200 5000
timers throttle lsa 50 200 5000
timers lsa arrival 100
mpls ldp sync
!
```

Example: Configuring Remote LFA-FRR Globally

The following is a sample configuration of Remote LFA-FRR at a global level.

```
!
mpls label protocol ldp
mpls ldp discovery targeted-hello accept
no l3-over-l2 flush buffers
asr901-platf-frr enable
!
```

Example: Configuring Remote LFA-FRR on a GigabitEthernet Interface

The following is a sample configuration of Remote LFA-FRR on a GigabitEthernet Interface.

```
!
interface GigabitEthernet0/7
 no ip address
 negotiation auto
 service instance 7 ethernet
  encapsulation dot1q 7
  rewrite ingress tag pop 1 symmetric
  bridge-domain 7
!
```

Example: Configuring Remote LFA-FRR on an SVI Interface

The following is a sample configuration of Remote LFA-FRR on an SVI Interface.

```
!
interface Vlan7
 ip address 7.7.7.2 255.255.25
 ip router isis
 mpls ip
```

```
 isis network point-to-point
!
```

Example: Configuring EoMPLS Pseudowire Redundancy over FRR

The following is a sample configuration of EoMPLS pseudowire redundancy over FRR.

```
!
interface GigabitEthernet0/0
 no ip address
 load-interval 30
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  xconnect 3.3.3.3 1 encapsulation mpls
   backup peer 4.4.4.4 1
   mtu 1500
!
```

Example: Configuring LFA-FRR on ATM/IMA

The following is a sample configuration of LFA-FRR on ATM/IMA, which also includes pseudowire redundancy.

```
!
controller E1 0/0
 ima-group 2
!
interface ATM0/IMA1
 no ip address
 no atm enable-ilmi-trap
 xconnect 2.2.2.2 90 encapsulation mpls
  backup peer 180.0.0.201 90
!
```

Example: Configuring LFA-FRR on CESoPSN

The following is a sample configuration of LFA-FRR on CESoPSN, which also includes pseudowire redundancy.

```
!
controller E1 0/0
 clock source internal
 cem-group 0 timeslots 1-31
 description E1 CESoPSN example
!
!
interface CEM0/2
 no ip address
 cem 1
  xconnect 2.2.2.2 111 encapsulation mpls pw-class test
   backup peer 180.0.0.201 111
 !
```

Example: Configuring LFA-FRR on SAToP

The following is a sample configuration of LFA-FRR on SAToP, which also includes pseudowire redundancy.

```
!
controller E1 0/0
 clock source internal
 cem-group 1 unframed
 description E1 SATOP example
!
interface CEM0/0
 no ip address
 cem 0
  xconnect 2.2.2.2 111 encapsulation mpls
   backup peer 180.0.0.201 111
 !
!
```

Additional References

The following sections provide references related to Remote Loop-Free Alternate - Fast Reroute feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference
IS-IS Remote LFA FRR	IS-IS Remote Loop-Free Alternate Fast Reroute
OSPFv2 LFA FRR	OSPFv2 Loop-Free Alternate Fast Reroute

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Remote Loop-Free Alternate - Fast Reroute

Table 46: Feature Information for Remote Loop-Free Alternate - Fast Reroute, on page 752 lists the features in this module and provides links to specific configuration information.

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 Table 46: Feature Information for Remote Loop-Free Alternate - Fast Reroute, on page 752 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 46: Feature Information for Remote Loop-Free Alternate - Fast Reroute

Feature Name	Releases	Feature Information
Remote Loop-Free Alternate - Fast Reroute	15.2(2)SNI	This feature was introduced on the Cisco ASR 901 routers. The following sections provide information about this feature:
Remote Loop-Free Alternate - Fast Reroute for EoMPLS	15.3(2)S	This feature was introduced on the Cisco ASR 901 routers. The following section provides information about this feature:
Remote Loop-Free Alternate - Fast Reroute for TDM Pseudowires.	15.3(3)S	Support for TDM Pseudowires was added.

Feature Name	Releases	Feature Information
EoMPLS Pseudowire Redundancy over FRR	15.4(1)S	Support was added for EoMPLS pseudowire redundancy over FRR.
TDM Pseudowire Redundancy over FRR	15.4(1)S	Support was added for TDM pseudowire redundancy over FRR.

CHAPTER 41

Digital Optical Monitoring

This feature module provides information on the digital optical monitoring (DOM) feature for the Cisco ASR 901 Series Aggregation Services Router.

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 table at the end of this module.

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.

Feature Overview

The ASR 901 router supports DOM as per the standard SFF-8724 Multi-Source Agreement (MSA). This feature allows monitoring real-time parameters of the router, such as optical input and output power, temperature, laser bias current, and transceiver supply voltage. These parameters are monitored against the threshold values. The real-time DOM parameters can be monitored using command line interface or SNMP interface. Effective with Cisco IOS Release 15.3(3)S, Cisco ASR 901 supports DOM for both 1G and 10G SFPs.

DOM allows the user to view the threshold violation messages. To display the threshold violation messages, you must enable transceiver monitoring. For information on enabling transceiver monitoring, see How to Enable Transceiver Monitoring, on page 756.

The command line output for the real-time parameters is shown using the **show interfaces transceiver** command. To enable threshold notification in the transceiver via SNMP, use the **snmp-server enable traps**

transceiver command. You can use the show controllers gig 0/x command to check whether SFP's are DOM capable. This command displays the SFP details.

How to Enable Transceiver Monitoring

Complete the following steps to enable transceiver monitoring:

Restrictions

- You need the transceiver module compatibility information for configuring transceiver monitoring. The compatibility matrix that lists the support for DOM in the Cisco transceiver modules is available at the following URL: http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_8031.html
- In case of combo ports with SFP and RJ45 provision, when SFP is inserted in slot or port and media type is not configured to SFP, DOM is functional only if global transceiver monitoring is enabled.
- CISCO-ENTITY-SENSOR-MIB traps are sent only once after the threshold violation. However, SYSLOG traps are sent according to the monitoring interval.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**transceiver type all** **Example:** `Router(config)# transceiver type all`	Enters the transceiver type configuration mode.
Step 4	**monitoring** **Example:** `Router(config-xcvr-type)# monitoring`	Enables monitoring of all optical transceivers.
Step 5	**monitoring interval**; **Example:** `Router(config-xcvr-type)# monitoring interval 500`	(Optional) Specifies the time interval for monitoring optical transceivers. Valid range is 300 to 3600 seconds, and the default value is 600 seconds.

Examples

The real-time parameters of the router, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage can be monitored using the **show interfaces transceiver** command.

This section provides sample output for monitoring the real-time parameters on the Cisco ASR 901 router:

Example: Displaying Transceiver Information

This example shows how to display transceiver information:

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                           Optical   Optical
           Temperature  Voltage  Current   Tx Power  Rx Power
Port       (Celsius)    (Volts)  (mA)      (dBm)     (dBm)
---------  -----------  -------  --------  --------  --------
Gi0/10       36.9       3.25     537.7      -4.5      -9.7
Gi0/11       35.8       3.22     393.6      -5.5      -5.0
```

Example: Displaying Detailed Transceiver Information

This example shows how to display detailed transceiver information:

```
Router# show interfaces transceiver detail
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
                              High Alarm  High Warn  Low Warn   Low Alarm
           Temperature        Threshold   Threshold  Threshold  Threshold
Port       (Celsius)          (Celsius)   (Celsius)  (Celsius)  (Celsius)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       33.9                   85.0       75.0        0.0       -5.0
Gi0/11       32.8                   85.0       75.0        0.0       -5.0
                              High Alarm  High Warn  Low Warn   Low Alarm
           Voltage            Threshold   Threshold  Threshold  Threshold
Port       (Volts)            (Volts)     (Volts)    (Volts)    (Volts)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       3.25                   3.70       3.59       3.09       3.00
Gi0/11       3.23                   3.70       3.59       3.09       3.00
                              High Alarm  High Warn  Low Warn   Low Alarm
           Current            Threshold   Threshold  Threshold  Threshold
Port       (milliamperes)     (mA)        (mA)       (mA)       (mA)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10      533.3                    N/A        N/A        N/A        N/A
Gi0/11      391.1                    N/A        N/A        N/A        N/A
           Optical            High Alarm  High Warn  Low Warn   Low Alarm
           Transmit Power     Threshold   Threshold  Threshold  Threshold
Port       (dBm)              (dBm)       (dBm)      (dBm)      (dBm)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       -4.5                   -3.5       -4.0       -9.5      -10.0
Gi0/11       -5.5                   -3.5       -4.0       -9.5      -10.0
```

```
          Optical           High Alarm  High Warn  Low Warn   Low Alarm
          Receive Power     Threshold   Threshold  Threshold  Threshold
Port      (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
--------- ----------------- ----------  ---------  ---------  ---------
Gi0/10      -5.2                  0.0        0.0      -17.0      -17.1
Gi0/11      -7.5                  0.0        0.0      -17.0      -17.1
```

Example: Displaying List of Supported Transceivers

This example shows how to display the list of supported DOM transceivers:

```
Router# show interfaces transceiver supported-list
Transceiver Type           Cisco p/n min version
                               supporting DOM
------------------       -------------------------
   DWDM GBIC                ALL
   DWDM SFP                 ALL
   RX only WDM GBIC         ALL
   DWDM XENPAK              ALL
   DWDM X2                  ALL
   DWDM XFP                 ALL
   CWDM GBIC                NONE
   CWDM X2                  ALL
   CWDM XFP                 ALL
   XENPAK ZR                ALL
   X2 ZR                    ALL
   XFP ZR                   ALL
   Rx_only_WDM_XENPAK       ALL
   XENPAK_ER                10-1888-04
   X2_ER                    ALL
   XFP_ER                   ALL
   XENPAK_LR                10-1838-04
   X2_LR                    ALL
   XFP_LR                   ALL
   XENPAK_LW                ALL
   X2_LW                    ALL
   XFP_LW                   NONE
   XENPAK SR                NONE
   X2 SR                    ALL
   XFP SR                   ALL
   XENPAK LX4               NONE
   X2 LX4                   NONE
   XFP LX4                  NONE
   XENPAK CX4               NONE
   X2 CX4                   NONE
   SX GBIC                  NONE
   LX GBIC                  NONE
   ZX GBIC                  NONE
   CWDM_SFP                 ALL
   Rx_only_WDM_SFP          NONE
   SX_SFP                   ALL
   LX_SFP                   ALL
   ZX_SFP                   ALL
   EX_SFP                   ALL
   SX SFP                   NONE
   LX SFP                   NONE
   ZX SFP                   NONE
   GIgE BX U SFP            NONE
   GigE BX D SFP            ALL
   X2 LRM                   ALL
```

Example: Displaying Threshold Tables

This example shows how to display the threshold tables for all transceivers on the Cisco ASR 901 router:

```
Router# show interfaces transceiver threshold table
              Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                    current
             -------------  -------------  ------   ------------  ---------
 DWDM GBIC
Min1             -0.50         -28.50      0            N/A          4.50
Min2             -0.30         -28.29      5            N/A          4.75
Max2              3.29          -6.69      60           N/A          5.25
Max1              3.50           6.00      70           N/A          5.50
 DWDM SFP
Min1             -0.50         -28.50      0            N/A          3.00
Min2             -0.30         -28.29      5            N/A          3.09
Max2              4.30          -9.50      60           N/A          3.59
Max1              4.50           9.30      70           N/A          3.70
 RX only WDM GBIC
Min1              N/A          -28.50      0            N/A          4.50
Min2              N/A          -28.29      5            N/A          4.75
Max2              N/A           -6.69      60           N/A          5.25
Max1              N/A            6.00      70           N/A          5.50
 DWDM XENPAK
Min1             -1.50         -24.50      0            N/A          N/A
Min2             -1.29         -24.29      5            N/A          N/A
Max2              3.29          -6.69      60           N/A          N/A
Max1              3.50           4.00      70           N/A          N/A
 DWDM X2
Min1             -1.50         -24.50      0            N/A          N/A
Min2             -1.29         -24.29      5            N/A          N/A
Max2              3.29          -6.69      60           N/A          N/A
Max1              3.50           4.00      70           N/A          N/A
 DWDM XFP
Min1             -1.50         -24.50      0            N/A          N/A
Min2             -1.29         -24.29      5            N/A          N/A
Max2              3.29          -6.69      60           N/A          N/A
Max1              3.50           4.00      70           N/A          N/A
 CWDM X2
Min1              N/A            N/A       0            N/A          N/A
Min2              N/A            N/A       0            N/A          N/A
Max2              N/A            N/A       0            N/A          N/A
Max1              N/A            N/A       0            N/A          N/A
 CWDM XFP
Min1              N/A            N/A       0            N/A          N/A
Min2              N/A            N/A       0            N/A          N/A
Max2              N/A            N/A       0            N/A          N/A
Max1              N/A            N/A       0            N/A          N/A
 XENPAK ZR
Min1             -0.50         -24.50      0            N/A          N/A
Min2             -0.80         -24.29      5            N/A          N/A
Max2              4.30          -6.69      60           N/A          N/A
Max1              4.50           4.00      70           N/A          N/A
 X2 ZR
Min1             -0.50         -24.50      0            N/A          N/A
Min2             -0.80         -24.29      5            N/A          N/A
Max2              4.30          -6.69      60           N/A          N/A
Max1              4.50           4.00      70           N/A          N/A
 XFP ZR
Min1             -0.50         -24.50      0            N/A          N/A
Min2             -0.80         -24.29      5            N/A          N/A
Max2              4.30          -6.69      60           N/A          N/A
Max1              4.50           4.00      70           N/A          N/A
```

```
 Rx_only_WDM_XENPAK
Min1            N/A         -24.50        0             N/A          N/A
Min2            N/A         -24.29        5             N/A          N/A
Max2            N/A          -6.69        60            N/A          N/A
Max1            N/A           4.00        70            N/A          N/A
 XENPAK_ER
Min1           -5.00        -16.50        0             N/A          N/A
Min2           -4.69        -15.80        5             N/A          N/A
Max2            4.00         -0.50        60            N/A          N/A
Max1            4.50          0.00        70            N/A          N/A
 X2_ER
Min1           -5.00        -16.50        0             N/A          N/A
Min2           -4.69        -15.80        5             N/A          N/A
Max2            4.00         -0.50        60            N/A          N/A
Max1            4.50          0.00        70            N/A          N/A
 XFP_ER
Min1           -5.00        -16.50        0             N/A          N/A
Min2           -4.69        -15.80        5             N/A          N/A
Max2            4.00         -0.50        60            N/A          N/A
Max1            4.50          0.00        70            N/A          N/A
 XENPAK_LR
Min1           -8.50        -15.00        0             N/A          N/A
Min2           -8.19        -14.39        5             N/A          N/A
Max2            0.50          0.50        60            N/A          N/A
Max1            1.00          1.00        70            N/A          N/A
 X2_LR
Min1           -8.50        -15.00        0             N/A          N/A
Min2           -8.19        -14.39        5             N/A          N/A
Max2            0.50          0.50        60            N/A          N/A
Max1            1.00          1.00        70            N/A          N/A
 XFP_LR
Min1           -8.50        -15.00        0             N/A          N/A
Min2           -8.19        -14.39        5             N/A          N/A
Max2            0.50          0.50        60            N/A          N/A
Max1            1.00          1.00        70            N/A          N/A
 XENPAK_LW
Min1           -8.50        -15.00        0             N/A          N/A
Min2           -8.19        -14.39        5             N/A          N/A
Max2            0.50          0.50        60            N/A          N/A
Max1            1.00          1.00        70            N/A          N/A
 X2_LW
Min1           -8.50        -15.00        0             N/A          N/A
Min2           -8.19        -14.39        5             N/A          N/A
Max2            0.50          0.50        60            N/A          N/A
Max1            1.00          1.00        70            N/A          N/A
 X2 SR
Min1          -11.30        -13.89        -4            N/A          N/A
Min2           -7.30         -9.89        0             N/A          N/A
Max2           -1.00         -1.00        70            N/A          N/A
Max1            3.00          3.00        74            N/A          N/A
 XFP SR
Min1          -10.30        -12.89        0             N/A          N/A
Min2           -7.30         -9.89        5             N/A          N/A
Max2           -1.00         -1.00        60            N/A          N/A
Max1            2.00          2.00        70            N/A          N/A
 CWDM_SFP
Min1           -4.00        -32.00        -4           84.00         3.00
Min2            0.00        -28.00        0            70.00         3.09
Max2            5.00         -7.00        85            4.00         3.50
Max1            8.00         -3.00        90            2.00         3.59
 SX_SFP
Min1          -10.00        -17.50        -5            N/A          3.00
Min2           -9.50        -17.00        0             N/A          3.09
Max2           -4.00          0.00        75            N/A          3.59
```

```
Max1             -3.50          0.00        85            N/A          3.70
 LX_SFP
Min1            -10.00        -19.50        -5            N/A          3.00
Min2             -9.50        -19.00        0             N/A          3.09
Max2             -3.00         -3.00        75            N/A          3.59
Max1             -2.50          0.00        85            N/A          3.70
 ZX_SFP
Min1             -5.00        -24.00        -5            N/A          3.00
Min2              0.00        -23.00        0             N/A          3.09
Max2              5.00         -3.00        75            N/A          3.59
Max1              5.50          5.00        85            N/A          3.70
 EX_SFP
Min1             -5.00        -25.00        -45           N/A          3.00
Min2             -1.00        -22.50        -15           N/A          3.09
Max2              3.00          1.00        95            N/A          3.59
Max1              6.00          4.00        97            N/A          3.70
 GigE BX D SFP
Min1              N/A           N/A         0             N/A          N/A
Min2              N/A           N/A         0             N/A          N/A
Max2              N/A           N/A         0             N/A          N/A
Max1              N/A           N/A         0             N/A          N/A
 X2 LRM
Min1            -10.50        -12.39        -4            N/A          N/A
Min2             -6.50         -8.39        0             N/A          N/A
Max2              0.50          0.50        70            N/A          N/A
Max1              3.00          3.00        74            N/A          N/A
```

Example: Displaying Threshold Violations

This example shows how to display the threshold violations for all transceivers on a Cisco ASR 901 router:

```
Router# show interfaces transceiver threshold violations
Rx: Receive, Tx: Transmit.
DDDD: days, HH: hours, MM: minutes, SS: seconds
                          Time since Last Known
          Time in slot    Threshold Violation     Type(s) of Last Known
Port      (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS)        Threshold Violation(s)
--------- --------------- ----------------------  ----------------------
Gi0/10     0000:02:50:19    Not applicable        Not applicable
Gi0/11     0000:02:51:15                          Rx power low alarm
                                                -31.0 dBm < -17.1 dBm
```

Example: Displaying Threshold Violations on a Specific Interface

This example shows how to display violations for the transceiver on a specific interface:

```
Router# show interfaces GigabitEthernet 0/9 transceiver

ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                           Optical   Optical
           Temperature  Voltage  Current   Tx Power  Rx Power
Port       (Celsius)    (Volts)  (mA)      (dBm)     (dBm)
---------  -----------  -------  --------  --------  --------
Gi0/9        32.5       3.20     385.1      -5.5      -5.0
```

Example: When Transceiver Monitoring is Disabled

This example shows how to disable transceiver monitoring for all transceivers:

```
Router(config-xcvr-type)# no monitoring
```

This example shows the sample output when transceiver monitoring is disabled:

```
Router# show interfaces transceiver detail
Transceiver monitoring is disabled for all interfaces.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
                              High Alarm  High Warn  Low Warn   Low Alarm
           Temperature        Threshold   Threshold  Threshold  Threshold
Port       (Celsius)          (Celsius)   (Celsius)  (Celsius)  (Celsius)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       34.1                  85.0       75.0        0.0       -5.0
Gi0/11       32.8                  85.0       75.0        0.0       -5.0
                              High Alarm  High Warn  Low Warn   Low Alarm
           Voltage            Threshold   Threshold  Threshold  Threshold
Port       (Volts)            (Volts)     (Volts)    (Volts)    (Volts)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       3.25                  3.70       3.59       3.09       3.00
Gi0/11       3.23                  3.70       3.59       3.09       3.00
                              High Alarm  High Warn  Low Warn   Low Alarm
           Current            Threshold   Threshold  Threshold  Threshold
Port       (milliamperes)     (mA)        (mA)       (mA)       (mA)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10      533.9                   N/A        N/A        N/A        N/A
Gi0/11      391.1                   N/A        N/A        N/A        N/A
           Optical            High Alarm  High Warn  Low Warn   Low Alarm
           Transmit Power     Threshold   Threshold  Threshold  Threshold
Port       (dBm)              (dBm)       (dBm)      (dBm)      (dBm)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       -4.5                  -3.5       -4.0       -9.5      -10.0
Gi0/11       -5.5                  -3.5       -4.0       -9.5      -10.0
           Optical            High Alarm  High Warn  Low Warn   Low Alarm
           Receive Power      Threshold   Threshold  Threshold  Threshold
Port       (dBm)              (dBm)       (dBm)      (dBm)      (dBm)
---------  -----------------  ----------  ---------  ---------  ---------
Gi0/10       -5.2                   0.0        0.0      -17.0      -17.1
Gi0/11       -7.5                   0.0        0.0      -17.0      -17.1
```

Example: Displaying SFP Details

The following is the sample output from the **show controller gig0/x** command.

```
Router# show controllers gig0/4
Switch Unit: 0    port: 10
PHY info:
       0x00: 0x1140    0x01: 0x79ED    0x02: 0x0362    0x03: 0x5DB1
       0x04: 0x0581    0x05: 0xC001    0x06: 0x006F    0x07: 0x2001
       0x08: 0x4FF5    0x09: 0x0600    0x0A: 0x7800    0x0B: 0x0000
       0x0C: 0x0000    0x0D: 0x0000    0x0E: 0x0000    0x0F: 0x3000
       0x10: 0x0001    0x11: 0x0F00    0x12: 0x0003    0x13: 0xFFFF
       0x14: 0x0707    0x15: 0x0000    0x16: 0x0000    0x17: 0x0F04
       0x18: 0x7067    0x19: 0xFF1C    0x1A: 0x257F    0x1B: 0xFFFF
       0x1C: 0x7EA8    0x1D: 0x064C    0x1E: 0x0000    0x1F: 0x0000
```

```
== SFP EEPROM content ==
Reg 0x00:   03  04  07  00  00  00  02  00
Reg 0x08:   00  00  00  01  0D  00  0A  64
Reg 0x10:   37  37  00  00  43  49  53  43
Reg 0x18:   4F  2D  53  55  4D  49  54  4F
Reg 0x20:   4D  4F  20  20  00  00  00  5F
Reg 0x28:   53  43  50  36  47  34  34  2D
Reg 0x30:   43  31  2D  42  4D  48  20  20
Reg 0x38:   41  20  20  20  05  1E  00  28
Reg 0x40:   00  1A  00  00  53  50  43  31
Reg 0x48:   35  32  34  30  43  50  36  20
Reg 0x50:   20  20  20  20  31  31  30  36
Reg 0x58:   31  32  43  38  68  F0  01  64
Reg 0x60:   00  00  0B  CC  81  5C  0A  9E
Reg 0x68:   3B  41  84  F5  19  46  DD  C3
Reg 0x70:   BC  EB  9E  00  00  00  00  00
Reg 0x78:   00  00  00  00  A3  0A  62  04
Reg 0x80:   00
  identifier            0x03 (SFP)
  connector             0x07 (LC)
  sfp_transceiver_code  0x02 (1000BaseLX)
  encoding              0x01 (8B10B)
  br_nominal   (100MHz) 13
  length_9km   (100m)   10
  length_9m    (100m)   100
  length_50m   (100m)   55
  length_62_5m (100m)   55
  length_cu    (10m)    0
  vendor_name           CISCO-SUMITOMO
  vendor_oui            0x00 00 5F
  vendor_pn             SCP6G44-C1-BMH
  vendor_rev            A
  cc_base               0x28
  options[0]            0x00000000
  options[1]            0x0000001A
  br_max (%)            0
  br_min (%)            0
  vendor_sn             SPC15240CP6
  date_code             110612C8 (yymmddvv, v=vendor specific)
  cc_ext                0x64
  DOM support           yes
```

Additional References

The following sections provide references to digital optical monitoring feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Autonomic Networking commands	Cisco IOS Autonomic Networking Command Reference

Technical Assistance

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

Feature Information for Digital Optical Monitoring

Table 47: Feature Information for Digital Optical Monitoring, on page 764 lists the features in this module and provides links to specific configuration information.

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 Table 47: Feature Information for Digital Optical Monitoring, on page 764 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 47: Feature Information for Digital Optical Monitoring

Feature Name	Releases	Feature Information
Support for Digital Optical Monitoring on Cisco ASR 901 Router	15.2(2)SNI	This feature was introduced on the Cisco ASR 901 router. The following sections provide information about this feature:

CHAPTER 42

IPv4 Multicast

This feature module describes how to configure IP multicast in an IPv4 network. IP multicast is an efficient way to use network resources, especially for bandwidth-intensive services such as audio and video.

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 table at the end of this module.

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 IPv4 Multicast

- Cisco IOS Release 15.4(1)S or a later release that supports the IPv4 Multicast feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You must enable the **asr901-multicast source** command on the SVI interface that is connected to the traffic source for PIM sparse mode.

Restrictions for IPv4 Multicast

- Source Specific Multicast (SSM) mapping takes a group G join from a host and identifies this group with an application associated with one or more sources. The SSM mapping can support only one such application per group G.
- When both SSM mapping and Internet Group Management Protocol Version 3 (IGMPv3) are enabled and the hosts already support IGMPv3 (but source specific information is not present), they start sending IGMPv3 group reports. These IGMPv3 group reports are not supported with SSM mapping and the router does not correctly associate sources with these reports.
- PIM Dense Mode is not supported.
- Only PIM version 2 is supported.
- PIM SM in VRF lite is not supported.
- Time-To-Live (TTL) threshold is not supported.
- Mroute ageing is not supported.
- Bi-Directional PIM (BIDIR-PIM) is not supported.
- Mroute based counter or rate statistics are not supported. Multicast counters are not supported.
- Multicast counters on physical and SVI interfaces are not supported till Cisco IOS Release 15.5(1)S.
- Multicast VPN (MVPN) is not supported.
- Multicast is *not* supported on Serial and MLPPP interfaces.
- PIM SSM IPv4 Multicast routing for VRF lite is supported only from Cisco IOS Release 15.4(3)S.
- Multiple L3 SVI interfaces on PoCH as replication VLAN's for multicast traffic are not supported.
- IP Multicast on loopback interface is not supported.

Information About IPv4 Multicast

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packets and IP multicast routers and multilayer switches forward the incoming IP multicast packets out of all interfaces that lead to the members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

Effective with Cisco IOS Release 15.4(1)S, IPv4 multicast is supported on the Cisco ASR 901 series routers. The router supports up to 500 unique multicast IP address entries, which includes both (*, G) and (S, G) entries. Multicast support is provided for source and multicast groups using IGMP (IGMPv1 or IGMPv2 or IGMPv3) report messages.

For more information on IP Multicast Technology, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html.

Supported Protocols

- Basic multicast routing
- IP Multicast Routing for VRF Lite
- IGMP
- PIMv4 SSM
- PIMv4 SSM Mapping
- PIM MIB
- PIM sparse mode
- PIM BFD
- Static Rendezvous Point (RP)
- Auto RP
- Bootstrap router (BSR)

PIM SSM for IPv4

PIM SSM is the routing protocol that supports the implementation of SSM and is derived from the PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMPv3 supports source filtering, which is required for SSM. In order for SSM to run with IGMPv3, SSM must be supported in the device (the host where the application is running) and in the application itself.

Source Specific Multicast

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569 . The following two components together support SSM:

- PIM SSM
- IGMPv3

Protocol Independent Multicast

The PIM protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent, and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the RPF check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

For more information on SSM and PIM, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html

PIM SSM Address Range

SSM can coexist with the Internet Standard Multicast (ISM) service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Cisco IOS software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range (unless the application is modified to use explicit (S, G) channel subscription).

For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.

IGMP

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout the network with the use of special multicast queriers and hosts.

For more information on IGMP, see the IP Multicast: IGMP Configuration Guide at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/xe-3s/imc_customizing_igmp.html

IGMPv1

IGMP version 1 is a simple protocol consisting of two messages. It provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.

IGMPv2

IGMP version 2 extends the functionality of IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.

IGMPv3

IGMP version 3 provides for source filtering, which enables a multicast receiver host to signal to a device which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. In addition, IGMPv3 supports the link local address 224.0.0.22, which is the destination IP address for IGMPv3 membership reports; all IGMPv3-capable multicast devices must listen to this address. RFC 3376 defines IGMPv3.

IGMP Snooping

IGMP snooping allows a router to examine IGMP packets and make forwarding decisions based on their content. IGMP, which runs at Layer 3 on a multicast router, generates Layer 3 IGMP queries in subnets where the multicast traffic has to be routed. Using IGMP snooping, the router intercepts IGMP messages from the host and updates its multicast table accordingly.

You can configure the router to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

You can configure the IGMP snooping lookup method for each VLAN. Layer 3 IGMP snooping lookup uses destination IP addresses in the Layer 2 multicast table (This is the default behavior). Layer 2 IGMP snooping lookup uses destination MAC addresses in the Layer 2 multicast table.

For more information on IGMP snooping, see the *IPv4 Multicast IGMP Snooping* document at: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/ipv4_igmp_snooping.html

IGMP Snooping Support

IGMP snooping is supported with the following specifics:

- Source-specific IGMP snooping is not supported.
- When IGMP snooping is configured, unknown multicast packets are flooded to the BD.
- The **ip igmp snooping tcn flood** and **ip igmp snooping tcn query solicit** commands are not supported.

Layer 2 VPN on the Physical Interface

- Default and port-based Xconnet—IGMP packets (control and data) are sent over the L2 VPN session.
- Dot1Q based Xconnect—If Xconnect is configured for a customer VLAN, IGMP packets (control and data) are carried into an L2 VPN. If they are not IGMP control packets, they are handled as reserved multicast packets in the BD VLAN, and data packets are forwarded according to the data in the IGMP snooping tables.

Layer 3 IP Multicast with IP IGMP Snooping

- Flows destined for PIM Sparse Mode-enabled and PIM Source-Specific Multicast-enabled groups are forwarded using Layer 3 IP Multicast logic.
- Flows destined for groups that are populated using IGMP snooping table are forwarded using IGMP snooping forward logic.
- Flows that are common (destined to groups that are populated using PIM-SM or PIM-SSM and IGMP snooping):
    - The accept interface of PIM-SM or PIM-SSM Multicast Forwarding Information Base (MFIB) is the same as the BD VLAN in which IGMP snooping based forwarding takes place.
    - Layer 3 forwarding takes place using output Layer 3 interface of PIM-SM or PIM-SSM MFIB.
    - Layer 2 forwarding takes place using the output ports from the IGMP snooping logic.

REP and MSTP Interworking

- After the Resilient Ethernet Protocol (REP) and Multiple Spanning Tree Protocol (MSTP) topology change, the routers in the ring generate IGMP general queries, and the convergence is based on the host replying to the general queries.

The following are supported as part of IGMP snooping:

- IGMP report and query processing
- IPv4 IGMP snooping

- Packet forwarding at hardware within bridge domain using IP multicast address lookup and IPv4 IGMP information.

PIM SSM Mapping

PIM SSM mapping supports SSM transition in cases where neither the URD nor IGMP v3lite is available, or when supporting SSM on the end system is not feasible. SSM mapping enables you to leverage SSM for video delivery to legacy set-top boxes (STBs) that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack. URD and IGMPv3lite are applications used on receivers which do not have SSM support.

SSM mapping introduces a means for the last hop router to discover sources sending to groups. When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the router translates this report into one or more (S, G) channel memberships for the well-known sources associated with this group.

SSM mapping only needs to be configured on the last hop router connected to receivers. No support is needed on any other routers in the network. When the router receives an IGMPv1 or IGMPv2 membership report for a group G, the router uses SSM mapping to determine one or more source IP addresses for the group G. SSM mapping then translates the membership report as an IGMPv3 report INCLUDE (G, [S1, G], [S2, G]...[Sn, G] and continues as if it had received an IGMPv3 report.

Static SSM Mapping

SSM static mapping enables you to configure the last hop router to use a static map to determine the sources sending to groups. Static SSM mapping requires that you configure access lists (ACLs) to define group ranges. The groups permitted by those ACLs then can be mapped to sources using the **ip igmp static ssm-map** command.

For more information on SSM Mapping, see the IP Multicast: IGMP Configuration Guide at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/xe-3s/imc_ssm_map.html

Reverse Path Forwarding

Reverse-path forwarding is used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, it means the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM SSM uses source trees to forward datagrams; the RPF check is performed as follows:

- If a PIM router has source-tree state (that is, an [S, G] entry is present in the multicast routing table), the router performs the RPF check against the IPv4 address of the source of the multicast packet.
- Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S, G) joins (which are source-tree states) are sent toward the source.

For more information on Reverse Path Forwarding, see the *Configuring Unicast Reverse Path Forwarding* document at: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

IP Multicast VRF Lite

The IP Multicast VRF Lite feature provides IPv4 multicast support for multiple virtual routing and forwarding (VRF) contexts. The scope of these VRFs is limited to the router in which the VRFs are defined.

This feature enables separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless explicitly configured. The IPv4 Multicast VRF Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF.

PIM BFD

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols and independent of the higher layer protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier and reconvergence time is consistent and predictable.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new neighbors and for detecting failures between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM Hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed.

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers just once for both PIM and IPv6 PIM.

At PIMs request (as a BFD client), BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature.

Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

Configuring IPv4 Multicast

Enabling IPv4 Multicast Routing

To configure IPv4 multicast on the Cisco ASR 901 series routers, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables the privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables multicast routing.
Step 4	**asr901-platf-multicast enable** **Example:** `Router(config)# asr901-platf-multicast enable`	Enables multicast on the Cisco ASR 901 series routers.
Step 5	**ip pim rp-address** *rp-address* **Example:** `Router(config)# ip pim rp-address 192.168.0.1`	Configures the address of a PIM RP for multicast groups.
Step 6	**interface** *type number* **Example:** `Router(config)# interface vlan 5`	Configures the interface type and enters interface configuration mode.
Step 7	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables the PIM sparse mode.
Step 8	**asr901-multicast source** **Example:** `Router(config-if)# asr901-multicast source`	Configures the router to send multicast packets to the CPU enabling it to transmit register packets to the RP. **Note** This command should be enabled on the SVI which is facing the source and is applicable only for PIM SM.

Configuring PIM SSM

To configure PIM SSM, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip pim ssm [default | range** *access-list***]** **Example:** `Router(config-if)# ip pim ssm default`	Configures SSM service. The **default** keyword defines the SSM range access list. The **range** keyword specifies the standard IP access list number or name that defines the SSM range.
Step 4	**interface** *type number* **Example:** `Router(config)# interface vlan 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface.
Step 6	**ip igmp version 3** **Example:** `Router(config-if)# ip igmp version 3`	Enables IGMPv3 on an interface.

Configuring PIM SSM Mapping

To configure PIM SSM mapping, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip igmp ssm-map query dns** **Example:** `Router(config)# no ip igmp ssm-map query dns`	Disables DNS-based SSM mapping.
Step 4	**ip igmp ssm-map enable** **Example:** `Router(config)# ip igmp ssm-map enable`	Enables SSM mapping for groups in the configured SSM range.
Step 5	**ip igmp ssm-map static** *access-list source-address* **Example:** `Router(config)# ip igmp ssm-map static 11 172.16.8.11`	Configures static SSM mapping.

Configuring Multicast Receivers in VRF Interface

The Cisco ASR 901 router supports multicast receivers in VRF interface, if source and RP are present in the global routing table. To configure multicast receivers in VRF interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mroute vrf** *vrf-name source-address mask* **fallback-lookup global** **Example:**	Configures the RPF lookup originating in Multicast Receiver VRF interface to continue and to be resolved in global routing table using static mroute.

	Command or Action	Purpose
	`Router(config)# ip mroute vrf ABC 100.0.0.2 255.255.255.255 fallback-lookup global`	• **vrf**—Configures a static mroute in the MVRF instance specified for the *vrf-name* argument. • *source-address*—IP route prefix or explicit IP address of the source. • *mask*—Mask associated with the IP address or IP route prefix. • **global**—Specifies that the Multicast Source is in the global routing table.
Step 4	**end** **Example:** `Router(config)# end`	Exits the global configuration mode.

Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

Restrictions

Cisco ASR 901 routers support only the following encapsulations for IGMP snooping.

- Untagged
- Dot1q (with or without rewrite)
- Routed QinQ (with rewrite pop 2)

These sections describe how to configure IGMP snooping:

Enabling IGMP Snooping Globally

IGMP snooping is enabled by default. If IGMP snooping is disabled, to globally enable IGMP snooping on the router, perform this procedure:

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ip igmp snooping** **Example:** `Router(config)# ip igmp snooping`	Enables IGMP snooping globally.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling IGMP Snooping on a VLAN

To enable IGMP snooping on a VLAN, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping** **Example:** `Router(config)# ip igmp snooping`	Enables IGMP snooping globally.
Step 4	**ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# ip igmp snooping vlan 102`	Enables IGMP snooping on the VLAN. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring an IGMP Snooping Query

To configure IGMP snooping query characteristics for a router or for a VLAN, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**asr901-platf-multicast enable** **Example:** `Router(config)# asr901-platf-multicast enable`	Enables multicast on the Cisco ASR 901 Router.
Step 4	**ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# ip igmp snooping vlan 5`	Enables IGMP snooping on a VLAN. • *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 5	**ip igmp snooping vlan** *vlan-id* **check rtr-alert-option** **Example:** `Router(config)# ip igmp snooping vlan 5 check rtr-alert-option`	Enforces IGMP snooping check and enables a device or interface to intercept packets only if the Router Alert (rtr-alert) option is enabled.
Step 6	**ip igmp snooping vlan** *vlan-id* **check ttl** **Example:** `Router(config)# ip igmp snooping vlan 5 check ttl`	Accepts IGMP packets with TTL=1.
Step 7	**ip igmp snooping vlan** *vlan-id* **immediate-leave** **Example:** `Router(config)# ip igmp snooping vlan 5 immediate-leave`	Minimizes the leave latency of IGMP memberships when IGMP Version 2 is used and only one receiver host is connected to each interface.

	Command or Action	Purpose
Step 8	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *interval* **Example:** `Router(config)# ip igmp snooping vlan 5 last-member-query-count-count 3`	Configures how often IGMP snooping sends query messages when an IGMP leave message is received. • *interval*—The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.
Step 9	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *interval* **Example:** `Router(config)# ip igmp snooping vlan 5 last-member-query-interval 100`	Sets the last member query interval of the bridge domain. • *interval*—Length of time, in milliseconds, after which the group record is deleted if no reports are received. The default is 1000.
Step 10	**ip igmp snooping vlan** *vlan-id* **report-suppression** **Example:** `Router(config)# ip igmp snooping vlan 5 report-suppression`	Enables report suppression on the bridge domain.
Step 11	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *variable* **Example:** `Router(config)# ip igmp snooping vlan 5 robustness-variable 2`	Sets the robust variable for the bridge domain. • *variable*—Robustness variable number. The range is from 1 to 3. The default is 2.
Step 12	**ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-name interface-number* **Example:** `Router(config)# ip igmp snooping vlan 106 static 226.1.1.2 interface gigabitEthernet 0/10`	Configures static group membership entries on an interface. • *ip-address*—IP address of the IGMP snooping group. • **interface**—Specifies that one or more interfaces configured to a static router port are to be added to the group being configured.
Step 13	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Disabling IGMP Snooping

To disable IGMP snooping, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip igmp snooping** **Example:** `Router(config)# no ip igmp snooping`	Disables IGMP snooping.
Step 4	**no ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# no ip igmp snooping vlan 10`	Disables IGMP snooping from a VLAN.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring IPv4 Multicast Routing for VRF Lite

To configure IPv4 multicast routing for VRF Lite, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpe_1`	Names the VRF and enters VRF configuration mode. The *vrf-name*is the name assigned to a VRF. **Note**

	Command or Action	Purpose
		Configure the **ip pim vrf** *vrf-name* **ssm default** command on the Last Hop Router (LHR).
Step 4	**vrf definition** *vrf-name* **Example:** `Router(config-vrf)# vrf definition vpe_1`	Configures a VRF routing table instance and enters VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1.1.1.1:100`	Specifies a route distinguisher (RD) for a VRF instance. The *route-distinguisher*is an 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.
Step 6	**address-family ipv4** **Example:** `Router(config-vrf)# address-family ipv4`	Specifies the address family submode for configuring routing protocols.
Step 7	**exit address-family** **Example:** `Router(config-router-af)# exit address-family`	Exits the address family submode.

Enabling a VRF Under the VLAN Interface

To configure a VRF under the VLAN interface, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Router(config-if)# vrf forwarding vpe_1`	Associates a VRF instance or a virtual network with an interface or subinterface. The *vrf-name* is the name assigned to a VRF.

	Command or Action	Purpose
Step 5	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 192.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 6	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface. The **sparse-mode** keyword enables sparse mode of operation.
Step 7	**ip ospf** *process-id* **area** *area-id* **Example:** `Router(config-if)# ip ospf 1 area 0`	Enables OSPFv2 on an interface . • *process-id*—A decimal value in the range 1 to 65535 that identifies the process ID. • *area-id*—A decimal value in the range 0 to 4294967295, or an IP address.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 9	**ip pim vrf** *vrf-name* **ssm default** **Example:** `Router(config)# ip pim vrf vpe-1 ssm default`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses. • *vrf-name*—Name assigned to the VRF. • **default**—Defines the SSM range access list to 232/8.. **Note** This command should be configured on the Last Hop Router (LHR).

Configuring PIM BFD on an IPv4 Interface

To configure PIM BFD on an IPv4 interface, perform this task:

Restriction

- This feature is supported only on switch virtual interfaces on which both PIM and BFD are supported.
- For ECMP, PIM BFD is used to detect quick neighbor failure.
- For non-ECMP, BFD for IGP should be configured for faster convergence.
- Timers that are less than 50 ms for 3 sessions are not supported.

Before you begin

- IP multicast must be enabled and Protocol Independent Multicast (PIM) must be configured on the interface.

• Ensure that Bidirectional Forwarding Detection (BFD) for IGP is always configured along with PIM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ip pim bfd** **Example:** `Router(config-if)# ip pim bfd`	Enables PIM BFD on an interface.

Verifying IPv4 Multicast Routing

Use the following **show** command to verify the IPv4 multicast routing.

```
Router# show asr901 multicast-support

Platform support for IPv4(v6) Multicast: ENABLED
```

Verifying PIM SSM

Use the **show** commands listed below to verify the PIM SSM configuration.

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the **show ip igmp groups** command described in the following example.

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1         Vlan70                  04:10:01  stopped   70.1.1.10
224.0.1.40        Vlan16                  04:17:35  00:02:58  16.1.1.3
224.0.1.40        Vlan23                  05:08:03  00:02:54  23.1.1.1
```

To display the contents of the IP multicast routing table, use the **show** command described in the following example.

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(9.1.1.1, 232.1.1.1), 00:00:03/00:02:57, flags: sTI
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan70, Forward/Sparse, 00:00:04/00:02:56
(5.1.1.1, 232.1.1.1), 00:00:04/00:02:56, flags: sTI
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan70, Forward/Sparse, 00:00:04/00:02:56
(*, 224.0.1.40), 00:00:12/00:02:47, RP 6.6.6.6, flags: SJCL
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan23, Forward/Sparse, 00:00:12/00:02:47
```

Verifying PIM SSM Mapping

Use the **show** commands listed below to verify the PIM SSM Mapping configuration.

To display information about SSM mapping, use the **show** command described in the following example.

```
Router# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Disabled
Cast domain : ssm-map.cisco.com
Name servers : 255.255.255.255
```

To display the sources that SSM mapping uses for a particular group, use the show command described in the following example.

```
Router# show ip igmp ssm-mapping 232.1.1.1

Group address: 232.1.1.1
Database     : Static
Source list  : 5.1.1.1
               9.1.1.1
```

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the show command described in the following examples.

- **show ip igmp groups group-address**

```
Router# show ip igmp groups 232.1.1.1

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1        Vlan70                   04:14:26  stopped   70.1.1.10
```

- **show ip igmp groups interface-type** *interface-number*

```
Router# show ip igmp groups vlan70

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1        Vlan70                   04:15:33  stopped   70.1.1.10
```

- **show ip igmp groups interface-type detail**

```
Router# show ip igmp groups vlan70 detail

Flags: L - Local, U - User, SG - Static Group, VG - Virtual Group,
       SS - Static Source, VS - Virtual Source,
       Ac - Group accounted towards access control limit
Interface:      Vlan70
Group:          232.1.1.1
Flags:          SSM
Uptime:         04:15:37
Group mode:     INCLUDE
Last reporter:  70.1.1.10
CSR Grp Exp:    00:02:04
Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, M - SSM Mapping, L - Local,
                    Ac - Channel accounted towards access control limit)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  5.1.1.1          04:15:37  stopped   00:02:04  Yes  CM
  9.1.1.1          04:15:37  stopped   00:02:04  Yes  CM
```

Verifying Static Mroute

To display information about static mroute, use the **show ip mroute [vrf** *vrf-name*] *group-address* command described in the following examples.

```
Router# show ip mroute

mroute vrf VPN_A 239.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
```

```
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.1), 00:03:57/stopped, RP 4.4.4.4, flags: SJCL
  Incoming interface: Vlan21, RPF nbr 21.1.1.1, using vrf IPv4 default
  Outgoing interface list:
    Vlan72, Forward/Sparse, 00:03:56/00:02:10

(70.1.1.10, 239.1.1.1), 00:00:49/stopped, flags: LT
  Incoming interface: Vlan22, RPF nbr 22.1.1.2, using vrf IPv4 default
  Outgoing interface list:
    Vlan72, Forward/Sparse, 00:00:49/00:02:10
```

Verifying IGMP Snooping

Use the show commands listed below to verify the IGMP snooping configuration.

To display the IGMP snooping configuration of a device, use the **show ip igmp snooping** command, as shown in the following example:

```
Router# show ip igmp snooping

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 101:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes

Vlan 102:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes

Vlan 105:
```

```
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
```

To display the IGMP snooping configuration, use the **show ip igmp snooping vlan** *bridge-domain* command, as shown in the following example:

```
Router# show ip igmp snooping vlan 105

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 105:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
Query Interval                      : 0
Max Response Time                   : 10000
```

To display the IGMP snooping configuration, use the **show ip igmp snooping groups** command, as shown in the following examples:

```
Router# show ip igmp snooping groups

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan Group/source Type Version Port List
-----------------------------------------------------------------------
104 232.0.0.5 I v3 Gi0/0
104 232.0.0.6 I v3 Gi0/0
104 232.0.0.7 I v3 Gi0/0
104 232.0.0.8 I v3 Gi0/0
104 232.0.0.9 I v3 Gi0/0


Router# show ip igmp snooping groups vlan 104

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
```

```
Vlan Group/source Type Version Port List
-----------------------------------------------------------------------
104 232.0.0.5 I v3 Gi0/0
104 232.0.0.6 I v3 Gi0/0
104 232.0.0.7 I v3 Gi0/0
104 232.0.0.8 I v3 Gi0/0
104 232.0.0.9 I v3 Gi0/0


Router# show ip igmp snooping groups count

Total number of groups: 6
Total number of (S,G): 0

-----------------------------------------------------------------------
```

Verifying IP Multicast Routing for VRF Lite

Use the **show** commands listed below to verify IPv4 multicast routing for VRF Lite configuration.

To view information about the interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface detail** command:

```
Router# show ip pim vrf vpe_2 interface detail

Vlan80 is administratively down, line protocol is down
  Internet address is 192.108.1.27/24
  Multicast switching: fast
  Multicast packets in/out: 0/0
  Multicast TTL threshold: 0
  PIM: enabled
    PIM version: 2, mode: sparse
    PIM DR: 0.0.0.0
    PIM neighbor count: 0
    PIM Hello/Query interval: 30 seconds
    PIM Hello packets in/out: 0/0
    PIM J/P interval: 60 seconds
    PIM State-Refresh processing: enabled
    PIM State-Refresh origination: disabled
    PIM NBMA mode: disabled
    PIM ATM multipoint signalling: disabled
    PIM domain border: disabled
    PIM neighbors rpf proxy capable: FALSE
    PIM BFD: disabled
    PIM Non-DR-Join: FALSE
  Multicast Tagswitching: disabled
```

To view the information in a PIM topology table, use the **show ip mroute vrf** command:

```
Router# show ip mroute vrf vpe_2

IP Multicast Forwarding is not enabled.
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
```

```
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
```

To view the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB), use the **show ip mfib vrf** command:

```
Router# show ip mfib vrf

Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: C
   SW Forwarding: 0/0/0/0, Other: 8/8/0
 (*,224.0.1.39) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   4106200/12/60/5, Other: NA/NA/NA
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
   Loopback0 Flags: NS
 (4.4.4.4,224.0.1.39) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   876500/12/60/5, Other: NA/NA/NA
   Loopback0 Flags: A
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   5369900/12/60/5, Other: NA/NA/NA
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
   Loopback0 Flags: F IC NS
     Pkts: 0/0
 (2.2.2.2,224.0.1.40) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   200/0/60/0, Other: NA/NA/NA
   Vlan24 Flags: A
   Loopback0 Flags: F IC NS
     Pkts: 0/0
```

```
 (*,232.0.0.1) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Tunnel4 Flags: A
 (70.1.1.10,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 2/0/2
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Tunnel4 Flags: A
   Vlan24 Flags: NS



VRF VPN_C
 (*,224.0.0.0/4) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Vlan131 Flags: IC
 (*,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
 (171.1.1.10,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   923200/12/60/5, Other: NA/NA/NA
   Vlan134 Flags: A
   Vlan131 Flags: F NS
     Pkts: 0/0

VRF VPN_B
 (*,224.0.0.0/4) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   5369300/12/60/5, Other: NA/NA/NA
   Vlan121 Flags: IC
```

Verifying PIM BFD Support

Use the **show** commands listed below to verify PIM BFD support.

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies for an IPv4 neighbor, use the **show bfd neighbors ipv4** command:

```
Router# show bfd neighbors ipv4

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
24.24.24.1 3/3 Up Up Vl24
101.101.101.1 1/3 Up Up Vl101
```

To display BFD's registered clients such as PIM, OSPF, and so on, use the **show bfd neighbors ipv4 details** command:

```
Router# show bfd neighbors ipv4 details

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
```

```
24.24.24.1 3/3 Up Up Vl24
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 24.24.24.2
Handle: 3
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 126(0), Hello (hits): 50(36644)
Rx Count: 36656, Rx Interval (ms) min/max/avg: 1/56/45 last: 24 ms ago
Tx Count: 36647, Tx Interval (ms) min/max/avg: 1/56/46 last: 8 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPF
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 5 last_rx_auth_seq 4
Uptime: 00:27:47
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 3 - Your Discr.: 3
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
101.101.101.1 1/3 Up Up Vl101
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 101.101.101.2
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 126(0), Hello (hits): 50(37036)
Rx Count: 37014, Rx Interval (ms) min/max/avg: 1/56/46 last: 24 ms ago
Tx Count: 37037, Tx Interval (ms) min/max/avg: 1/60/46 last: 0 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPF
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 4 last_rx_auth_seq 6
Uptime: 00:28:03
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 3 - Your Discr.: 1
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0
```

Configuration Examples for IPv4 Multicast

Example: IPv4 Multicast Routing

The following is a sample configuration of IPv4 Multicast routing feature on the Cisco ASR 901 Router:

```
!
Building configuration...
Current configuration : 120 bytes
!
ip multicast-routing
asr901-platf-multicast enable
!
interface Vlan5
 asr901-multicast source
 ip address 22.1.1.2 255.255.255.0
 ip pim sparse-mode
!
end
```

Example: Configuring PIM SSM

The following is a sample configuration of PIM SSM on the Cisco ASR 901 Router:

```
!
Building configuration...
Current configuration : 116 bytes
!
ip multicast-routing
asr901-platf-multicast enable
!
ip pim ssm default
interface Vlan70
ip address 70.1.1.2 255.255.255.0
ip pim sparse-mode
ip igmp version 3
ip ospf 1 area 0
end
```

Example: Configuring PIM SSM Mapping

The following is a sample configuration of PIM SSM Mapping on the Cisco ASR 901 Router:

```
!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
!
ip multicast-routing
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
.
.
.
!
interface vlan10
 description Sample IGMP Interface Configuration for SSM-Mapping Example
 ip address 10.20.1.2 255.0.0.0
 ip pim sparse-mode
 ip igmp static-group 232.1.2.1 source ssm-map
 ip igmp version 3
```

```
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
!
```

Example: Configuring Rendezvous Point

For a sample configuration of RP, see the *Configuring a Rendezvous Point* document at: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Example: Configuring Multicast Receivers in the VRF Interface

The following is a sample configuration multicast receivers in the VRF interface on the Cisco ASR 901 Router:

```
ip mroute vrf ABC 100.0.0.2 255.255.255.255 fallback-lookup global
```

Example: Configuring IGMP Snooping

The following is a sample IGMP snooping configuration:

```
Building configuration...

Current configuration : 3509 bytes
!
.
.
.
asr901-platf-multicast enable
ip multicast-routing
ip igmp snooping explicit-tracking limit 1000
ip igmp snooping vlan 106 immediate-leave
ip igmp snooping vlan 106 robustness-variable 3
ip igmp snooping vlan 106 last-member-query-count 6
ip igmp snooping vlan 106 last-member-query-interval 1000
ipv6 unicast-routing
ipv6 cef
!
.
.
.
```

Example: Configuring IPv4 Multicast Routing for VRF Lite

The following is a sample configuration of IPv4 multicast routing for VRF Lite:

```
!Building configuration...
!
!
```

```
!
!
vrf definition vpe_2
 rd 1.1.1.1:100
 !
 address-family ipv4
 exit-address-family
!
!
!

ip multicast-routing
asr901-platf-multicast enable
license boot level AdvancedMetroIPAccess
!
ip multicast-routing vrf vpe_2
ip pim vrf vpe_2 ssm default
!
interface Vlan80
 vrf forwarding vpe_2
 ip address 192.108.1.27 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 shutdown
!
end
```

Example: Configuring PIM BFD on an IPv4 Interface

The following is a sample configuration of PIMv4 BFD on an interface:

```
Building configuration...

Current configuration : 6735 bytes
!
! Last configuration change at 17:19:42 IST Wed May 21 2014
!
version 15.4
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone IST 5 30
ip cef
!
!
!
!
no ip domain lookup

ip multicast-routing



asr901-platf-multicast enable


interface Loopback1
```

```
ip address 3.3.3.3 255.255.255.255
ip ospf 1 area 0
!

!
interface GigabitEthernet0/0
no ip address
negotiation auto
service instance 24 ethernet
encapsulation dot1q 24
rewrite ingress tag pop 1 symmetric
bridge-domain 24


!
interface Vlan24
ip address 24.24.24.2 255.255.255.0
ip pim sparse-mode
ip pim bfd
ip igmp version 3
bfd interval 50 min_rx 50 multiplier 3

!
router ospf 1
router-id 3.3.3.3
timers throttle spf 50 50 5000
timers throttle lsa 10 20 5000
timers lsa arrival 10
timers pacing flood 5
network 24.24.24.0 0.0.0.255 area 0
network 25.25.25.0 0.0.0.255 area 0
network 55.55.55.0 0.0.0.255 area 0
network 101.101.101.0 0.0.0.255 area 0
bfd all-interfaces

ip pim ssm default



end
```

Troubleshooting Tips

To display IGMP packets received and sent, use the following **debug** command:

```
Router# debug ip igmp
```

To display debugging messages about IGMP snooping, use the following **debug** command:

```
Router# debug ip igmp snooping
```

To display debugging messages about IP PIM, use the following **debug** command:

```
Router# debug ip pim hello
```

To display PIM packets received and sent, and to display PIM-related events for BFD, use the following **debug** command:

```
Router# debug ip pim bfd
```

To display debugging messages about BFD, use the following **debug** command:

```
Router# debug bfd event
```

Note We recommend that you do not use these **debug** commands without TAC supervision.

Additional References

The following sections provide references related to IPv4 Multicast feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference
IP Multicast Technology Overview	IP Multicast: PIM Configuration Guide
Customizing IGMP	IP Multicast: IGMP Configuration Guide
Configuring Unicast Reverse Path Forwarding	Cisco IOS Security Configuration Guide

Standards and RFCs

Standards/RFCs	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 2236	Internet Group Management Protocol, Version 2
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3569	Source-Specific Multicast

MIBs

MIB	MIBs Link
PIM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for IPv4 Multicast

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 48: Feature Information for IPv4 Multicast

Feature Name	Releases	Feature Information
Source Specific Multicast	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** • See the “ Configuring Source Specific Multicast ” chapter of the *IP Multicast: IGMP Configuration Guide*.
Source Specific Multicast Mapping	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the “ SSM Mapping ” chapter of the *IP Multicast: IGMP Configuration Guide*.

Feature Name	Releases	Feature Information
IGMP Version 1	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Version 2	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Version 3	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Snooping	15.4(2)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • IGMP Snooping, on page 768 • Configuring IGMP Snooping, on page 775
IP Multicast VRF Lite	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • IP Multicast VRF Lite, on page 771 • Configuring IPv4 Multicast Routing for VRF Lite, on page 779
BFD Support for Multicast (PIM)	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • PIM BFD, on page 771 • Configuring PIM BFD on an IPv4 Interface, on page 781

CHAPTER 43

IPv6 Multicast

This feature module describes how to configure basic IP multicast in an IPv6 network.

Prerequisites for IPv6 Multicast

- Cisco IOS Release 15.4(1)S or a later release that supports the IPv6 Multicast feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing.

Restrictions for IPv6 Multicast

- PIM Dense Mode is not supported.
- Bidirectional Protocol Independent Multicast (PIM) is not supported.
- You must disable the Source Specific Multicast (SSM) map query dns when static mapping is configured.
- You must configure the **asr901-platf-multicast enable** command to enable multicast on the Cisco ASR 901 router.
- You must enable the **asr901-multicast source** command on the SVI interface that is connected to the traffic source.
- Mroute based counter or rate statistics are not supported. Multicast counters are not supported.
- Multicast VPN (MVPN) is not supported.
- PIM IPv6 SSM in VRF lite is supported only from Cisco IOS release 15.4(3)S.
- PIM IPv6 SM in VRF lite is not supported.
- IPv6 PIM interface counters are not supported till Cisco IOS Release 15.5(1)S.
- Multicast is *not* supported on Serial and MLPPP interfaces.

- Multiple L3 SVI interfaces on PoCH as replication VLAN's for multicast traffic are not supported.
- IP Multicast on loopback interface is not supported.

Information About IPv6 Multicast

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries—receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local device. This signaling is achieved with the MLD protocol.

Devices use the MLD protocol to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use that address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

How active a multicast group is, its duration, and its membership can vary from group to group and from time to time. A group that has members may have no activity.

IPv6 Multicast Groups

An IPv6 address must be configured on an interface for the interface to forward IPv6 traffic. Configuring a site-local or global IPv6 address on an interface automatically configures a link-local address and activates IPv6 for that interface. Additionally, the configured interface automatically joins the following required multicast groups for that link:

- Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104 for each unicast and anycast address assigned to the interface
- All-nodes link-local multicast group FF02::1
- All-routers link-local multicast group FF02::2

IPv6 Multicast Routing Implementation

The Cisco IOS software supports the following protocols to implement IPv6 multicast routing:

- MLD for IPv6: MLD is used by IPv6 routers to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD:
    - MLD version 1 is based on version 2 of the IGMP for IPv4

  - MLD version 2 is based on version 3 of the IGMP for IPv4.

- IPv6 multicast for Cisco IOS software uses both MLD version 2 and MLD version 1. MLD version 2 is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 interoperates with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in PIM SSM has the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

Multicast Listener Discovery Protocol for IPv6

To start implementing multicasting in a network, users must first define who receives the multicast. The MLD protocol is used by IPv6 devices to discover the presence of multicast listeners (for example, nodes that want to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. It is used for discovering local group and source-specific group membership. The MLD protocol provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

The differences between multicast queriers and hosts are as follows:

- A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that send report messages to inform the querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use MLD reports to join and leave multicast groups and to begin receiving group traffic.

MLD uses the Internet Control Message Protocol (ICMP) to carry its messages. All MLD messages are link-local with a hop limit of 1, and they all have the alert option set. The alert option implies an implementation of the hop-by-hop option header.

MLD has three types of messages:

- Query—General, group-specific, and multicast-address-specific. In a query message, the multicast address field is set to 0 when MLD sends a general query. The general query learns which multicast addresses have listeners on an attached link. Group-specific and multicast-address-specific queries are the same. A group address is a multicast address.
- Report—In a report message, the multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- Done—In a done message, the multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

An MLD report must be sent with a valid IPv6 link-local source address, or the unspecified address (::). If the sending interface has not yet acquired a valid link-local address. Sending reports with the unspecified address is allowed to support the use of IPv6 multicast in the Neighbor Discovery Protocol.

For stateless autoconfiguration, a node is required to join several IPv6 multicast groups in order to perform duplicate address detection (DAD). Prior to DAD, the only address the reporting node has for the sending interface is a tentative one, which cannot be used for communication. Therefore, the unspecified address must be used.

MLD states that result from MLD version 2 or MLD version 1 membership reports can be limited globally or by interface. The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. Membership reports in excess of the configured limits are not entered in the MLD cache, and traffic for those excess membership reports are not forwarded.

MLD provides support for source filtering. Source filtering allows a node to report interest in listening to packets only from specific source addresses (as required to support SSM), or from all addresses except specific source addresses sent to a particular multicast address.

When a host using MLD version 1 sends a leave message, the device needs to send query messages to reconfirm that this host was the last MLD version 1 host joined to the group before it can stop forwarding traffic. This function takes about 2 seconds. This “leave latency” is also present in IGMP version 2 for IPv4 multicast.

MLD Snooping

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes looking to receive IPv6 multicast packets) on its directly attached links, and to discover which multicast packets are of interest to neighboring nodes.

Using MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that looks to receive the data, instead of data being flooded to all the ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

For more information on MLD snooping, see the *IPv6 MLD Snooping* document at:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/ipv6_mld_snooping.html

MLD Snooping Support

IP address-based MLD snooping is enabled on the Cisco ASR 901 Routers with the following specifics:

- Source specific MLD snooping is not supported.
- When MLD snooping is configured, unknown multicast packets are flooded to the BD.

Layer 2 VPN on the Physical Interface

- Default and port-based Xconnet—MLD packets (control and data) are sent over an L2 VPN session.
- Dot1Q-based Xconnect—If Xconnect is configured for a customer VLAN, MLD packets (control and data) are carried into an L2 VPN. If they are not MLD control packets they are handled as reserved multicast packets in the BD VLAN, and data packets are forwarded according to the data in the MLD snooping tables.

Layer 3 IP Multicast with IP MLD Snooping

- Flows destined for PIM Sparse Mode-enabled and PIM Source-Specific Multicast-enabled groups are forwarded using Layer 3 IP multicast logic.
- Flows destined for groups that are populated using data in the MLD snooping table are forwarded using MLD snooping forward logic.
- Flows that are common (destined for groups that are populated using PIM-SM or PIM-SSM and MLD snooping):
    - The accept interface of PIM-SM or PIM-SSM Multicast Forwarding Information Base (MFIB) is the same as the BD VLAN in which MLD snooping-based forwarding takes place.
    - Layer 3 forwarding takes place using Layer 3 interface output of PIM-SM or PIM-SSM MFIB.

- Layer 2 forwarding takes place using the output ports from the MLD snooping logic.

The following are supported as part of MLD snooping:

- MLD message processing
- IPv6 MLD snooping
- Packet forwarding at hardware within bridge domain using IP multicast address lookup and IPv6 MLD information.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs. PIM works independently of the unicast routing protocol to perform send or receive multicast route updates like other protocols. Regardless of which unicast routing protocols are being used in the LAN to populate the unicast routing table, Cisco IOS PIM uses the existing unicast table content to perform the Reverse Path Forwarding (RPF) check instead of building and maintaining its own separate routing table.

For more information on PIM, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html

PIM Source Specific Multicast

PIM SSM is the routing protocol that supports the implementation of SSM and is derived from PIM SM. However, unlike PIM SM where data from all multicast sources are sent when there is a PIM join, the SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, thus optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. Further, instead of the use of RP and shared trees, SSM uses information found on source addresses for a multicast group. This information is provided by receivers through the source addresses relayed to the last-hop devices by MLD membership reports, resulting in shortest-path trees directly to the sources.

In SSM, delivery of datagrams is based on the (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IPv6 unicast source address S and the multicast group address G as the IPv6 destination address. Systems receive this traffic by becoming members of the (S, G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources.

MLD version 2 is required for SSM to operate. MLD allows the host to provide source information. Before SSM runs with MLD, SSM must be supported in the Cisco IPv6 device, the host where the application is running, and the application itself.

For more information on PIM Source-Specific Multicast, see the *IP Multicast: PIM Configuration Guide* at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-pim-ssm.html

Source Specific Multicast Mapping for IPv6

SSM mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for MLD version 1 receivers. This feature allows deployment of IPv6 SSM with hosts that are incapable of providing MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application.

SSM mapping allows the device to look up the source of a multicast MLD version 1 report either in the running configuration of the device or from a DNS server. The device can then initiate an (S, G) join toward the source.

For more information on IPv6 Source Specific Multicast Mapping, see the *IP Multicast: PIM Configuration Guide* at:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-ssm-map.html

PIM-Sparse Mode

PIM-SM uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data receive the traffic.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network.

For more information on PIM Sparse Mode, see the *IP Multicast: PIM Configuration Guide* at:
http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/ip6-mcast-pim-sm.html

Rendezvous Point

A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM). The protocol is described in RFC 2362.

For more information on RP, see the Configuring a Rendezvous Point guide at:
http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

The recommended methods for configuring an RP in a PIM-SM network are given below:

- Static RP
- Bootstrap router
- Anycast RP

IPv6 Multicast VRF Lite

The IPv6 Multicast VRF Lite feature provides IPv6 multicast support for multiple virtual routing/forwarding contexts (VRFs). The scope of these VRFs is limited to the router in which the VRFs are defined.

This feature provides separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless it is explicitly configured. The IPv6 Multicast VRF Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF.

Note Only PIM SSM is supported, PIM SM is not supported in VRF Lite.

PIM BFD

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols and independent of the higher layer protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier and reconvergence time is consistent and predictable.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new neighbors and for detecting failures between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM Hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed.

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers just once for both PIM and IPv6 PIM.

At PIMs request (as a BFD client), BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature.

Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

Configuring IPv6 Multicast

Enabling IPv6 Multicast Routing

To enable IPv6 Multicast Routing feature, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ipv6 multicast-routing** *[***vrf** *vrf-name]* **Example:** `Router(config)# ipv6 multicast-routing`	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.
Step 4	**asr901-platf-multicast enable** **Example:**	Enables the platform multicast routing.

	Command or Action	Purpose
	`Router(config)# asr901-platf-multicast enable`	

Disabling IPv6 Multicast Forwarding

This procedure disables IPv6 multicast forwarding on the router. The IPv6 multicast forwarding is turned on by default when IPv6 multicast routing is enabled.

To disable IPv6 multicast forwarding, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**no ipv6 mfib** **Example:** `Router(config)# no ipv6 mfib`	Disables IPv6 multicast forwarding on the router.

Disabling MLD Device-Side Processing

MLD is enabled on every interface when IPv6 multicast routing is configured. This procedure disables MLD router side processing on that interface. The router stops sending MLD queries and stops keeping track of MLD members on the LAN. If the **ipv6 mld join-group** command is configured on this interface, the interface continues with the MLD host functionality and report group membership when MLD query is received.

To turn off MLD device-side processing on a specified interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 105`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**no ipv6 mld router** **Example:** `Router(config)# no ipv6 mld router`	Disables MLD device-side processing on a specified interface.

Configuring MLD Protocol on an Interface

To configure Multicast Listener Discovery Protocol on an interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 mld query-interval** *seconds* **Example:** **Example:** `Router(config-if)# ipv6 mld query-interval 60`	Configures the frequency of MLD Host-Query packets transmitted. A designated router for a LAN is the only router that transmits queries. The default value is 60 seconds.

	Command or Action	Purpose
Step 5	**ipv6 mld query-max-response-time** *seconds* **Example:** `Router(config-if)# ipv6 mld query-max-response-time 20`	Specifies the maximum query response time advertised in the MLD queries. Default value is 10 seconds. Configuring a value less than 10 seconds enables the router to prune groups faster.
Step 6	**ipv6 mld query-timeout** *seconds* **Example:** `Router(config-if)# ipv6 mld query-timeout 130`	Specifies the timeout for the router to take over as the querier for the interface, after the previous querier has stopped querying. The default value is 2 * query-interval. If the router hears no queries for the timeout period, it becomes the querier.
Step 7	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} **Example:** `Router(config-if)# ipv6 mld join-group ff04::12 exclude 2001:DB8::10:11`	Configures MLD reporting for given *group* with MLDv1 or given *source* and *group* with MLDv2. The packets that are addressed to this group address are passed up to the client process in the router as well forwarded out the interface.

Step 8	**ipv6 mld static-group** [*group-address*] [**include | exclude**] {*source-address* | **source-list** [*acl*]}
	Example:
	`Router(config-if)# ipv6 mld static-group`
	`ff04::10 include 100::1`
		Configures forwarding of traffic for the multicast group onto this interface and behave as if an MLD joiner was present on the interface. The packets to the group get fastswitched or hardware switched (whatever is available on the platform).
		Note
		This command is not a sufficient condition for traffic to be forwarded onto the interface. Other conditions such as absence of a route, not being the DR or losing an assert can cause the router to not forward traffic even if the command is configured.

Configuring MLD Snooping

MLD snooping is not enabled by default. You have to configure it globally, which enables snooping on all the VLANs.

You can enable and disable MLD snooping on a per-VLAN basis. However, if you disable MLD snooping globally, it is disabled on all the VLANs. If global snooping is enabled, you can enable or disable VLAN snooping.

Restrictions

Cisco ASR 901 Routers support only the following encapsulations for MLD snooping:

- Untagged
- Dot1q (with or without rewrite)

- Routed QinQ (with rewrite pop 2)

The following commands are not supported: **ipv6 mld snooping tcn flood** and **ipv6 mld snooping tcn query solicit**.

Note In the context of REP and G8032, topology change may cause the routers in the ring topology to trigger general queries that may impact the convergence time (because this time is based on the report received from the host).

Enabling MLD Snooping Globally

To enable MLD snooping globally on the router, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping** **Example:** `Router(config)# ipv6 mld snooping`	Enables MLD snooping globally.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling MLD Snooping on a VLAN

To enable MLD snooping on a VLAN, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping** **Example:** `Router(config)# ipv6 mld snooping`	Enables MLD snooping globally.
Step 4	**ipv6 mld snoopingvlan** *vlan-id* **Example:** `Router(config)# ipv6 mld snooping vlan 1001`	Enables MLD snooping on the VLAN. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring a Static Multicast Group

Hosts or Layer 2 ports normally join multicast groups dynamically. However, you can also statically configure an IPv6 multicast address and member ports for a VLAN.

To add a Layer 2 port as a member of a multicast group, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snoopingvlan** *vlan-id* **static** *ipv6-multicast-address* **interface** *interface-id* **Example:** `Router(config)# ipv6 mld snooping vlan 104`	Configures statically a multicast group with a Layer 2 port as a member of a multicast group: • *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.

	Command or Action	Purpose
	`static FF45::5 interface gigabitethernet0/4`	• *ipv6-multicast-address*— The 128-bit group IPv6 address. The address must be in the form specified in RFC 2373. • *interface-id*—The member port. It can be a physical interface or a port channel.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring a Multicast Router Port

To add a multicast router port to a VLAN, perform this task:

Procedure

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

Step 3	**ipv6 mld snoopingvlan** *vlan-id* **mroute interface** *interface-id*
	Example:
	`Router(config)# ipv6 mld snooping vlan 104`
	`mrouter interface gigabitEthernet 0/4`
		Specifies the multicast router VLAN ID, and the interface of the multicast router.
		• *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
		• *interface-id*—The member port. It can be a physical interface or a port channel.

Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Enabling MLD Immediate Leave

To enable MLDv1 Immediate Leave, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snoopingvlan** *vlan-id* **immediate-leave** **Example:** `Router(config)# ipv6 mld snooping vlan 104 immediate-leave`	Enables MLD Immediate Leave on the VLAN interface.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring an MLD Snooping Query

To configure MLD snooping query characteristics for the router or for a VLAN, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping check hop-count** **Example:** `Router(config)# ipv6 mld snooping check hop-count`	Enables hop-count checking.

	Command or Action	Purpose
Step 4	**ipv6 mld snooping explicit-tracking limit** *limit* **Example:** `Router(config)# ipv6 mld snooping explicit-tracking limit 1000`	Enables explicit host tracking.
Step 5	**ipv6 mld snooping last-listener-query-count** *count* **Example:** `Router(config)# ipv6 mld snooping last-listener-query-count 3`	Sets the last listener query count on a VLAN basis. This value overrides the value configured globally. The range is from 1 to 7. The default is 0. When set to 0, the global count value is used. Queries are sent 1 second apart.
Step 6	**ipv6 mld snooping last-listener-query-interval** *interval* **Example:** `Router(config)# ipv6 mld snooping last-listener-query-interval 1000`	Sets the maximum response time that the switch waits for after sending out a MASQ before deleting a port from the multicast group. The range is from 100 to 32,768 thousandth of a second. The default is 1000 (1 second).
Step 7	**ipv6 mld snooping listener-message-suppression** **Example:** `Router(config)# ipv6 mld snooping listener-message-suppression`	Enables listener message suppression.
Step 8	**ipv6 mld snooping robustness-variable** *interval* **Example:** `Router(config)# ipv6 mld snooping robustness-variable 3`	Sets the number of queries that are sent before the router deletes a listener (port) that does not respond to a general query. The range is from 1 to 3. The default is 2.
Step 9	**ipv6 mld snooping vlan** *vlan-id* **Example:** `Router(config)# ipv6 mld snooping vlan 104`	Enables MLD snooping for VLAN. • *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Disabling MLD Listener Message Suppression

To disable MLD listener message suppression, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ipv6 mld snooping listener-message-suppression** **Example:** `Router(config)# no ipv6 mld snooping listener-message-suppression`	Disables listener message suppression.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring a Rendezvous Point

To configure a rendezvous point (RP) in a Protocol Independent Multicast sparse mode (PIM-SM) network, see the Configuring a Rendezvous Point guide at:

http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

This guide provides scenario descriptions and basic configuration examples for the following options:

- Static RP
- Bootstrap router
- Anycast RP

Configuring PIM SSM Options

To configure PIM Source-Specific Multicast options, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 pim** **Example:** `Router(config-if)# ipv6 pim`	Configures PIM, if it is disabled. PIM runs on every interface after configuring IPv6 multicast routing.
Step 5	**ipv6 pim hello-interval** *interval-in-seconds* **Example:** `Router(config-if)# ipv6 pim hello-interval 45`	Configures periodic hello interval for this interface. Default is 30 seconds. Periodic hellos are sent out at intervals randomized by a small amount instead of on exact periodic interval.
Step 6	**ipv6 pim join-prune-interval** *interval-in-seconds* **Example:** `Router(config-if)# ipv6 pim join-prune-interval 75`	Configures periodic Join-Prune announcement interval for this interface. Default is 60 seconds.

Disabling PIM SSM Multicast on an Interface

To disable PIM SSM multicast on a specified interface, complete the following steps.

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 104`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**no ipv6 pim** **Example:** `Router(config-if)# no ipv6 pim`	Disables PIM on the specified interface.

Configuring IPv6 SSM Mapping

When the SSM mapping feature is enabled, DNS-based SSM mapping is automatically enabled, which means that the device looks up the source of a multicast MLD version 1 report from a DNS server.

You can configure either DNS-based or static SSM mapping, depending on your device configuration. If you choose to use static SSM mapping, you can configure multiple static SSM mappings. If multiple static SSM mappings are configured, the source addresses of all matching access lists are used.

To configure IPv6 SSM mapping, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable** **Example:** `Router(config-if)# ipv6 mld ssm-map enable`	Enables the SSM mapping feature for groups in the configured SSM range. **Note** You should first create ACL to define the group that needs to be mapped.
Step 4	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address* **Example:**	Configures static SSM mappings.

	Command or Action	Purpose
	`Router(config-if)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	
Step 5	**no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns** **Example:** `Router(config-if)# no ipv6 mld ssm-map query dns`	Disables DNS-based SSM mapping. **Note** You must disable SSM-map query dns when static mapping is configured.

Configuring IPv6 Multicast Routing for VRF Lite

To configure IPv6 multicast routing for VRF Lite, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast-routing vrf** *vrf-name* **Example:** `Router(config)# ipv6 multicast-routing vrf vpe_1`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router.
Step 4	**vrf definition***vrf-name* **Example:** `Router(config-vrf)# vrf definition vpe_1`	Configures a VRF routing table instance and enter VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1.1.1.1:100`	Specifies a route distinguisher (RD) for a VRF instance. The *route-distinguisher* is an 8-byte value to be added to an IPv6 prefix to create a VPN IPv6 prefix.
Step 6	**address-family ipv6** **Example:** `Router(config-vrf)# address-family ipv6`	Specifies the address family submode for configuring routing protocols.
Step 7	**exit-address-family** **Example:**	Exits the address family submode.

	Command or Action	Purpose
	Router(config-router-af)# exit-address-family	

Enabling VRF Under a VLAN Interface

To configure VRF under a VLAN interface, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Router(config-if)# vrf forwarding vpe_1`	Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface or subinterface. The *vrf-name* is the name assigned to a VRF.
Step 5	**ipv6 address** *ipv6-address* **Example:** `Router(config-if)# ipv6 address my-prefix 0:0:0:7272::72/64`	Configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.

Configuring PIM BFD on an IPv6 Interface

To configure PIM BFD on an IPv6 interface, perform this task:

Restriction

- This feature is supported only on switch virtual interfaces on which both PIM and BFD are supported.
- For ECMP, PIM BFD is used to detect quick neighbor failure.
- For non-ECMP, BFD for IGP should be configured for faster convergence.
- Timers that are less than 50 ms for 3 sessions are not supported.

Before you begin

- IPv6 multicast must be enabled and Protocol Independent Multicast (PIM) must be configured on the interface.
- Ensure that Bidirectional Forwarding Detection (BFD) for IGP is always configured along with PIM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 pim bfd** **Example:** `Router(config-if)# ipv6 pim bfd`	Enables PIMv6 BFD on an interface.

Verifying IPv6 Multicast

Use the **show** commands listed below to verify the IPv6 Multicast configuration.

To display the group membership information on various interfaces on a router, use the **show** command described in the following example.

```
Router# show ipv6 mld groups

MLD Connected Group Membership
Group Address                             Interface          Uptime    Expires
FF04::10                                  Vlan104            00:18:41  never
FF04::12                                  Vlan104            00:19:10  never
FF34::4                                   Vlan104            00:35:00  not used
FF45::5                                   Vlan104            00:35:04  00:01:44
```

To display the MLD interface specific parameters, use the **show** command described in the following example.

```
Router# show ipv6 mld interface vlan 104

Vlan104 is up, line protocol is up
Internet address is FE80::4255:39FF:FE89:6283/10
MLD is enabled on interface
Current MLD version is 2
```

```
MLD query interval is 60 seconds
MLD querier timeout is 130 seconds
MLD max query response time is 20 seconds
Last member query response interval is 1 seconds
MLD activity: 18 joins, 7 leaves
MLD querying router is FE80::4255:39FF:FE89:6283 (this system)
```

To display the MLD traffic counters, use the **show** command described in the following example.

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared: 02:29:12

                              Received     Sent
Valid MLD Packets               784         385
Queries                         4           167
Reports                         776         218
Leaves                          4           0
Mtrace packets                  0           0

Errors:
Malformed Packets                           0
Martian source                              10
Non link-local source                       0
Hop limit is not equal to 1                 0
```

To display interface specific information for PIM, use the **show** command described in the following example.

```
Router# show ipv6 pim interface

Interface          PIM   Nbr   Hello  DR
                         Count Intvl  Prior

Vlan102            on    1     30     1
    Address: FE80::4255:39FF:FE89:5283
    DR     : FE80::4255:39FF:FE89:5284
Null0              off    0     30     1
    Address: FE80::1
    DR     : not elected
FastEthernet0/0    off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/8 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/9 off    0     30     1
    Address: ::
    DR     : not elected
Gi0/10             off    0     30     1
    Address: ::
    DR     : not elected
Gi0/11             off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/0 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/1 off    0     30     1
    Address: ::
    DR     : not elected
```

```
GigabitEthernet0/2 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/3 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/4 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/5 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/6 off    0     30     1
    Address: ::
    DR     : not elected
GigabitEthernet0/7 off    0     30     1
    Address: ::
    DR     : not elected
Vlan1              off    0     30     1
    Address: ::
    DR     : not elected
Port-channel1      off    0     30     1
    Address: ::
    DR     : not elected
Tunnel0            off    0     30     1
    Address: FE80::7EAD:74FF:FE9D:94C8
    DR     : not elected
Loopback1          off    0     30     1
    Address: ::
    DR     : not elected
Vlan104            on    1     45     1
    Address: FE80::4255:39FF:FE89:6283
    DR     : FE80::4255:39FF:FE89:6284
Tunnel1            off    0     30     1
    Address: FE80::7EAD:74FF:FE9D:94C8
    DR     : not elected
```

To display the number of (*, G) and (S, G) membership reports present in the MLD cache, use the **show** command described in the following example.

```
Router# show ipv6 mld groups summary

MLD Route Summary
  No. of (*,G) routes = 9
  No. of (S,G) routes = 3
```

To display the number of PIM neighbors on each interface, as well as, the total number of PIM neighbors, use the **show** command described in the following example.

```
Router# show ipv6 pim neighbor count

Interface          Nbr count

Vlan104            1
Vlan102            1

Total Nbrs         2
```

To display the number of PIM neighbors discovered, use the **show** command described in the following example.

```
Router# show ipv6 pim neighbor

PIM Neighbor Table
Mode: B - Bidir Capable, G - GenID Capable
Neighbor Address           Interface          Uptime    Expires  Mode DR pri

FE80::4255:39FF:FE89:5284  Vlan102            02:30:51  00:01:38 B G  DR 1
FE80::4255:39FF:FE89:6284  Vlan104            00:09:49  00:01:16 B G  DR 1
```

To display the information in the PIM topology table in a format similar to the **show ip mroute** command, use the show command described in the following example.

```
Router# show ipv6 mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, Y - Joined MDT-data group,
       y - Sending to MDT-data group
       g - BGP signal originated, G - BGP Signal received,
       N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
       q - BGP Src-Active originated, Q - BGP Src-Active received
       E - Extranet
Timers: Uptime/Expires
Interface state: Interface, State

(2006::1, FF34::4), 00:38:41/never, flags: sPTI
  Incoming interface: Vlan102
  RPF nbr: FE80::4255:39FF:FE89:5284
  Immediate Outgoing interface list:
    Vlan104, Null, 00:38:41/never

(100::1, FF04::10), 00:22:21/never, flags: SPI
  Incoming interface: Null
  RPF nbr: ::
  Immediate Outgoing interface list:
    Vlan104, Null, 00:22:21/never

(*, FF04::12), 00:22:50/never, RP 2021::2021, flags: SPCL
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null

(2001:DB8::10:11, FF04::12), 00:22:50/never, RP 2021::2021, flags: SPLRI
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null

(*, FF45::5), 00:38:44/never, RP 2021::2021, flags: SPC
  Incoming interface: Vlan104
  RPF nbr: FE80::4255:39FF:FE89:6284
  Outgoing interface list: Null
```

To display PIM topology table for given group or all groups, use the **show** command described in the following example.

```
Router# show ipv6 pim topology

IP PIM Multicast Topology Table
```

```
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info Upstream Mode
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected, Y - Joined MDT-data group,
    y - Sending to MDT-data group
    BGS - BGP Signal Sent, !BGS - BGP signal suppressed
    SAS - BGP Src-Act Sent, SAR - BGP Src-Act Received
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary, BS - BGP Signal,
    BP - BGP Shared-Tree Prune, BPT - BGP Prune Time

(2006::1,FF34::4)
SSM SPT UP: 00:39:23 JP: Null(never) Flags:
RPF: Vlan102,FE80::4255:39FF:FE89:5284
  Vlan104            00:39:23  off     LI

(100::1,FF04::10)
SM UP: 00:23:04 JP: Null(never) Flags:
RPF: ,::
  Vlan104            00:23:04  off     LI

(*,FF04::12)
SM UP: 00:23:33 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:23:33  off     LI II

(2001:DB8::10:11,FF04::12)
SM RPT UP: 00:23:33 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:23:33  off     LD ID

(*,FF45::5)
SM UP: 00:39:27 JP: Null(never) Flags:
RP: 2021::2021
RPF: Vlan104,FE80::4255:39FF:FE89:6284
  Vlan104            00:39:27  off     LI IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR - Sending Registers,
E - MSDP External, DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF0E::E0:1:1:1)
SM UP: 04:27:50 JP: Join(never) Flags: LH
RP: 51::1:1:2*
RPF: Tunnel1,51::1:1:2*
FastEthernet4/10 04:27:50 fwd Join(00:02:48) LI LH
(47::1:1:3,FF0E::E0:1:1:1)
SM SPT UP: 04:27:20 JP: Join(never) Flags: KAT(00:01:04) AA PA RA SR
RPF: Vlan47,47::1:1:3*
FastEthernet4/10 04:27:16 fwd Join(00:03:14)
Tunnel0 04:27:17 fwd
```

To display the count of the ranges, (*, G), (S, G) and (S, G) RPT routes in the pim topology tables, use the **show** command described in the following example.

```
Router# show ipv6 pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 47
  No. of (*,G) routes = 11
  No. of (S,G) routes = 2
  No. of (S,G)RPT routes = 1
```

To display the IP multicast group mapping table, use the **show** command described in the following example. It shows group to mode mapping and RP information in case of sparse-mode groups.

```
Router# show ipv6 pim group-map FF0E::E0:1:1:1

IP PIM Group Mapping Table
(* indicates group mappings being used)

FF00::/8*
    SM, RP: 2021::2021
    RPF: Vl104,FE80::4255:39FF:FE89:6284
    Info source: Static
    Uptime: 02:33:31, Groups: 3
```

To display the IPv6 multicast range-lists on a per client (config/autorp/BSR) and per mode (SSM/SM/DM/Bidir) basis, use the **show** command described in the following example.

```
Router# show ipv6 pim range-list

Static SSM Exp: never Learnt from : ::
  FF33::/32 Up: 02:33:46
  FF34::/32 Up: 02:33:46
  FF35::/32 Up: 02:33:46
  FF36::/32 Up: 02:33:46
  FF37::/32 Up: 02:33:46
  FF38::/32 Up: 02:33:46
  FF39::/32 Up: 02:33:46
  FF3A::/32 Up: 02:33:46
  FF3B::/32 Up: 02:33:46
  FF3C::/32 Up: 02:33:46
  FF3D::/32 Up: 02:33:46
  FF3E::/32 Up: 02:33:46
  FF3F::/32 Up: 02:33:46
Static SM RP: 2021::2021 Exp: never Learnt from : ::
  FF00::/8 Up: 02:33:44
```

To display information about the PIM register encapsulation and decapsulation tunnels, use the **show** command described in the following example.

```
Router# show ipv6 pim tunnel

Tunnel0*
  Type  : PIM Encap
  RP    : Embedded RP Tunnel
  Source: 2003::2
Tunnel1*
  Type  : PIM Encap
  RP    : 2021::2021
  Source: 2003::2
```

To display information about the PIM traffic counters, use the **show** command described in the following example.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 02:34:35

                              Received     Sent
Valid PIM Packets               613         629
Hello                           613         622
Join-Prune                      0           7
Data Register                   0           -
Null Register                   0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets drops due to PIM queue limits       0
```

To display the average Join/Prune aggregation for the last (1000/10000/50000) packets for each interface, use the **show** command described in the following example.

```
Router# show ipv6 pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          MTU        Transmitted            Received

Vlan102            1500       0    / 0    / 0         0    / 0    / 0
Null0              1500       0    / 0    / 0         0    / 0    / 0
FastEthernet0/0    1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/8 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/9 1280       0    / 0    / 0         0    / 0    / 0
Gi0/10             1280       0    / 0    / 0         0    / 0    / 0
Gi0/11             1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/0 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/1 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/2 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/3 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/4 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/5 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/6 1280       0    / 0    / 0         0    / 0    / 0
GigabitEthernet0/7 1280       0    / 0    / 0         0    / 0    / 0
Vlan1              1280       0    / 0    / 0         0    / 0    / 0
Port-channel1      1280       0    / 0    / 0         0    / 0    / 0
Tunnel0            1452       0    / 0    / 0         0    / 0    / 0
Loopback1          1280       0    / 0    / 0         0    / 0    / 0
Vlan104            1500       0    / 0    / 0         0    / 0    / 0
Tunnel1            1452       0    / 0    / 0         0    / 0    / 0
```

To display the MRIB table, use the **show** command described in the following example. All entries are created by various clients of MRIB, such as, MLD, PIM and MFIB. The flags on each entry or interface, serve as communication mechanism between various clients of MRIB.

```
Router# show ipv6 mrib route FF0E::E0:1:1:1

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
    ME - MoFRR ECMP Flow based, MNE - MoFRR Non-ECMP Flow based,
    MP - Primary MoFRR Non-ECMP Flow based entry
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied, MI - mLDP Interest
    A2 - MoFRR ECMP Backup Accept

(*,FF45::5) RPF nbr: FE80::4255:39FF:FE89:6284 Flags: C
  Vlan104 Flags: A LI
```

To display the count of the number of routes in the Multicast RIB, use the **show** command described in the following example.

```
Router# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 57
  No. of (S,G) routes = 3
  No. of Route x Interfaces (RxI) = 22
```

To display information about the various MRIB clients, use the **show** command described in the following example.

```
Router# show ipv6 mrib client

IP MRIB client-connections
igmp (0x0):309  (connection id 1)
pim (0x0):342   (connection id 2)
IPv6_mfib(0x1031AFB0):0.358     (connection id 3)

2024#show ipv6 mfib ff45::5
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,FF45::5) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Vlan104 Flags: A
```

To display information about the IPv6 Multicast Forwarding Information Base, in terms of forwarding entries and interfaces, use the **show** command described in the following example.

```
Router# show ipv6 mfib FF0E::E0:1:1:1

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF0E::E0:1:1:1) Flags: C
Forwarding: 0/0/0/0, Other: 0/0/0
Tunnel1 Flags: A NS
FastEthernet4/10 Flags: F NS
Pkts: 0/0
(47::1:1:3,FF0E::E0:1:1:1) Flags:
Forwarding: 9592618/0/182/0, Other: 0/0/0
Vlan47 Flags: A
Tunnel0 Flags: F NS
Pkts: 0/0
FastEthernet4/10 Flags: F NS
Pkts: 0/9592618
```

To display the general MFIB configuration status and operational status, use the **show** command described in the following example.

```
Router# show ipv6 mfib status

IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 358
    Tables 1/1/0 (active/mrib/io)
```

To display summary information about the number of IPv6 MFIB entries and interfaces, use the **show** command described in the following example.

```
Router# show ipv6 mfib summary

Default
 60 prefixes (60/0/0 fwd/non-fwd/deleted)
 21 ioitems (21/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [3 (S,G), 11 (*,G), 46 (*,G/m)]
 Table id 0x0, instance 0x1031AFB0
 Database: epoch 0

2024#show ipv6 mfib in
2024#show ipv6 mfib int
2024#show ipv6 mfib interface
IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
```

```
    Process Status: may enable - 3 - pid 358
    Tables 1/1/0 (active/mrib/io)

MFIB interface            status    CEF-based output
                                 [configured,available]
Vlan102                   up     [yes       ,yes      ]
Vlan104                   up     [yes       ,yes      ]
Tunnel0                   up     [yes       ,no       ]
Tunnel1                   up     [yes       ,yes      ]
```

To display the IPv6 multicast-enabled interfaces and their forwarding status, use the **show** command described in the following example.

```
Router# show ipv6 mfib interface

IPv6 Multicast Forwarding (MFIB) status:
Configuration Status: enabled
Operational Status: running
MFIB interface status CEF-based output
[configured,available]
Loopback0 up [yes ,? ]
Vlan46 up [yes ,? ]
Vlan47 up [yes ,? ]
Tunnel0 down [yes ,no ]
Tunnel1 down [yes ,no ]
```

To display how IPv6 multicast routing does Reverse Path Forwarding, use the **show** command described in the following example.

```
Router# show ipv6 rpf FE80::4255:39FF:FE89:7404

RPF information for 3::3
  RPF interface: Vlan10
  RPF neighbor: FE80::4255:39FF:FE89:7404
  RPF route/mask: 3::3/128
  RPF type: Unicast
  RPF recursion count: 0
  Metric preference: 110
  Metric: 2
```

Verifying MLD Snooping

Use the **show** commands listed below to verify the MLD snooping configuration.

To verify whether IPv6 MLD snooping report suppression is enabled or disabled, use the **show** command used in the following example:

```
Router# show ipv6 mld snooping

Global MLD Snooping configuration:
-------------------------------------------
MLD snooping Oper State      : Enabled
MLDv2 snooping               : Enabled
Listener message suppression : Disabled
EHT DB limit/count           : 1000/2
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 3
```

```
Last listener query count    : 3
Last listener query interval : 1000
Check Hop-count=1            : Yes

Vlan 102:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Disabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/0
Check Hop-count=1                   : Yes

Vlan 104:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Enabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/2
Check Hop-count=1                   : Yes

Vlan 1001:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Disabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/0
Check Hop-count=1                   : Yes
```

To display all or a specified IP Version 6 (IPv6) multicast address information maintained by MLD snooping, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping address

Flags: M -- MLD snooping, S -- Static

Vlan Group/source Type Version Port List
-----------------------------------------------------------------------
104 FF34::1 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF34::2 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF34::3 M v2 Gi0/6 Gi0/10 Po1
/2006::1 M Gi0/6 Gi0/10 Po1
104 FF02::FB M v2 Gi0/0
```

To display the number of multicast groups on a router or in a specified VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping address count

Total number of groups: 4
Total number of (S,G): 3
```

To display the MLD snooping membership summary on a router or in a specified VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping membership

Snooping Membership Summary for Vlan 104
------------------------------------------
Total number of channels: 1
Total number of hosts   : 2

Source/Group                  Interface Reporter                      Uptime   Last-Join/

                                                                               Last-Leave
-----------------------------------------------------------------------------------------

2006::1/FF34::4                Gi0/1     FE80::4255:39FF:FE89:6284      00:47:22 00:00:11
 /
                                                                                     -


2006::1/FF34::4                Gi0/10    FE80::200:4EFF:FE72:F91F       00:47:26 00:00:09
 /
                                                                                     -
```

To display the MLD snooping that is dynamically learned and manually configured on the multicast router ports for a router or for a specific multicast VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping mrouter

Vlan    ports
----    -----
 102    Po1(dynamic)
 104    Gi0/1(dynamic), Gi0/4(static)
```

To display the configuration and operation information for the MLD snooping configured on a router, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping querier

Vlan      IP Address               MLD Version   Port
-------------------------------------------------------------
102       FE80::4255:39FF:FE89:5284
                                   v2            Po1
104       FE80::4255:39FF:FE89:6284
                                   v2            Gi0/1
```

To verify a static member port and an IPv6 address, use the **show** command described in the following example:

```
Router# show mac-address-table multicast mld-snooping

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
```

To verify if IPv6 MLD snooping is enabled on a VLAN interface, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping mrouter vlan 104

Vlan    ports
----    -----
 104    Gi0/1(dynamic), Gi0/4(static)
```

To verify if Immediate Leave is enabled on a VLAN interface, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping vlan 104

Global MLD Snooping configuration:
-------------------------------------------
MLD snooping Oper State      : Enabled
MLDv2 snooping               : Enabled
Listener message suppression : Disabled
EHT DB limit/count           : 1000/2
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 3
Last listener query count    : 3
Last listener query interval : 1000
Check Hop-count=1            : Yes

Vlan 104:
--------
MLD snooping Admin State            : Enabled
MLD snooping Oper State             : Enabled
MLD immediate leave                 : Enabled
Explicit host tracking              : Enabled
Listener message suppression        : Enabled
Robustness variable                 : 3
Last listener query count           : 3
Last listener query interval        : 1000
EHT DB limit/count                  : 100000/2
Check Hop-count=1                   : Yes
Query Interval                      : 125
Max Response Time                   : 10000
```

To verify the MLD snooping querier information for a router or for a VLAN, use the **show** command described in the following example:

```
Router# show ipv6 mld snooping querier vlan 102

IP address               : FE80::4255:39FF:FE89:5284
MLD  version             : v2
Port                     : Gi0/3
Max response time        : 10s
Query interval           : 125s
Robustness variable      : 2
```

Verifying IPv6 Multicast Routing for VRF Lite

Use the **show** commands listed below to verify IPv6 multicast routing for VRF Lite configuration.

To view information about the interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command:

```
Router# show ipv6 pim vrf VPN_B interface

Interface          PIM   Nbr   Hello  DR
                         Count Intvl  Prior

Vlan122            on    1     30     1
    Address: FE80::7EAD:74FF:FEDC:E4AC
    DR     : this system
Vlan123            on    1     30     1
    Address: FE80::7EAD:74FF:FEDC:E4AC
    DR     : this system
Tunnel1            off    0     30     1
    Address: FE80::7EAD:74FF:FEDC:E4B0
    DR     : not elected
```

To view the information in a PIM topology table, use the **show ipv6 mroute** command:

```
Router# show ipv6 mroute vrf VPN_B

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, Y - Joined MDT-data group,
       y - Sending to MDT-data group
       g - BGP signal originated, G - BGP Signal received,
       N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
       q - BGP Src-Active originated, Q - BGP Src-Active received
       E - Extranet
Timers: Uptime/Expires
Interface state: Interface, State

(170:1::3, FF36::1), 21:11:23/00:03:23, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:23

(170:1::3, FF36::2), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::3), 21:11:23/00:02:33, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:02:33

(170:1::3, FF36::4), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::5), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
```

```
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::6), 21:11:23/00:02:33, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:02:33

(170:1::3, FF36::7), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::8), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::9), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

(170:1::3, FF36::A), 21:11:23/00:03:13, flags: sT
  Incoming interface: Vlan123
  RPF nbr: FE80::462B:3FF:FE48:DA54
  Immediate Outgoing interface list:
    Vlan122, Forward, 21:11:23/00:03:13

Pura-5#
```

To view the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the **show ipv6 mfib** command:

```
Router# show ipv6 mfib vrf VPN_B

Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
VRF VPN_B
 (*,FF00::/8) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF00::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,FF02::/16) Flags:
   SW Forwarding: 0/0/0/0, Other: 4/4/0
 (*,FF10::/15) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
```

```
(*,FF12::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF20::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF22::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF30::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF32::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF33::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF34::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF35::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF36::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(170:1::3,FF36::1) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::2) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::3) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::4) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::5) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::6) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::7) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::8) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
```

```
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::9) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(170:1::3,FF36::A) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwarding:   955000/12/60/5, Other: NA/NA/NA
  Vlan123 Flags: A
  Vlan122 Flags: F NS
    Pkts: 0/0
(*,FF37::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF38::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF39::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3A::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3B::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3C::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3D::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3E::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF3F::/32) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF40::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF42::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF50::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF52::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF60::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF62::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF70::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF72::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF80::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF82::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF90::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF92::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFA0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFA2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFB0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFB2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
```

```
(*,FFC0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFC2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFD0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFD2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFE0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFE2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFF0::/15) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
(*,FFF2::/16) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
```

Verifying PIM BFD Support

Use the **show** commands listed below to verify PIM BFD support.

To view a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors ipv6** command:

```
Router# show bfd neighbors ipv6

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::4255:39FF:FE89:5284 4/4 Up Up Vl24
FE80::FE99:47FF:FE37:FBC0 2/4 Up Up Vl101
```

To view all BFD protocol parameters, timers, and clients such as PIM, OSPF, and so on for each neighbor, use the **show bfd neighbors ipv6 details** command:

```
Router# show bfd neighbors ipv6 details

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::4255:39FF:FE89:5284 4/4 Up Up Vl24
Session state is UP and not using echo function.
Session Host: Software
OurAddr: FE80::4255:39FF:FE89:6284
Handle: 4
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 110(0), Hello (hits): 50(52910)
Rx Count: 52927, Rx Interval (ms) min/max/avg: 1/56/45 last: 40 ms ago
Tx Count: 52912, Tx Interval (ms) min/max/avg: 1/56/45 last: 12 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPFv3
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 5 last_rx_auth_seq 4
Uptime: 00:40:05
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
```

```
My Discr.: 4 - Your Discr.: 4
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0

IPv6 Sessions
NeighAddr LD/RD RH/RS State Int
FE80::FE99:47FF:FE37:FBC0 2/4 Up Up Vl101
Session state is UP and not using echo function.
Session Host: Software
OurAddr: FE80::4255:39FF:FE89:6284
Handle: 2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 142(0), Hello (hits): 50(53327)
Rx Count: 53317, Rx Interval (ms) min/max/avg: 1/56/45 last: 8 ms ago
Tx Count: 53330, Tx Interval (ms) min/max/avg: 1/56/46 last: 24 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPFv3
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 4 last_rx_auth_seq 5
Uptime: 00:40:24
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 4 - Your Discr.: 2
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0
```

Configuration Examples for IPv6 Multicast

Example: Enabling IPv6 Multicast Routing

The following is a sample configuration of IPv6 Multicast feature on the Cisco ASR 901 Router.

```
!
!
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
asr901-platf-multicast enable
!
!
```

Example: Configuring IPv6 SSM Mapping

The following is a sample configuration of IPv6 SSM mapping on the Cisco ASR 901 router.

```
!
!
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1
ipv6 mld ssm-map query dns
```

```
!
!
```

Example: Configuring IPv6 MLD Snooping

The following is a sample configuration of IPv6 MLD snooping on a Cisco ASR 901 Router.

```
!
Building configuration...
!
!
!
!
asr901-platf-multicast enable
ip multicast-routing
ipv6 unicast-routing
ipv6 cef
ipv6 mld snooping explicit-tracking limit 1000
ipv6 mld snooping check hop-count
ipv6 mld snooping robustness-variable 3
ipv6 mld snooping last-listener-query-count 6
ipv6 mld snooping last-listener-query-interval 10000
ipv6 mld snooping vlan 104 mrouter interface Gi0/4
ipv6 mld snooping vlan 104 immediate-leave
ipv6 mld snooping vlan 104 static FF45::5 interface Gi0/4
ipv6 mld snooping
ipv6 multicast-routing
!
!
```

Example: Configuring Rendezvous Point

For a sample configuration of RP, see the *Configuring a Rendezvous Point* document at: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Example: Configuring IPv6 Multicast Routing for VRF Lite

The following is a sample configuration of IPv6 multicast routing for VRF Lite:

```
Building configuration...

!
!
!
vrf definition vpe_2
 rd 1.1.1.1:100
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
!
!
```

```
ipv6 multicast-routing
ipv6 multicast-routing vrf VPN_B
ipv6 multicast-routing vrf VPN_C
ipv6 multicast-routing vrf vpe_2
!
!
!
multilink bundle-name authenticated
l3-over-l2 flush buffers
asr901-platf-multicast enable
asr901-storm-control-bpdu 1000
!
!
!
interface Vlan80
 vrf forwarding vpe_2
 ip address 192.108.1.27 255.255.255.0
 ip pim sparse-mode
 ipv6 address my-prefix ::7272:0:0:0:72/64
!
!
!
end
```

Example: Configuring BFD PIM on an IPv6 Interface

The following is a sample configuration of BFD PIM on an IPv6 interface:

```
!
Building configuration...

Current configuration : 6679 bytes
!
! Last configuration change at 17:03:42 IST Wed May 21 2014
!

hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone IST 5 30
ip cef
!
!
!
!
no ip domain lookup

ip multicast-routing
ipv6 unicast-routing
ipv6 cef
ipv6 mld snooping
ipv6 multicast-routing
!
!

asr901-platf-multicast enable
```

```
!
interface Loopback1
ip address 3.3.3.3 255.255.255.255

interface GigabitEthernet0/0

service instance 24 ethernet
encapsulation dot1q 24
rewrite ingress tag pop 1 symmetric
bridge-domain 24

!
interface Vlan24
ipv6 address 2024::2/64
ipv6 pim bfd
ipv6 ospf 1 area 0
bfd interval 50 min_rx 50 multiplier 3


ipv6 router ospf 1
router-id 3.3.3.3
bfd all-interfaces
timers throttle spf 50 50 5000
timers throttle lsa 10 20 5000
timers lsa arrival 10
timers pacing flood 5
!
!

!
!
end
```

Troubleshooting Tips

Use the following **debug** commands to enable the debug feature to help troubleshoot the IPv6 Multicast feature on the Cisco ASR 901 Router.

Note We recommend that you do not use these **debug** commands without TAC supervision.

Command Name	Description
[no] debug ipv6 mld	Enables debugging MLD protocol activity.
[no] debug ipv6 mld snooping	Enables debugging IPv6 MLD snooping activity.
[no] debug ipv6 pim	Enables debugging PIM protocol activity.
[no] debug ipv6 pim neighbor	Enables debugging for PIM Hello message processing.
[no] debug ipv6 mrib route	Enables debugging MRIB routing entry related activity.
[no] debug ipv6 mrib client	Enables debugging MRIB client management activity.

Command Name	Description
[no] debug ipv6 mrib io	Enables debugging MRIB I/O events.
[no] debug ipv6 mrib table	Enables debugging MRIB table management activity.
[no] debug platform hardware cef ip multicast	
[no] debug ip pim vrf	Enables debugging for PIM-related events.
[no] debug ipv6 pim neighbor	Enables debugging on PIM protocol activity.
[no] debug ipv6 pim bfd	Enables debugging on PIM protocol activity for BFD.
[no] debug bfd event	Enables debugging messages about BFD. on PIM protocol activity.

CHAPTER 44

Configuring Switched Port Analyzer

This feature module describes how to configure a switched port analyzer (SPAN) on the Cisco ASR 901 Router.

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 table at the end of this module.

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.

SPAN Limitations and Configuration Guidelines

The following limitations and configuration guidelines apply when configuring SPAN on the Cisco ASR 901 Router:

- Only one SPAN session is supported.
- Only one local SPAN destination interface is supported.
- You cannot configure a local SPAN destination interface to receive ingress traffic.
- Use a network analyzer to monitor interfaces.
- Outgoing CDP and BPDU packets are not replicated.
- Ethernet loopback and Traffic generator are not supported when SPAN is enabled. For egress SPAN, the traffic is mirrored before egress xlate translation.
- Egress SPAN is only supported for port and not supported for VLAN, EFP, or Port-Channel interfaces.
- When you specify source interfaces and do not specify a traffic type [Transmit (Tx), Receive (Rx), or Both], both type is used by default.

- Use the no monitor session session_number command with no other parameters to clear the SPAN session number.

Understanding SPAN

The following sections describe SPAN:

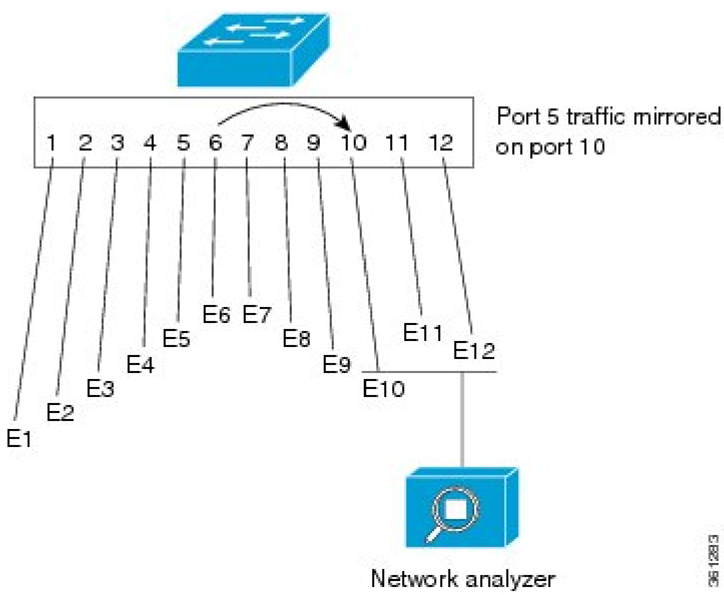
Overview

Effective with Cisco IOS Release 15.4(1)S, the Cisco ASR 901 supports Local SPAN. Local SPAN supports a SPAN session entirely within one switch. You can analyze network traffic passing through ports or VLANs by using SPAN to send a copy of the traffic to another port on the switch that has been connected to a network analyzer or other monitoring or security devices. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports, VLANs, or EFPs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs or EFPs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored. You can use the SPAN destination port to inject traffic from a network security device.

In example, all traffic on Ethernet port 5 (the source port) is mirrored on Ethernet port 10. A network analyzer on Ethernet port 10 receives all the network traffic from Ethernet port 5 without being physically attached to Ethernet port 5.

Figure 42: Example of Local SPAN Configuration



SPAN does not affect the switching of network traffic that is received on source ports; a copy of the packets that are received by the source ports is still sent to the destination port.

SPAN Session

A local SPAN session is an association of a destination interface with a set of source interfaces. You configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic on one or more interfaces and to send either ingress traffic, egress traffic, or both to one destination interface. You can configure a SPAN session with separate sets of SPAN source interfaces or VLANs; overlapping sets are not supported.

SPAN sessions do not interfere with the normal operation of the switch. The show monitor session all command displays the operational status of a SPAN session.

A SPAN session remains inactive after system power-up until the destination interface is operational.

Source Interface

A source interface (also called a monitored interface) is an interface monitored for network traffic analysis.

A source interface has these characteristics:

- A single VLAN, EFP, or port-channel source per session is supported for ingress.
- A single physical source port is supported for ingress and egress.
- A maximum of five physical ports can be used in a single session for ingress SPAN (Rx).
- When an interface is configured as a destination interface, it cannot be configured as a source interface.

Destination Interface

A destination interface (also called a monitoring interface) is a switched interface to which SPAN sends packets for analysis. You can have only one SPAN destination interface.

A destination interface has these restrictions:

- It needs to be a single physical port.
- It cannot be used as an ingress interface.
- When an interface is configured as a destination interface, it cannot be configured as a source interface.

Traffic Types

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces. Specifying the configuration option both copies network traffic received and transmitted by the source interfaces to the destination interface.

SPAN Traffic

Network traffic, including multicast, can be monitored using local SPAN. Multicast packet monitoring is enabled by default. In some local SPAN configurations, multiple copies of the same source packet are sent to the local SPAN destination interface. For example, a bidirectional (both ingress and egress) local SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

Configuring SPAN

The following sections describe how to configure SPAN:

Creating a SPAN Session

To create a SPAN session:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**monitor session** {session_number} type local **Example:** `Router(config)# monitor session 1 type local`	Specifies the SPAN session number.
Step 4	source {interface interface_type slot/port} | {vlan vlan_ID} | {service instance id interface_type slot/port} [, | - | rx | tx | both] **Example:** `Router(config-mon-local)# source interface gigabitethernet 0/8`	Specifies the source interfaces, VLANs, or service instances, and the traffic direction to be monitored.
Step 5	{destination {interface interface_type slot/port} **Example:** `Router(config-mon-local)# destination interface gigabitethernet 0/11`	Specifies the destination interface.
Step 6	no shutdown **Example:** `Router(config-mon-local)# no shutdown`	Enables the SPAN session using the no shutdown command.

What to do next

Removing Sources or Destination from a SPAN Session

To remove sources or destination from a SPAN session, use the following commands beginning in executive mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**no monitor session***type number* **Example:** `Router(config)# no monitor session 1`	Clears existing SPAN configuration for a session.

Configuration Examples for SPAN

This section shows a sample configuration for local SPAN session on Cisco ASR 901 router:

```
monitor session 1 type  local
source interface gigabitEthernet 0/8 tx
destination interface gigabitEthernet 0/11
no shut
exit
```

Verifying Local SPAN

The following is sample output from the show monitor session all command.

```
Session 1
---------
Type                    : Local Session
Status                  : Admin Enabled
Source Ports            :
    TX Only             : Gi0/8
Destination Ports       : Gi0/11
    Encapsulation : Native
          Ingress: Disabled
```

The following is sample output from the show monitor session all detail command.

```
Session 1
```

```
---------
Type                     : Local Session
Status                   : Admin Enabled
Description              : -
Source Ports             :
    RX Only              : None
    TX Only              : Gi0/8
    Both                 : None
Source VLANs             :
    RX Only              : None
    TX Only              : None
    Both                 : None
Source EFPs              :
    RX Only              : None
    TX Only              : None
    Both                 : None
Source RSPAN VLAN        : None
Destination Ports        : Gi0/11
    Encapsulation : Native
          Ingress: Disabled
Filter VLANs             : None
Dest RSPAN VLAN               : None
Source IP Address        : None
Source IP VRF            : None
Source ERSPAN ID         : None
Destination IP Address : None
Destination IP VRF       : None
MTU                      : None
Destination ERSPAN ID   : None
Origin IP Address        : None
IP QOS PREC              : 0
IP TTL                   : 255
```

Additional References

The following sections provide references to Switched Port Analyzer feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Switched Port Analyzer

Table 49: Feature Information for Switched Port Analyzer, on page 849 lists the features in this module and provides links to specific configuration information.

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 Table 49: Feature Information for Switched Port Analyzer, on page 849 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 49: Feature Information for Switched Port Analyzer

Feature Name	Releases	Feature Information
Switched Port Analyzer	15.4(1)S	This feature was introduced on the Cisco ASR 901 router. The following sections provide information about this feature:

CHAPTER 45

IP Security

This feature module describes how to configure the Internet Key Exchange (IKE) protocol for basic IP Security (IPsec) Virtual Private Networks (VPNs). IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets.

Prerequisites for IP Security

- Although the Cisco ASR 901 Router supports the IPsec feature, it is supported only on the A901-6CZ-FS-D and A901-6CZ-FS-A PIDs.
- For the IPsec and NAT/PAT to work on the ASR 901S router a physical loopback connection is required from the management port to any available Gigabit port before issuing the following command in configuration mode:

  platform mgmt loopback interface GigabitEthernet0/4.

  In this case, the physical connection is between the management port and Gigabit port 0/4.

Restrictions for IP Security

- This feature is available only on the new software image named asr901sec-universalk9.mz. (This feature is not available on the standalone software image named asr901-universalk9.mz. If you use asr901sec-universalk9.mz in an unsupported Cisco ASR 901 PID, the router issues a warning message and loads the software with only basic features.)
- Policy-based VPNs are not supported.
- Only the tunnel mode is supported, and only one tunnel is supported.

The following features are not supported:

- Authentication Header (AH) Hash Message Authentication Code (HMAC) with SHA512.
- QoS on tunnel interface.
- Combination of ESP as encryption and AH as hashing algorithm.
- Extensible Authentication Protocol (EAP) with Message Digest 5 (MD5).
- Low performance of non-UDP or TCP packets for IPsec.
- PAT support for port channel.
- Routing protocols, other than OSPF.
- IPsec MIB.
- Encapsulation of Security Payloads (ESP) with Null option.

Information About IP Security

The following features are supported on the Cisco ASR 901 Routers (A901-6CZ-FS-D and A901-6CZ-FS-A) from Cisco IOS Release 15.4(2)S onwards.

IKE Security Protocol

The IKE protocol is a key management protocol standard that is used in conjunction with the IPsec standard. IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

For more information on IKE for IPsec, see the *Configuring Internet Key Exchange for IPsec VPNs* document at:http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec.html

Advanced Encryption Standard

Advanced Encryption Standard (AES) is a cryptographic algorithm that protects sensitive, unclassified information. AES offers a large key size and supports variable key lengths—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For more information on AES, see the document at: http://www.cisco.com/c/en/us/td/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/xe_3s/sec_secure_connectivity_xe_3s_book/sec_key_exch_ipsec_xe.html

Triple DES Encryption

Triple DES (3DES) encryption is a strong form of encryption (168-bit) that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network-layer encryption.

For more information on 3DES Encryption, see the *Configuring Internet Key Exchange for IPSec VPNs* document at: http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec_xe.html

Encrypted Preshared Key

The Encrypted Preshared Key feature enables secure storage of plain text passwords in Type 6 (encrypted) format in NVRAM.

For more information on Encrypted Preshared Key, see the *Encrypted Preshared Key* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-3s/sec-encrypt-preshare.html

IKE Modes

IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPsec.

Phase 1 negotiation can occur using main mode or aggressive mode. The main mode protects all information during the negotiation; this means that no information is available to a potential attacker. When main mode is used, the identities of the two IKE peers are hidden. Although this mode of operation is very secure, it is relatively costly in terms of the time it takes to complete the negotiation. Aggressive mode takes less time to negotiate keys between peers; however, it gives up some of the security provided by main mode negotiation. For example, the identities of the two parties trying to establish a security association are exposed to an eavesdropper.

The two modes serve different purposes and have different strengths. The main mode is slower than the aggressive mode, but the main mode is more secure and more flexible because it can offer an IKE peer more security proposals than the aggressive mode.

For more information on IKE modes, see the *Configuring Internet Key Exchange for IPSec VPNs* document at:
http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec_xe.html

Supported Components

The following components are supported as part of the IPsec feature:

- IPsec in tunnel mode
- Route-based IP security tunnels
- IKEv2 support - in addition to IKEv1
- Periodic dead peer detection (DPD)
- IKE main mode (including 3 two-way exchanges)
- Pre-Shared Key Exchange mechanism—DH group 1, 2, 5, 14, 15, 16, 19, 20, 21, 24
- Encapsulation Security Payload (ESP) support
- Encryption algorithms—AES (128,192,256), DES, and 3DES
- Authentication algorithms—MD5, SHA-1, and SHA-2
- IP security tunneling for CPU generated traffic for in-band traffic
- IP security tunneling for Layer 3 forwarded traffic

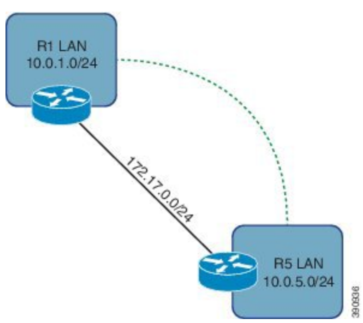
- Static routes
- Coexistence with Layer 2 traffic
- Coexistence with IP multicast
- ToS bytes preservation after encryption and decryption.
- NAT Traversal

For more information on IPsec see the documents listed in the “Additional References” section.

Configuring IP Security

The following topology is used for the configurations listed in this document.

Figure 43: Route-based VPN



Creating a Preshared Key

A preshared key is a secret key previously shared between two routers, using a secure channel, before the key can be used. The key does not require the use of a certificate authority (CA), and is easier to set up in a small network with fewer than ten nodes.

Based on the topology listed above (Route-based IPsec), create a *keyring* and *key* for R1. Use the same *keyring* and *key* on R5. To create a preshared key, complete the following steps:

Procedure

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

	Command or Action	Purpose
Step 3	**crypto keyring** *keyring-name* **Example:** `Router(config)# crypto keyring VPN`	Defines a crypto keyring to be used during IKE authentication. • *keyring-name*—Name of the crypto keyring.
Step 4	**pre-shared-key address** *address* **key** *key* **Example:** `Router(config-keyring)# pre-shared-key address 172.17.0.5 key AnotherSecretKey`	Defines a preshared key to be used for IKE authentication. • *address*—IP address of the remote peer. • *key*—Name of the secret key.

Creating an ISAKMP Policy

An Internet Security Association and Key Management Protocol (ISAKMP) policy provides configuration of the security and encryption parameters used for the security parameters of the ISAKMP communication channel, such as hashing, encryption, and key length.

To create an ISAKMP policy, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 10`	Defines an IKE policy and enters config-isakmp configuration mode. • *priority*—IKE policy priority.
Step 4	**encryption aes 256** **Example:** `Router(config-isakmp)# encryption aes 256`	Specifies the encryption algorithm within an IKE policy.
Step 5	**authentication pre-share** **Example:** `Router(config-isakmp)# authentication pre-share`	Specifies the authentication method within an IKE policy.

	Command or Action	Purpose
Step 6	**group 5** **Example:** `Router(config-isakmp)# group 5`	Specifies one or more Diffie-Hellman (DH) group identifiers for use in an IKE policy.
Step 7	**hash md5** **Example:** `Router(config-isakmp)# hash md5`	Specifies the hashing algorithm within IKE policy.

Creating an ISAKMP Profile

The ISAKMP profile is an enhancement to ISAKMP configuration. It enables modularity of ISAKMP configuration. The ISAKMP profile is required on both routers (R1 and R5. See the figure in Configuring IPsec section.) to match the peer IP address to the preshared key keyring.

To create an ISAKMP profile, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp profile** *profile-name* **Example:** `Router(config)# crypto isakmp profile R1_to_R5`	Defines an ISAKMP profile. • *profile-name*—Name of the user profile.
Step 4	**keyring** *keyring-name* **Example:** `Router(config-isa-prof)# keyring VPN`	Configures a keyring with an ISAKMP profile. • *keyring-name*—Name of the keyring, which must match the keyring name that was defined in the global configuration.
Step 5	**match identity address** *ip-address* **Example:** `Router(config-isa-prof)# match identity address 172.17.0.5 255.255.255.255`	Matches an identity from a peer in an ISAKMP profile . • *ip-address*—The IP address to match.
Step 6	**exit** **Example:**	Enters ISAKMP profile configuration mode. **Note**

	Command or Action	Purpose
	`Router(config-isa-prof)# exit`	Repeat step 3 to 6 to configure the ISAKMP profile on the second router. Remember to use a different *profile-name* and *ip-address*.

Defining an IPsec Transform Set

An IPsec transform set is an acceptable combination of security protocols and algorithms. You should define an IPsec transform set on both the routers (R1 and R5. See the figure in Configuring IPsec section.).

To define an IPsec transform set, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec transform-set** *transform-set-name transform1 transform2* **Example:** `Router(config)# crypto ipsec transform-set ESP-AES256-SHA1 esp-aes 256 esp-sha-hmac`	Defines a transform set, an acceptable combination of security protocols and algorithms. • *transform-set-name*—Name of the transform set to create (or modify. • *transform1/transform2*—Type of transform set. You can specify up to four transforms, one AH, one ESP encryption, one ESP authentication, and one compression. These transforms define the IPsec security protocols and algorithms.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Creating an IPsec Profile

An IPsec profile serves as a wrapper around one or more transform sets and other parameters used in the construction of an IPsec SA. You should create IPsec profiles on both the routers (R1 and R5. See the figure in Configuring IPsec section.).

To create an IPsec profile, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec profile** *profile-name* **Example:** `Router(config)# crypto ipsec profile Routed_VPN`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers (See the figure in Configuring IPsec section) and enters IPsec profile configuration mode. • *profile-name*—Name of the crypto ipsec profile.
Step 4	**set transform-set** *transform-set-name* **Example:** `Router(ipsec-profile)# set transform-set ESP-AES256-SHA1`	Attaches the desired transform set to IPsec profile.
Step 5	**set isakmp-profile** *profile-name* **Example:** `Router(ipsec-profile)# set isakmp-profile R1_to_R5`	Attaches the desired ISAKMP profile to IPsec profile.
Step 6	**exit** **Example:** `Router(ipsec-profile)# exit`	Exits ipsec profile configuration mode and enters global configuration mode.

Creating a VPN Tunnel Interface

A routed tunnel interface on both the routers ((R1 and R5. See the figure in Configuring IPsec section.) acts as logical VPN edge. The tunnel interfaces serve to encapsulate or encrypt egress traffic and decapsulate or decrypt ingress traffic. You should create tunnels on both the routers.

To create a VPN tunnel interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Tunnel0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *primary-ip-address seconary-ip-address* **Example:** `Router(config-if)# ip address 192.168.0.1 255.255.255.252`	Matches an identity from a peer in an ISAKMP profile. • *ip-address*—The ip-address to match.
Step 5	**tunnel source** *ip-address* **Example:** `Router(config-if)# tunnel source 172.17.0.1`	Sets the source address for a tunnel interface. • *ip-address*—Source IP address of the packets in the tunnel.
Step 6	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 172.17.0.5`	Specifies the destination for a tunnel interface. • *ip-address*—IP address of the host destination.
Step 7	**tunnel mode ipsec ipv4** **Example:** `Router(config-if)# tunnel mode ipsec ipv4`	Sets the encapsulation mode for a tunnel interface.
Step 8	**tunnel protection ipsec profile** *name* **Example:** `Router(config-if)# tunnel protection ipsec profile Routed_VPN`	Associates a tunnel interface with an IPsec profile. • *name*—Name of the IPsec profile.

Configuring Static Routing

Route-based VPNs cannot automatically discover remote networks that are reachable over the VPN. To communicate this information, you should configure a static route.

To create a static route, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip route** *ip-address mask* **interface** *number* **Example:** `Router(config)# ip route 10.0.5.0 255.255.255.0 tunnel0`	Configures a static route on the first router (R1 and R5. See the figure in Configuring IPsec section.). • *ip-address*—IP address of the host destination. • *mask*—Prefix mask for the destination. • *number*—Network interface type and interface number.
Step 4	**ip route** *ip-address mask* **interface** *number* **Example:** `Router(config)# ip route 10.0.1.0 255.255.255.0 tunnel0`	Configures a static route on the second router.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.

Verifying Static Routing

To display the contents of a routing table, use the **show ip route** commands, as shown in the following example:

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, GigabitEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, GigabitEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
S       10.0.3.0 [10/0] via 172.16.0.3
C       10.0.1.0 is directly connected, Loopback1
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
```

```
S        10.0.5.0 is directly connected, Tunnel0
```

To display current IKE SAs, use the **show crypto isakmp sa** command, as shown in the following example:

```
Router# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.17.0.5      172.17.0.1      QM_IDLE           4004 ACTIVE
```

Enabling Dynamic Routing

Route-based VPNs cannot automatically discover remote networks that are reachable over the VPN. To communicate this information, static routers (as mentioned in the section, Configuring Static Routing) or routing protocols can be configured. OSPF is the only protocol currently supported VPNs.

OSPF should be enabled for both the internal LAN interface (which a loopback pretending to be a /24 network) and the tunnel interface. An OSPF adjacency should form between R1 and R5 over the 192.168.0.0/30 network, inside the VPN.

To create a VPN tunnel interface, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Tunnel0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip ospf** *process-id* **area***area-id* **Example:** `Router(config-if)# ip ospf 1 area 0`	Enables Open Shortest Path First version 2 (OSPFv2) on an interface. • *process-id*—IP address of the host destination. • *area-id*—A decimal value in the range from 0 to 4294967295, or an IP address.
Step 5	**ip ospf mtu-ignore** **Example:** `Router(config-if)# ip ospf mtu-ignore`	Disables OSPF MTU mismatch detection on receiving database descriptor (DBD) packets.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface Loopback0`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**router ospf** *process-id* **area** *area-id* **Example:** `Router(config-if)# ip ospf 1 area 0`	Enables OSPFv2 on an interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.

Verifying Dynamic Routing

R1 and R5 should learn the LAN prefixes of each other through OSPF, and both networks should be immediately reachable through the VPN tunnel.

```
R1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, GigabitEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, GigabitEthernet0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S       10.0.3.0/24 [10/0] via 172.16.0.3
C       10.0.1.0/24 is directly connected, Loopback1
O       10.0.5.1/32 [110/1001] via 192.168.0.2, 00:01:29, Tunnel0
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Tunnel0

R1# ping 10.0.5.1 source 10.0.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.5.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Configuration Examples for IP Security

Example: Creating a Preshared Key

The following is a sample configuration for creating a preshared key and sharing it on two routers:

Router1

```
!
crypto keyring VPN
  pre-shared-key address 172.17.0.5 key AnotherSecretKey
!
```

Router5

```
!
crypto keyring VPN
  pre-shared-key address 172.17.0.1 key AnotherSecretKey
!
```

Example: Creating an ISAKMP Policy

The following is a sample configuration of an ISAKMP policy:

```
!
crypto isakmp policy 10
 hash md5
 encr aes 256
 authentication pre-share
 group 5
!
```

Example: Creating an ISAKMP Profile

The following is a sample configuration of an ISAKMP profile:

Router1

```
!
crypto isakmp profile R1_to_R5
   keyring VPN
   match identity address 172.17.0.5 255.255.255.255
!
```

Router5

```
!
crypto isakmp profile R5_to_R1
   keyring VPN
   match identity address 172.17.0.1 255.255.255.255
!
```

Example: Defining an IPsec Transform Set

The following is a sample configuration of an IPsec transform set:

```
!
crypto ipsec transform-set ESP-AES256-SHA1 esp-aes 256 esp-sha-hmac
!
```

Example: Creating an IPsec Profile

The following is a sample configuration of an IPsec profile:

```
!
crypto ipsec profile Routed_VPN
 set isakmp-profile R1_to_R5
 set transform-set ESP-AES256-SHA1
!
```

Example: Creating a VPN Tunnel Interface

The following is a sample configuration of a VPN tunnel interface:

Router1

```
!
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 tunnel source 172.17.0.1
 tunnel destination 172.17.0.5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Routed_VPN
!
```

Router5

```
!
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 tunnel source 172.17.0.5
 tunnel destination 172.17.0.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Routed_VPN
!
```

Example: Configuring Static Routing

The following is a sample configuration of static routing:

Router1

```
!
ip route 10.0.5.0 255.255.255.0 tunnel0
```

```
!
```

Router5

```
!
!
ip route 10.0.1.0 255.255.255.0 tunnel0
!
!
```

Example: Enabling Dynamic Routing

The following is a sample configuration of dynamic routing.

```
R1 and R5
router ospf 1
!
interface Loopback1
 ip ospf 1 area 0
!
interface Tunnel0
 ip ospf 1 area 0
 ip ospf mtu-ignore
```

NAT Traversal

The NAT Tranversal feature provides support for IP Security (IPsec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network. This feature provides this support by addressing many known incompatibilities between NAT and IPsec.

Before the introduction of this feature, a standard IPsec virtual private network (VPN) tunnel would not work if there were one or more NAT or PAT points in the delivery path of the IPsec packet. This feature makes NAT IPsec-aware; thereby, allowing remote access users to build IPsec tunnels to home gateways.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Restrictions for NAT Traversal

NAT Traversal feature has the following restrictions:

- NAT Traversal is only supported for IPv4.
- NAT Traversal supports IPSec end to end connectivity.
- NAT Traversal feature does not affect other feature functionality.

- ASR 901S routers do not support volume-based rekey. For interoperability deployments, vendor IPsec peer should also disable the volume-based rekey to prevent IPsec tunnel to flap.

Information About NAT Traversal

Feature Design of IPsec NAT Traversal

The IPsec NAT Transparency feature provides support for IPsec traffic to travel through NAT or PAT points in the network by encapsulating IPsec packets in a User Datagram Protocol (UDP) wrapper, which allows the packets to travel across NAT devices. The following sections define the details of NAT traversal:

- IKE Phase 1 Negotiation NAT Detection, on page 866
- IKE Phase 2 Negotiation NAT Traversal Decision, on page 866
- UDP Encapsulation of IPsec Packets for NAT Traversal, on page 867
- UDP Encapsulated Process for Software Engines Transport Mode and Tunnel Mode ESP Encapsulation, on page 868

IKE Phase 1 Negotiation NAT Detection

During Internet Key Exchange (IKE) phase 1 negotiation, two types of NAT detection occur before IKE Quick Mode begins--NAT support and NAT existence along the network path.

To detect NAT support, you should exchange the vendor identification (ID) string with the remote peer. During Main Mode (MM) 1 and MM 2 of IKE phase 1, the remote peer sends a vendor ID string payload to its peer to indicate that this version supports NAT traversal. Thereafter, NAT existence along the network path can be determined.

Detecting whether NAT exists along the network path allows you to find any NAT device between two peers and the exact location of NAT. A NAT device can translate the private IP address and port to public value (or from public to private). This translation changes the IP address and port if the packet goes through the device. To detect whether a NAT device exists along the network path, the peers should send a payload with hashes of the IP address and port of both the source and destination address from each end. If both ends calculate the hashes and the hashes match, each peer knows that a NAT device does not exist on the network path between them. If the hashes do not match (that is, someone translated the address or port), then each peer needs to perform NAT traversal to get the IPsec packet through the network.

The hashes are sent as a series of NAT discovery (NAT-D) payloads. Each payload contains one hash. If multiple hashes exist, multiple NAT-D payloads are sent. In most environments, there are only two NAT-D payloads--one for the source address and port and one for the destination address and port. The destination NAT-D payload is sent first, followed by the source NAT-D payload, which implies that the receiver should expect to process the local NAT-D payload first and the remote NAT-D payload second. The NAT-D payloads are included in the third and fourth messages in Main Mode and in the second and third messages in Aggressive Mode (AM).

IKE Phase 2 Negotiation NAT Traversal Decision

While IKE phase 1 detects NAT support and NAT existence along the network path, IKE phase 2 decides whether or not the peers at both ends will use NAT traversal. Quick Mode (QM) security association (SA) payload in QM1 and QM2 is used to for NAT traversal negotiation.

Because the NAT device changes the IP address and port number, incompatibilities between NAT and IPsec can be created. Thus, exchanging the original source address bypasses any incompatibilities.

UDP Encapsulation of IPsec Packets for NAT Traversal

In addition to allowing IPsec packets to traverse across NAT devices, UDP encapsulation also addresses many incompatibility issues between IPsec and NAT and PAT. The resolved issues are as follows:

Incompatibility Between IPsec ESP and PAT--Resolved

If PAT finds a legislative IP address and port, it drops the Encapsulating Security Payload (ESP) packet. To prevent this scenario, UDP encapsulation is used to hide the ESP packet behind the UDP header. Thus, PAT treats and processes the ESP packet as a UDP packet.

Incompatibility Between Checksums and NAT--Resolved

In the new UDP header, the checksum value is always assigned to zero. This value prevents an intermediate device from validating the checksum against the packet checksum; thereby, resolving the TCP UDP checksum issue because NAT changes the IP source and destination addresses.

Incompatibility Between Fixed IKE Destination Ports and PAT--Resolved

PAT changes the port address in the new UDP header for translation and leaves the original payload unchanged.

To see how UDP encapsulation helps to send IPSec packets, see the figures below.

Figure 44: Standard IPsec Tunnel Through a NAT/PAT Point (No UDP Encapsulation)

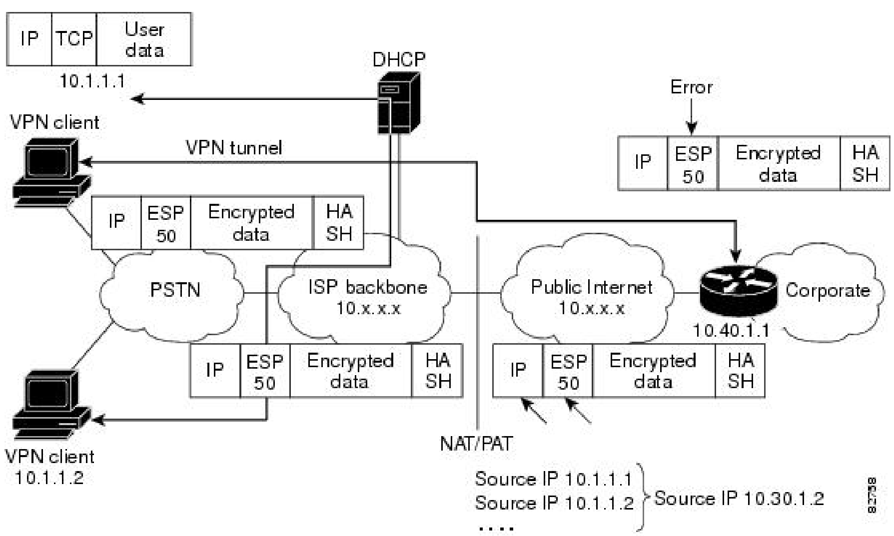
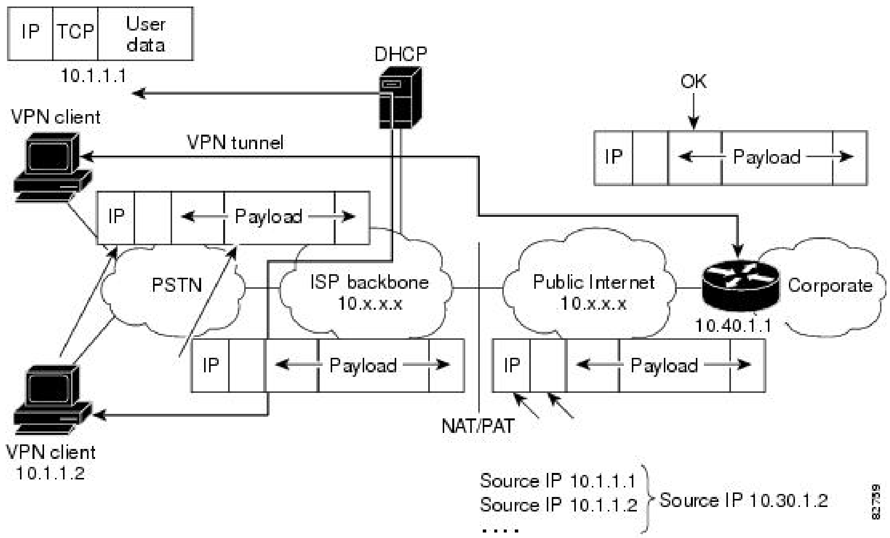


Figure 45: IPsec Packet with UDP Encapsulation



UDP Encapsulated Process for Software Engines Transport Mode and Tunnel Mode ESP Encapsulation

After the IPsec packet is encrypted by a hardware accelerator or a software crypto engine, a UDP header and a non-ESP marker (which is 4 bytes in length) are inserted between the original IP header and ESP header. The total length, protocol, and checksum fields are changed to match this modification.

NAT Keepalives

NAT keepalives are enabled to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of 1 byte. Although the current dead peer detection (DPD) implementation is similar to NAT keepalives, there is a slight difference: DPD is used to detect peer status, while NAT keepalives are sent if the IPsec entity did not send or receive the packet at a specified period of time in seconds--valid range is from 5 to 3600.

If NAT keepalives are enabled (through the **crypto isamkp nat keepalive** command), users should ensure that the idle value is shorter than the NAT mapping expiration time, which is 20 seconds.

How to Configure NAT and IPsec

Configuring NAT Traversal

NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T. If both VPN devices are NAT-T capable, NAT Traversal is auto detected and auto negotiated.

Disabling NAT Traversal

You may wish to disable NAT traversal if you already know that your network uses IPsec-awareness NAT (spi-matching scheme). To disable NAT traversal, use the following commands:

Procedure

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

Step 3	**no crypto ipsec nat-transparency udp-encapsulation**
	Example:
	`Router(config)#`
	`no crypto ipsec nat-transparency`
	`udp-encapsulation`
		Disables NAT traversal.

Configuring NAT Keepalives

To configure your router to send NAT keepalives, use the following commands:

Procedure

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

Step 3	**crypto isakmp nat keepalive** *seconds*
	Example:
	`Router(config)#`
	`crypto isakmp nat keepalive 20`
		Allows an IPsec node to send NAT keepalive packets.
		• *seconds* --The number of seconds between keepalive packets; range is from 5 to 3,600.
		Note
		When the timer is modified, it is modified for every Internet Security Association Key

	Command or Action	Purpose
		Management Protocol (ISAKMP) security association (SA) when the keepalive for that SA is sent based on the existing timer. **Note** A five-percent jitter mechanism value is applied to the timer to avoid security association rekey collisions. If there are many peer routers, and the timer is configured too low, then the router can experience high CPU usage.

Verifying IPsec Configuration

To verify your configuration, perform the following optional steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail** **Example:** `Router# show crypto ipsec sa`	Displays the settings used by current SAs.

Configuration Examples for IPsec and NAT

NAT Keepalives Configuration Example

The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
crypto isakmp key 1234 address 56.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-aes esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 56.0.0.1
 set transform-set t2
 match address 101
```

Additional References

The following sections provide references related to IP Security feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Commands
Internet Key Exchange for IPsec VPNs	Configuring Internet Key Exchange for IPsec VPNs
Security for VPNs with IPsec	Configuring Security for VPNs with IPsec

Standards

Table 50: Standard

Standard	Title
None	—

MIBs

MIB	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
None	—

Technical Assistance

Table 51: Technical Assistance

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

Feature Information for IP Security

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 52: Feature Information for IP Security

Feature Name	Releases	Feature Information
IP Security	15.4(2)S	This feature was introduced on the Cisco ASR 901 Series Routers. The following sections provide information about this feature: • Feature Overview • Configuring IPsec

CHAPTER 46

BCP Support on MLPPP

Short Description about BCP Support on MLPPP

BCP Support on MLPPP

This feature module describes how to configure Bridge Control Protocol (BCP) Support over Multilink PPP (MLPPP).

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 table at the end of this module.

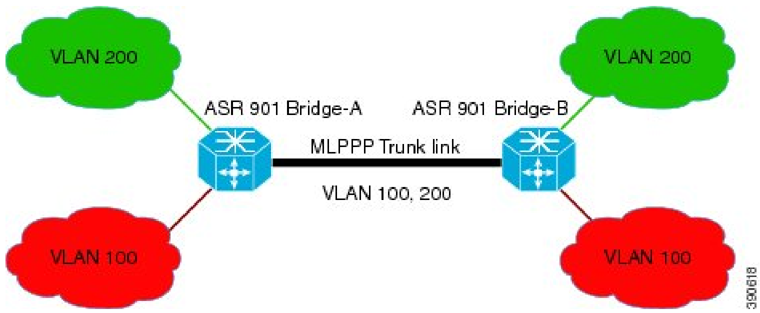
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

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.

Figure 46: BCP over MLPPP



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 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 53: Re-Marking Options

IP DSCP	VLAN CoS or PCP Bits
Set IP DSCP (re-mark IP DSCP)	Set IP DSCP
Set VLAN QoS or Priority Code Point (PCP) Bits	Set VLAN CoS Bits (re-mark VLAN CoS or PCP Bits)
Bandwidth Percent or Priority Percent	Bandwidth Percent or Priority Percent

Bridging and Routing

Both routing and bridging can co-exist on the same MLPPP interface. Routing is achieved on the MLPPP interface by running BCP after configuring an IP address on the SVI.

Note Configuring IP address on the SVI of the MLPPP interface does not bring up the IP Control Protocol (IPCP).

For information on configuring the IP address on the SVI of the MLPPP interface, see the "Enabling Routing on the MLPPP Interface Running BCP" section.

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:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 50`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 7	**bridge-domain** *bridge-id* **Example:**	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.

	Command or Action	Purpose
	`Router(config-if-srv)# bridge-domain 100`	

Adding an EFP to a Multilink

To add an EFP to a multilink, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 60`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.
Step 8	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode and enters the interface configuration mode. **Note** Repeat Step 4 to Step 7 to add another EFP to the Multilink.

Enabling Routing on an MLPPP Interface Running BCP

To enable routing on an MLPPP interface running BCP, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 60`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.
Step 8	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode and enters the interface configuration mode.
Step 9	**interface** *type number* **Example:** `Router(config)# interface VLAN 100`	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
Step 10	**ip adddress** *ip-address-primary ip-address-secondary* **Example:** `Router(config-if)# ip address 10.10.10.8 255.255.255.0`	Specifies a primary or secondary IP address for an interface.

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:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 60`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:**	Specifies that encapsulation modification occurs on packets at ingress.

	Command or Action	Purpose
	`Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.
Step 8	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode and enters the interface configuration mode. **Note** Repeat steps 3 to 7 to create another multilink and add the VLAN information.

Configuring QoS for BCP Support on MLPPP

The egress policy at 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).

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:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any dscpaf11`	Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode. • *class-map-name*—Name of the class for the class map. The class name is used for

	Command or Action	Purpose
		both the class map and to configure a policy for the class in the policy map.
Step 4	**match ip dscp** *dscp-list* **Example:** `Router(config-cmap)# match ip dscp af11`	Matches IP DSCP packeting using Assured Forwarding (AF) by entering the binary representation of the DSCP value.
Step 5	**class-map match-any** *class-map-name* **Example:** `Router(config-cmap)# class-map match-any qos-group3`	Creates a class map to be used for matching packets to a specified class.
Step 6	**match qos-group** *qos-group-value* **Example:** `Router(config-cmap)# match qos-group 3`	Identifies a specific quality of service (QoS) group value as a match criterion. • *qos-group-value*—The exact value used to identify a QoS group value. The valid range is from 0 to 7.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config-cmap)# policy-map bcpmlpppqos`	Creates a policy map that can be attached to one or more interfaces. • *poliicy-map-name*—Name of the policy map.
Step 8	**class** *class-name* **Example:** `Router(config-pmap)# class dscpaf11`	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. • *class-name*—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. .
Step 9	**priority percent** *percentage* **Example:** `Router(config-pmap-c)# priority percent 20`	Provides priority to a class of traffic belonging to a policy map. • *percentage*—Total available bandwidth to be set aside for the priority class. The valid range is from 1 to 100.
Step 10	**set ip dscp** *ip-dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp ef`	Marks a packet by setting the IP DSCP value in the type of service (ToS) byte. • *ip-dscp-value*—IP DSCP value; The valid values are from 0 to 63.
Step 11	**class** *class-name* **Example:**	Specifies the name of the class whose policy you want to create or change. Alternatively, is used to specify the default class (commonly

	Command or Action	Purpose
	`Router(config-pmap-c)# class qos-group3`	known as the class-default class) before you configure its policy.
Step 12	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Specifies the bandwidth allocated for a class belonging to a policy map. • *percentage*—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.
Step 13	**set qos-group** *group-id* **Example:** `Router(config-pmap-c)# set qos-group 4`	Sets a QoS group identifier (ID) that can be used later to classify packets. • *group-id*—group-id—Group ID number. The valid range is from 0 to 99.

Applying a QoS Policy on an MLPPP Interface

To apply a QoS policy on an MLPPP interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service-policy output** *policy-map-name* **Example:** `Router(config-if)# service-policy output bcpmlpppqos`	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. • *policy-map-name*—The name of a service policy map (created using the **policy-map** command) to be attached.

	Command or Action	Purpose
Step 5	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 20 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 50`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 8	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.

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

Multilink1
  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:
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0xB9026C received sequence
  Receive Class 1:
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x5D2E8F received sequence
  Transmit Class 0:
    0x5CBA5 sent sequence
  Transmit Class 1:
    0x146FA1 sent sequence
 Distributed MLP. Multilink in Hardware.
 Distributed Fragmentation is on. Fragment size: 256.
 Bundle status is: active
  Member links: 10 active, 0 inactive (max 255, min not set)
    Se0/6:0, since 01:36:49, 7680 weight, 256 frag size
```

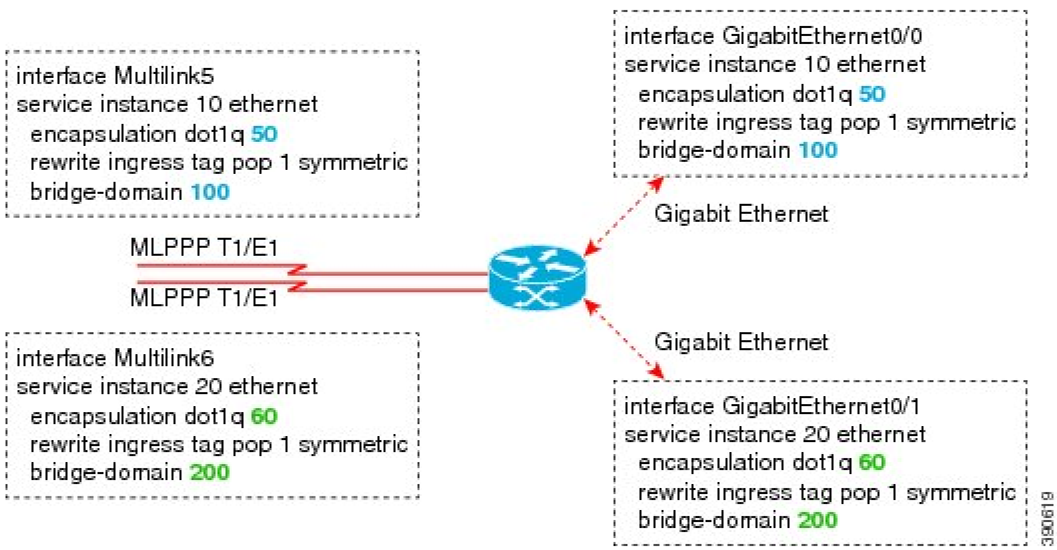
```
Se0/2:0, since 01:26:26, 7680 weight, 256 frag size
Se0/5:0, since 01:25:18, 7680 weight, 256 frag size
Se0/9:0, since 01:25:17, 7680 weight, 256 frag size
Se0/1:0, since 01:24:25, 7680 weight, 256 frag size
Se0/4:0, since 01:24:20, 7680 weight, 256 frag size
Se0/0:0, since 01:24:18, 7680 weight, 256 frag size
Se0/7:0, since 01:24:17, 7680 weight, 256 frag size
Se0/8:0, since 01:23:09, 7680 weight, 256 frag size
Se0/3:0, since 01:23:08, 7680 weight, 256 frag size
```

Configuration Examples for BCP Support on MLPPP

Example: Multilink with a Single EFP

The following is a sample configuration of a multilink with a single EFP.

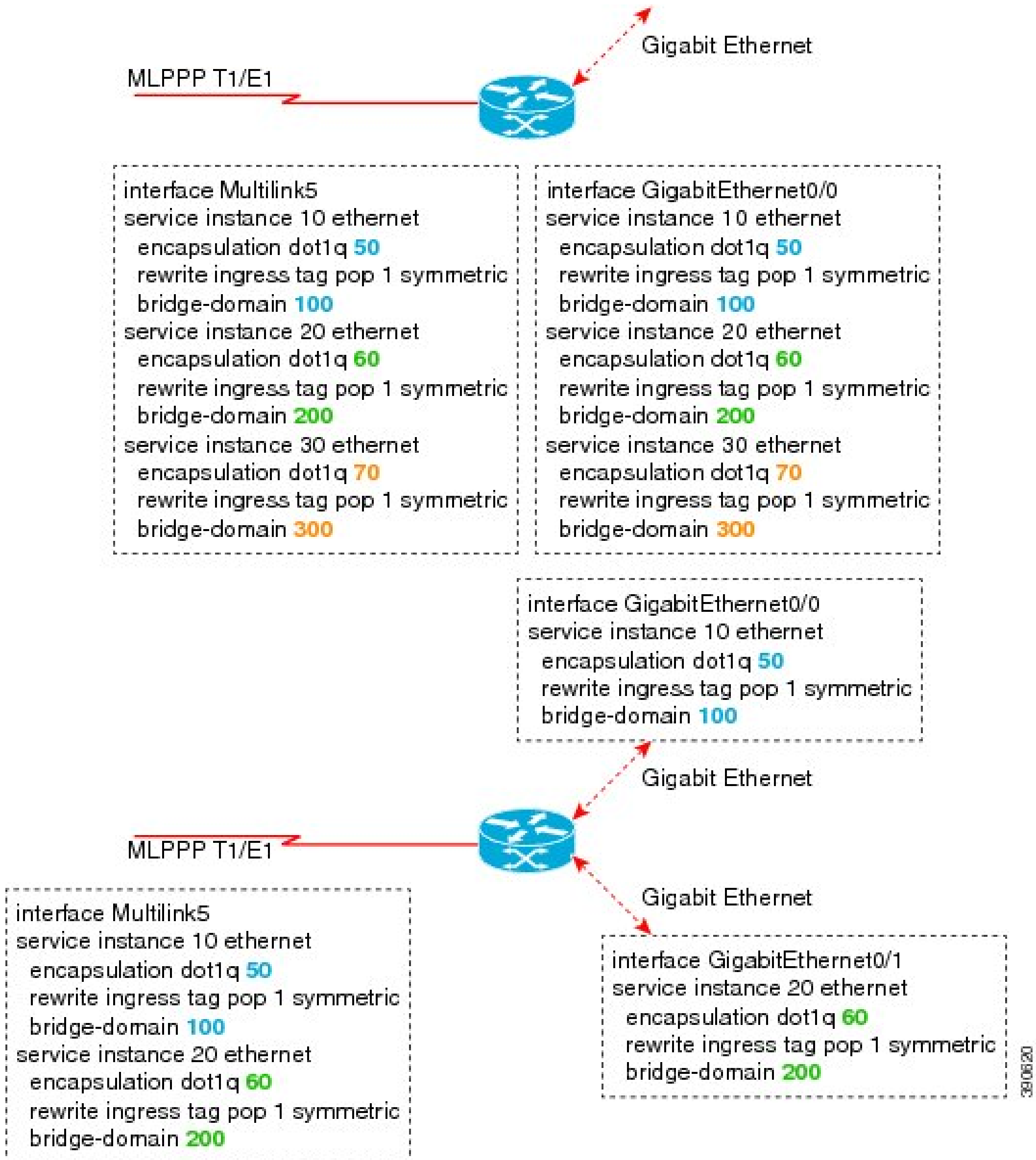
Figure 47: Multilink with a Single EFP



Example: Multilink with Multiple EFPs

The following is a sample configuration of a multilink with multiple EFPs.

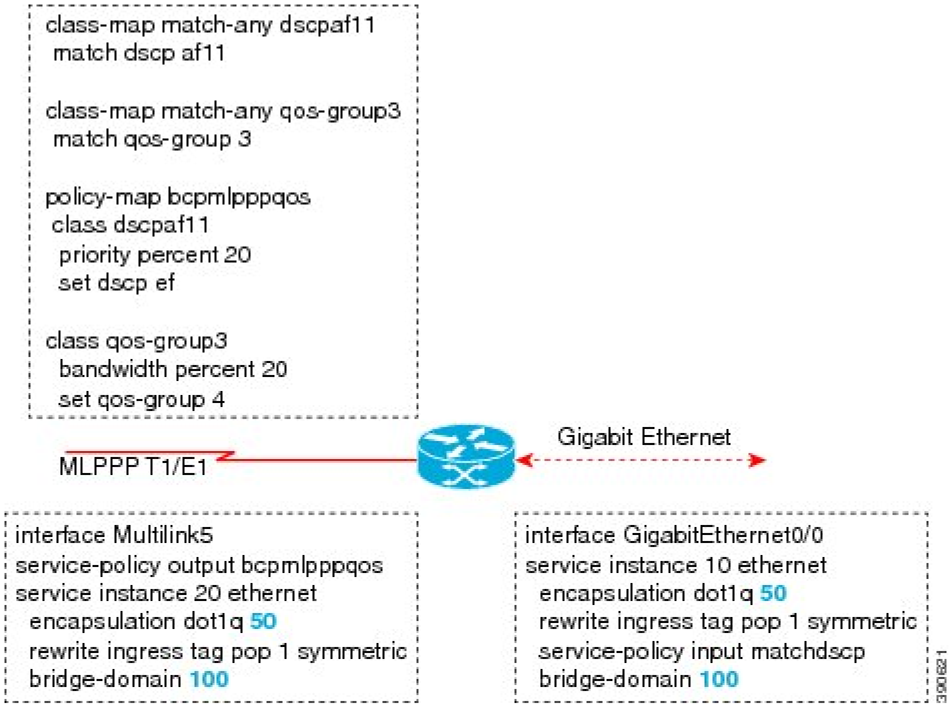
Figure 48: Multilink with Multiple EFPs



Example: Multilink with QoS

The following is a sample configuration of Multilink with QoS:

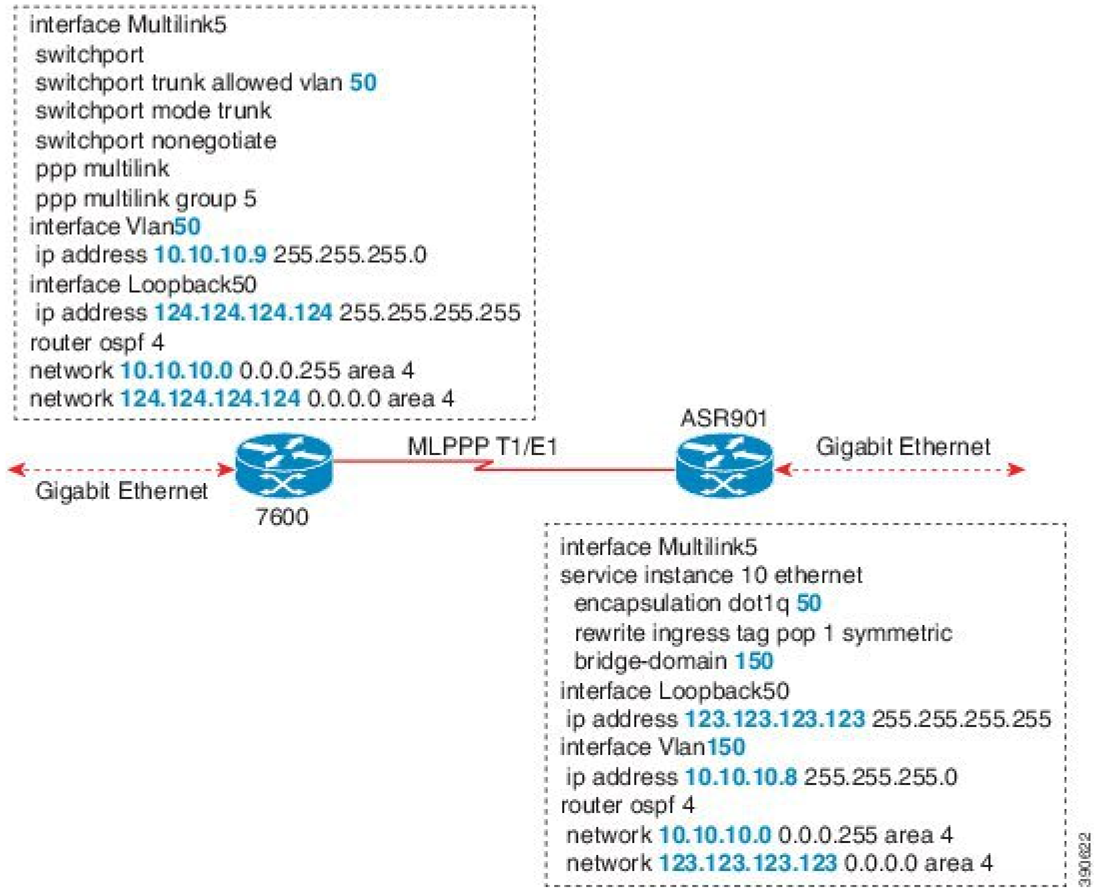
Figure 49: Multilink with QoS



Example: Multilink with Routing on an MLPPP Interface Running BCP

The following is a sample configuration to enable routing on an MLPPP interface running BCP:

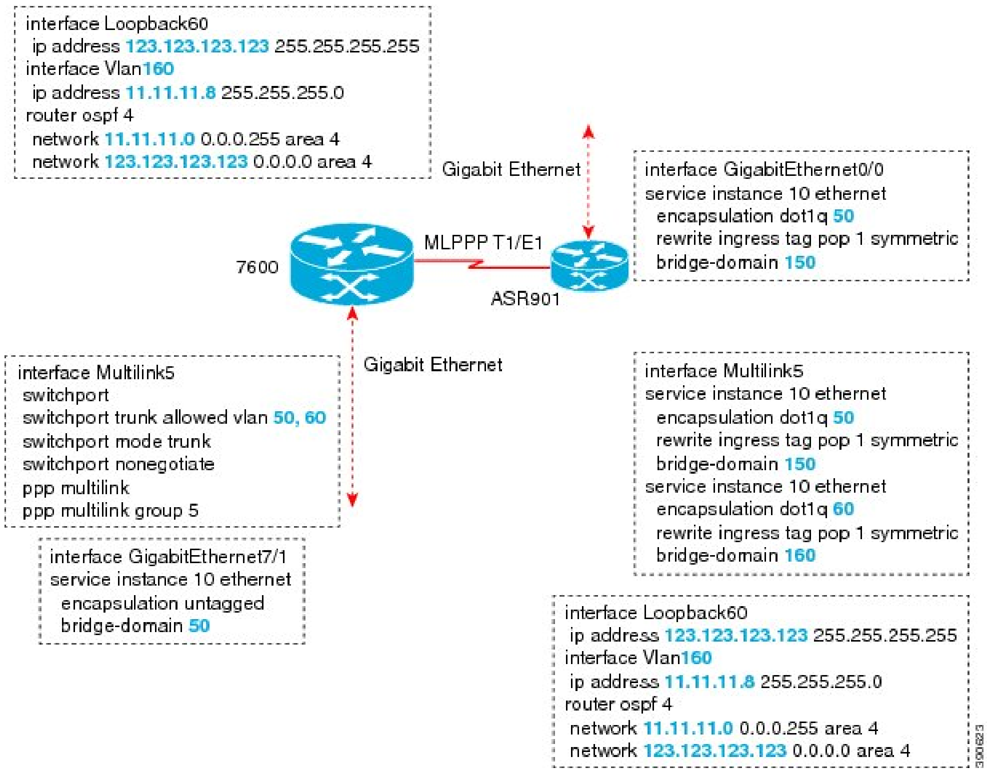
Figure 50: Multilink with Routing on an MLPPP Interface Running BCP



Example: Multilink Between Cisco ASR 901 Series Routers and Cisco C7600 Series Routers

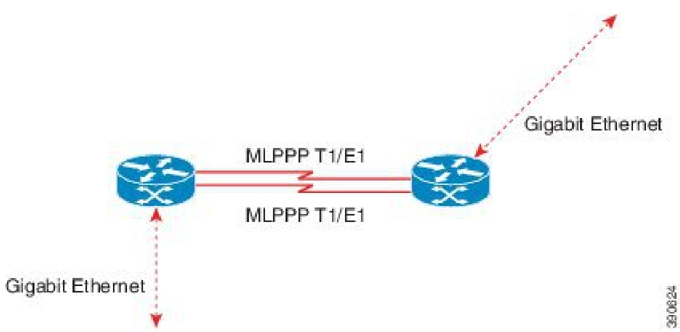
The following is a sample configuration of multilink between a Cisco ASR 901 Series Routers and Cisco C7600 Series Routers:

Figure 51: Multilink Between Cisco ASR 901 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.



The following sample configurations show how to configure multilink with maximum 10 links.

Policy Map 1

```
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
```

```
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-group7
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-policy output bcpmlpppqos
service instance 1 ethernet
  encapsulation  untagged
    bridge-domain 3000

interface Multilink2
service-policy output bcpmlpppqos
service instance 1 ethernet
  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-policy output bcpmlpppqos
service instance 2 ethernet
  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-policy output bcpmlpppdscp
service instance 1 ethernet
  encapsulation  untagged
    bridge-domain 3000
```

```
interface Multilink2
service-policy output bcpmlpppdscp
service instance 2 ethernet
  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-policy output bcpmlpppdscp
service instance 1 ethernet
  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-policy output bcpmlpppqos
 service instance 102 ethernet
  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
```

```
 ppp multilink group 1
interface Serial0/2:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/3:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/4:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/5:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/6:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/7:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/8:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/9:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Additional References

The following sections provide references related to BCP Support on MLPPP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco IOS Debug Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 3518	*Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)*

Technical Assistance

Table 54: Technical Assistance

[illegible]	[illegible]

CHAPTER 47

ITU-T G.8032 Ethernet Ring Protection Switching

The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

Effective from Cisco IOS Release 15.4 (3) S, the Cisco ASR 901 Router supports G.8032 on port-channel interface.

This chapter provides information about the following topics:

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 ITU-T G.8032 Ethernet Ring Protection Switching” 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 Configuring ITU-T G.8032 Ethernet Ring Protection Switching

- The Ethernet Flow Points (EFPs) must be configured.

Restrictions for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

- G.8032 is supported only on EFP bridgedomains on the physical interface and port-channel interface.
- G.8032 is supported only on EFP with dot1q, dot1ad, QinQ, or dot1ad-dot1Q encapsulation type.
- G.8032 is not supported on xconnect interface.
- G.8032 does not support more than two ERP instances per ring.
- CFM hardware offloading is supported on the Cisco ASR 901 Router only from Cisco IOS Release 15.4(3)S.
- Link flap occurs while configuring the inclusion or exclusion VLAN list.
- Admin shut down is highly recommended before making any changes in Connectivity Fault Management (CFM) configuration.
- The **efd notify** command must be used under CFM configuration to notify G.8032 of failures, if any.

Information About Configuring ITU-T G.8032 Ethernet Ring Protection Switching

The following features are supported on the Cisco ASR 901 Routers from Cisco IOS Release 15.4(2)S onwards.

G.8032 Overview

The G.8032 provides protection switching mechanisms, and a protocol for Ethernet layer network (ETH) rings. Ethernet rings provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol provide reliable and stable protection; and prevents loop formation, which could fatally affect network operation and service availability.

You can prevent loops in an Ethernet ring by ensuring that, at any moment, traffic can flow on all but one of the ring links, the Ring Protection Link (RPL), where the link is blocked in the working state. When the system detects a link failure, a Ring Automatic Protection Switching (RAPS) Signal Failure message is multicast to all the nodes, and the failed links end-point ports are blocked. When the RPL owner receives the message, it unblocks the RPL link. This triggers protection switching and a new traffic pattern is established on the ring. The blocked ports are then moved to the nodes next to the failed ones.

Effective from Cisco IOS Release 15.4(3)S, the Cisco ASR 901 Router supports G.8032 on port-channel interface and CFM hardware offloading.

The following functions of G.8032 are supported on the Cisco ASR 901 Router:

- Sub-second switching
- EFP bridge domain over physical and port-channel interfaces

- Up to six rings per node
- Up to two ERP instances per ring
- Open-ring and closed-ring support
- Open-ring without virtual channel
- G.8032-REP TCN interworking (TCN propagation)
- G.8032-G.8032 TCN interworking—TCN propagation from subring to major ring
- Minimum supported convergence time is 200 ms for a single instance, and 400 ms for multiple instances.
- Effective from Cisco IOS Release 15.4 (3) S, the Cisco ASR 901 Router supports CFM hardware offloading with CCM interval 100ms, 10ms, and 3.3ms.
- Minimum supported convergence time is 100 ms for a single instance, and 200 ms for multiple instances.

ITU-T G.8032 Ethernet Ring Protection Switching Functionality

The Ethernet ring protection functionality includes the following:

- Loop avoidance
- The use of learning, forwarding, and Filtering Database (FDB) mechanisms

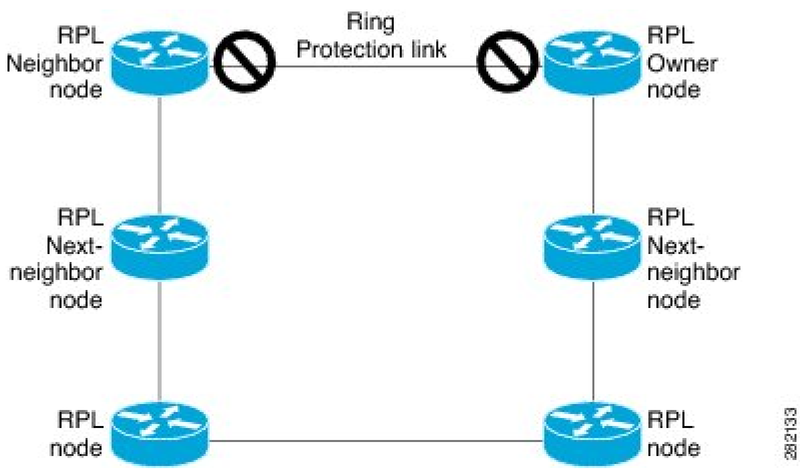
Loop avoidance in an Ethernet ring is achieved by ensuring that, at any time, traffic flows on all but the Ring Protection Link (RPL).

The following is a list of RPL types (or RPL nodes) and their functions:

- RPL owner—Responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic. There can be only one RPL owner in a ring.
- RPL neighbor node—An Ethernet ring node adjacent to the RPL. It is responsible for blocking its end of the RPL under normal conditions. This node type is optional and prevents RPL usage when protected.
- RPL next-neighbor node—Next-neighbor node is an Ethernet ring node adjacent to an RPL owner node or RPL neighbor node. It is mainly used for FDB flush optimization on the ring. This node is also optional.

The following figure illustrates the G.8032 Ethernet ring topology.

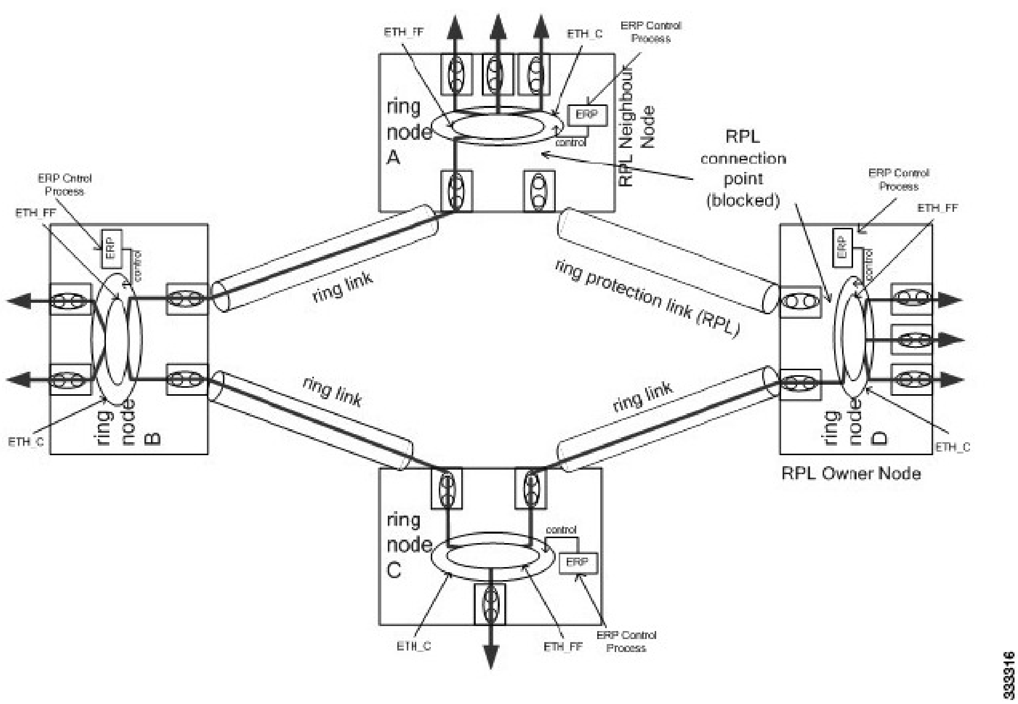
Figure 52: G.8032 Ethernet Ring Topology



Single-Ring Topology

The following figure shows a 4-node G.8032 single-ring topology. The RPL link is between node A and node D, and when the network works, the RPL link is blocked by the RPL owner node D and RPL neighbor node A.

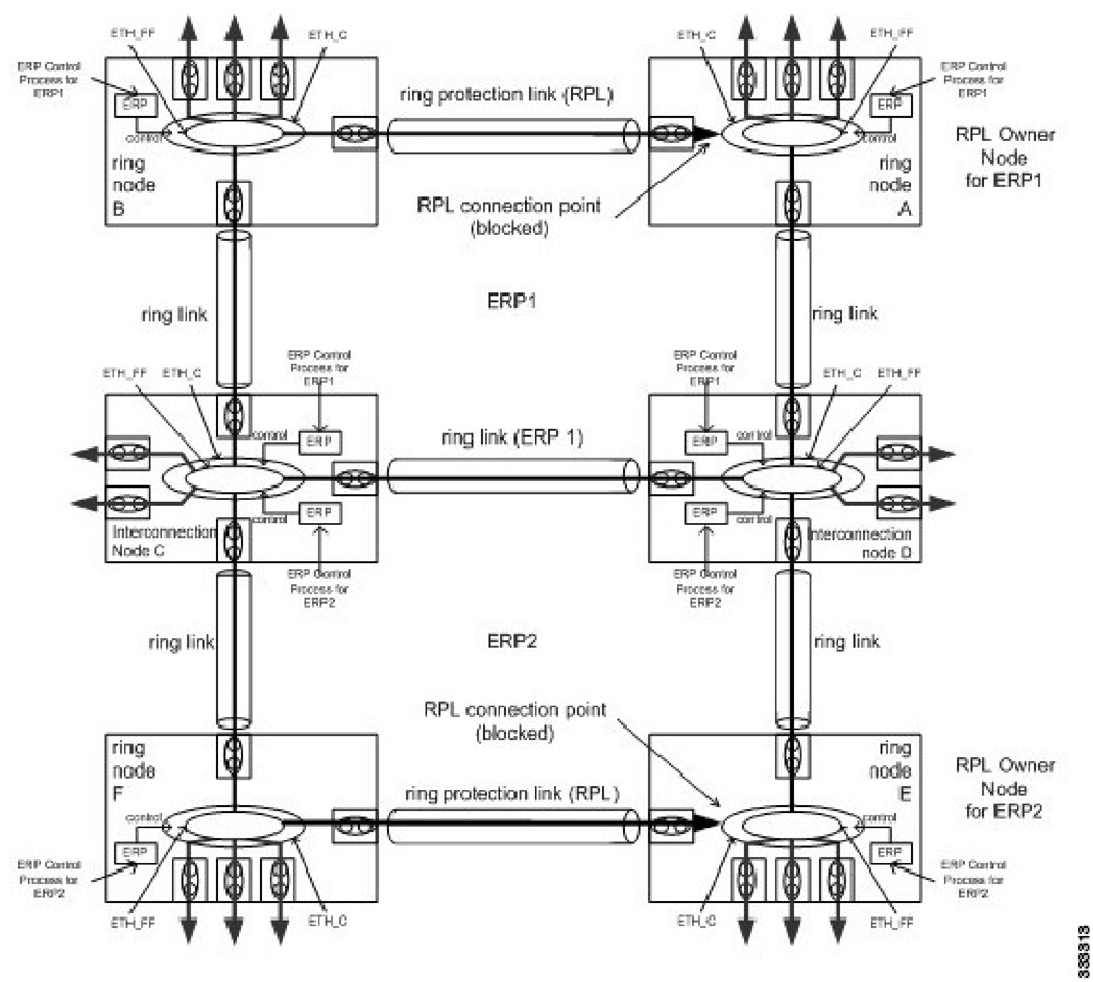
Figure 53: Single-Ring Topology



Multiple-Rings Topology

The following figure shows two interconnected rings in the multiple-rings topology. Ring ERP1 consists of nodes A, B, C, and D, and the links between these nodes. Ring ERP2 consists of nodes C, D, E, and F, and the links between C-to-F, F-to-E, and E-to-D. Ring ERP2 on its own does not form a closed loop since the link of C-to-D is owned and controlled by ring ERP1. The closed loop for ring ERP2 can be accomplished by introducing an RAPS virtual channel between the interconnected nodes, C and D, of the subring. The RAPS messages of ring ERP2 are encapsulated and transmitted over this virtual channel. If the RAPS virtual channel is not used to close the subring, the RAPS messages are terminated at the interconnected nodes. The blocked ports on all the nodes in the ring block only the data traffic, not the RAPS messages to prevent segmentation of the RAPS channel for a nonvirtual channel ring implementation.

Figure 54: Multiple-Rings Topology



R-APS Control Messages

Nodes on the ring use control messages called Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the ring protection link (RPL) on and off. Any failure along the ring triggers a R-APS Signal Failure (R-APS SF) message in both directions of the nodes adjacent to the failed link, after the nodes have blocked the port facing the failed link. On obtaining this message, the RPL owner unblocks the RPL port.

Note A single link failure in the ring ensures a loop-free topology.

CFM Protocols and Link Failures

Connectivity Fault Management (CFM) and link status messages are used to detect ring link failure and node failure. During the recovery phase, when the failed link is restored, the nodes adjacent to the restored link send RAPS No Request (RAPS-NR) messages. On obtaining this message, the RPL owner blocks the RPL port and sends a RAPS-NR or RAPS Root Blocked (RAPS-RB) message. These messages cause all other nodes, except the RPL owner in the ring, to unblock all the blocked ports. The Ethernet Ring Protection (ERP) protocol works for both unidirectional failure and multiple link failure scenarios in a ring topology.

When CFM monitoring is configured, note the following points:

- Static remote MEP (RMEP) checking should be enabled.
- The MEPs should be configured to enable Ethernet fault detection.

Note The G.8032 ERP protocol uses CFM Continuity Check Messages (CCMs) at an interval of 1 second. At this interval (which is supported only on selected platforms), SONET-like switching time performance and loop-free traffic can be achieved.

Note The G.8032 ERP protocol uses CFM Continuity Check Messages (CCMs) at an interval of 3.3 ms. At this interval (which is supported only on selected platforms), SONET-like switching time performance and loop-free traffic can be achieved.

Note For G.8032 with Connectivity Fault Management (CFM) hardware offload, the CFM VLANs must be included in the exclusion VLANs list to avoid the down state of G.8032 rings.

G.8032 Ring-Supported Commands and Functionality

A G.8032 ring supports these basic operator administrative commands:

- Force switch (FS)—Allows the operator to forcefully block a particular ring port. Note the following points about FS commands:
    - Effective even if there is an existing SF condition
    - Multiple FS commands for ring are supported
    - May be used to allow immediate maintenance operations

- Manual switch (MS)—Allows the operator to manually block a particular ring port. Note the following points about MS commands:
    - Ineffective in an existing FS or signal failure (SF) condition
    - Overridden by new FS or SF conditions
    - Multiple MS commands cancel all MS commands
- Clear—Cancels an existing FS or MS command on the ring port. The Clear command is used at the ring protection link (RPL) owner to clear a nonrevertive mode condition.

A G.8032 ring can support multiple instances. An instance is a logical ring running over a physical ring. Such instances are used for various reasons, such as load-balancing VLANs over a ring. For example, odd-numbered VLANs may go in one direction of the ring, and even-numbered VLANs may go in the other direction. Specific VLANs can be configured under only one instance. They cannot overlap multiple instances. Otherwise, data traffic or Ring Automatic Protection Switching (R-APS) messages may cross logical rings, which is not desirable.

G.8032 ERP Timers

The G.8032 Ethernet Ring Protection (ERP) protocol specifies the use of different timers to avoid race conditions and unnecessary switching operations:

- Delay timers—Used by the Ring Protection Link (RPL) owner to verify that the network has stabilized before blocking the RPL. Note the following points about delay timers.
    - After a signal failure (SF) condition, a Wait-to-Restore (WTR) timer is used to verify that the SF is not intermittent.
    - The WTR timer can be configured by the operator. The default time interval is 5 minutes; the time interval ranges from 1 to 12 minutes.
    - After a force switch (FS) or a manual switch (MS) command is issued, a Wait-to-Block (WTB) timer is used to verify that no background condition exists.

Note The WTB timer interval may be shorter than the WTR timer interval.

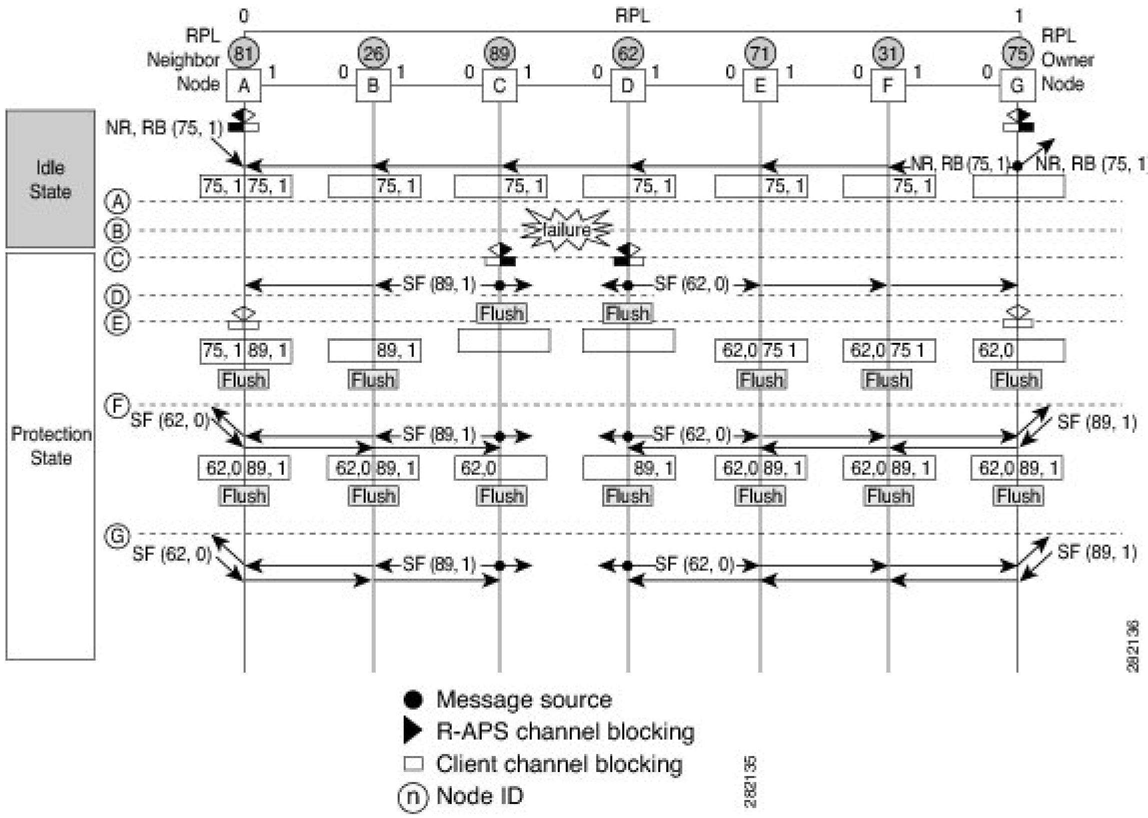
- Guard timer—Used by all nodes when changing state; the guard timer blocks latent outdated messages from causing unnecessary state changes. The guard timer can be configured. The default time interval is 500 ms; the time interval ranges from 10 to 2000 ms.
- Hold-off timers—Used by the underlying Ethernet layer to filter out intermittent link faults. The hold-off timer can be configured. The default time interval is 0 seconds; the time interval ranges from 0 to 10 seconds. Faults are reported to the ring protection mechanism only if this timer expires.

Protection Switching Functionality in a Single Link Failure and Recovery

The following figure illustrates protection switching functionality in a single-link failure.

The figure represents an Ethernet ring topology consisting of seven Ethernet ring nodes. The ring protection link (RPL) is the ring link between Ethernet ring nodes A and G. In this topology, both ends of the RPL are blocked. Ethernet ring node G is the RPL owner node, and Ethernet ring node A is the RPL neighbor node.

Figure 55: G.8032 Ethernet Ring Protection Switching in a Single-Link Failure

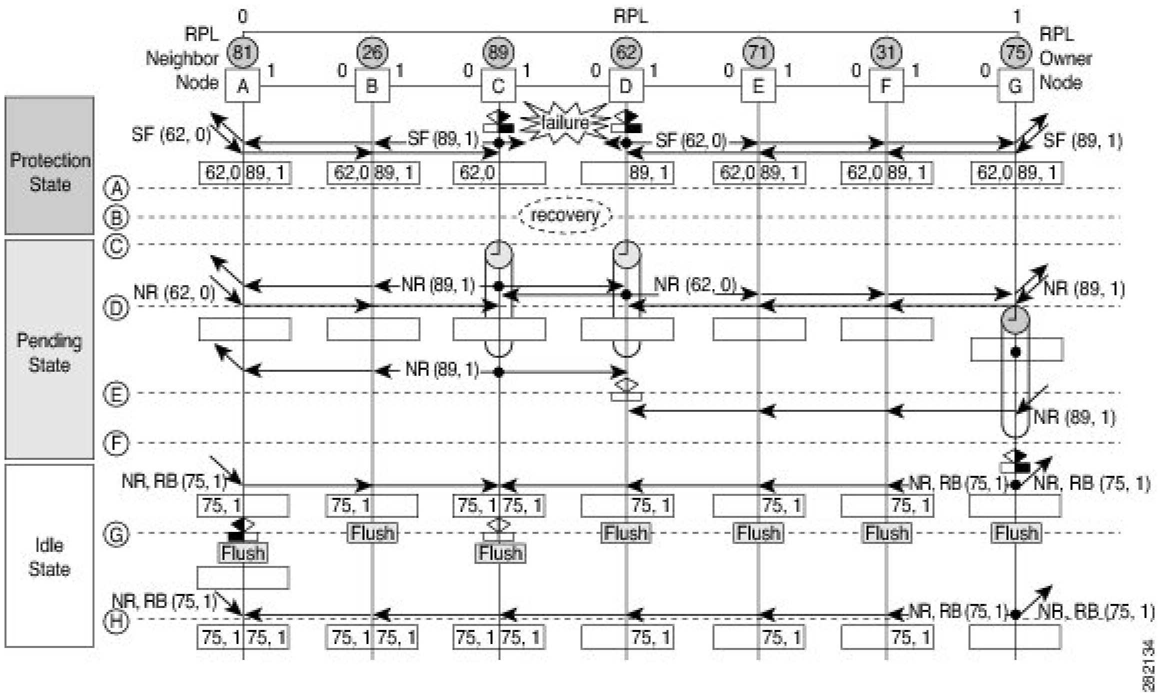


The following sequence describes the steps followed in the single-link failure:

1. A link operates in the normal condition.
2. A failure occurs.
3. Ethernet ring nodes C and D detect a local signal failure (SF) condition and after the hold-off time interval, block the failed ring port and perform the FDB flush.
4. Ethernet ring nodes C and D start sending Ring Automatic Protection Switching (R-APS) SF messages periodically along with the (node ID and bidirectional path-protected ring (BPR) identifier pair) on both ring ports while the SF condition persists.
5. All Ethernet ring nodes receiving an R-APS SF message perform the FDB flush. When the RPL owner node G and RPL neighbor node A receive an R-APS SF message, the Ethernet ring node unblocks its end of the RPL and performs the FDB flush.
6. All Ethernet ring nodes receiving a second R-APS SF message perform the FDB flush again; the additional FDB flush is because of the node ID and BPR-based configuration.
7. R-APS SF messages are detected on the Ethernet Ring indicating a stable SF condition. Further R-APS SF messages trigger no further action.

The following figure illustrates the steps taken in a revertive operation in a single-link failure.

Figure 56: Single-Link Failure Recovery (Revertive Operation)



The following sequence describes the steps followed in the single-link failure revertive (recovery) operation:

1. A link operates in the stable SF condition.
2. Recovery of link failure occurs.
3. Ethernet ring nodes C and D detect clearing of the SF condition, start the guard timer, and initiate periodic transmission of the R-APS No Request (NR) messages on both ring ports. (The guard timer prevents the reception of R-APS messages.)
4. When the Ethernet ring nodes receive an R-APS NR message, the node ID and BPR identifier pair of a receiving ring port is deleted and the RPL owner node starts the Wait-to-Restore (WTR) timer.
5. When the guard timer expires on Ethernet ring nodes C and D, the nodes may accept the new R-APS messages, if any. Ethernet ring node D receives an R-APS NR message with a higher node ID from Ethernet ring node C, and unblocks its nonfailed ring port.
6. When the WTR timer expires, the RPL owner node blocks its end of the RPL, sends R-APS (NR or route blocked [RB]) message with the (node ID and BPR identifier pair), and performs the FDB flush.
7. When Ethernet ring node C receives an R-APS (NR or RB) message, the node removes the block on its blocked ring ports, and stops sending R-APS NR messages. On the other hand, when the RPL neighbor node A receives an R-APS NR or RB message, the node blocks its end of the RPL. In addition, Ethernet ring nodes A to F perform the FDB flush when receiving an RAPS NR or RB message because of the node ID and BPR-based configuration.

How to Configure ITU-T G.8032 Ethernet Ring Protection Switching

Configuring the Ethernet Ring Profile

To configure an Ethernet ring profile, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet ring g8032 profile** *profile-name* **Example:** `Router(config)# ethernet ring g8032 profile profile1`	Creates the Ethernet ring profile and enters the Ethernet ring profile configuration mode.
Step 4	**timer{guard** *seconds*| **hold-off** *seconds* **| wtr** *minutes***}** **Example:** `Router(config-erp-profile)# timer hold-off 5`	Specifies the time interval for the guard, hold-off, and Wait-to-Restore (WTR) timers.
Step 5	**non-revertive** **Example:** `Router(config-erp-profile)# non-revertive`	Specifies a nonrevertive Ethernet ring instance. By default, Ethernet ring instances are revertive.
Step 6	**end** **Example:** `Router(config-erp-profile)# end`	Returns to privileged EXEC mode.

Configuring an Ethernet Protection Ring

To configure an Ethernet Protection Ring (EPR), complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet ring g8032** *ring-name* **Example:** `Router(config)# ethernet ring g8032 ring1`	Creates the Ethernet ring and enters the Ethernet ring port configuration mode.
Step 4	**port0 interface** *type number* **Example:** `Router(config-erp-ring)# port0 interface gigabitethernet 0/1`	Connects port0 of the local node to the Ethernet ring and enters Ethernet ring protection mode.
Step 5	**monitor service instance** *instance-id* **Example:** `Router(config-erp-ring-port)# monitor service instance 1`	(Optional) Assigns the Ethernet service instance to monitor the ring port (port0) and detect ring failures. If this command is used, the service instance should be configured with CFM sessions. In such a scenario, CFM session failures, if any, will be tracked as G.8032 link failures. **Note** We recommend that you use this command in microwave links where signal degradation will not be identified as physical link failures. If this command is not used, G.8032 will track only the physical link failures.
Step 6	**exit** **Example:** `Router(config-erp-ring-port)# exit`	Exits the Ethernet ring port configuration mode.

	Command or Action	Purpose
Step 7	**port1 {interface** *type number* **| none}** **Example:** `Router(config-erp-ring)# port1 interface gigabitethernet 0/1`	Connects port1 of the local node to the Ethernet ring and enters the Ethernet ring protection mode.
Step 8	**monitor service instance** *instance-id* **Example:** `Router(config-erp-ring-port)# monitor service instance 2`	(Optional) Assigns the Ethernet service instance to monitor the ring port (port1) and detect ring failures. If this command is used, the service instance should be configured with CFM sessions. In such a scenario, CFM session failures, if any, will be tracked as G.8032 link failures. **Note** We recommend that you use this command in microwave links where signal degradation will not be identified as physical link failures. If this command is not used, G.8032 will track only the physical link failures.
Step 9	**exit** **Example:** `Router(config-erp-ring-port)# exit`	Exits Ethernet ring port configuration mode.
Step 10	**exclusion-list vlan-ids** *vlan-id* **Example:** `Router(config-erp-ring)# exclusion-list vlan-ids 2`	(Optional) Specifies VLANs that are unprotected (unblocked) by the Ethernet ring protection mechanism. If the command is not used, VLANS that are not defined in the inclusion list in 16 will be completely blocked for the traffic. If the command is used, VLANS that are not defined in the inclusion list and exclusion list will be completely blocked for the traffic.
Step 11	**open-ring** **Example:** `Router(config-erp-ring)# open-ring`	(Optional) Specifies the Ethernet ring as an open ring. By default, Ethernet ring is closed.
Step 12	**instance** *instance-id* **Example:** `Router(config-erp-ring)# instance 1`	Configures the Ethernet ring instance and enters the Ethernet ring instance configuration mode.

	Command or Action	Purpose
Step 13	**description** *descriptive-name* **Example:** `Router(config-erp-inst)# description cisco_customer_instance`	Specifies a descriptive name for the Ethernet ring instance.
Step 14	**profile** *profile-name* **Example:** `Router(config-erp-inst)# profile profile1`	Specifies the profile associated with the Ethernet ring instance configured in 12.
Step 15	**rpl {port0 | port1 } { owner | neighbor | next-neighbor}** **Example:** `Router(config-erp-inst)# rpl port0 neighbor`	Specifies the Ethernet ring port on the local node as the RPL owner, neighbor, or next neighbor.
Step 16	**inclusion-list vlan-ids** *vlan-id* **Example:** `Router(config-erp-inst)# inclusion-list vlan-ids 11`	Specifies the VLANs that are protected by the Ethernet ring protection mechanism.
Step 17	**aps-channel** **Example:** `Router(config-erp-inst)# aps-channel`	Enters the Ethernet ring instance aps-channel configuration mode.
Step 18	**level** *level-value* **Example:** `Router(config-erp-inst-aps)# level 5`	Specifies the Automatic Protection Switching (APS) message level for the node on the Ethernet ring. All the nodes in the Ethernet ring must be configured at the same level. The default level is 7.
Step 19	**port0 service instance** *instance-id* **Example:** `Router(config-erp-inst-aps)# port0 service instance 100`	Associates APS channel information with port0.
Step 20	**port1 service instance** *instance-id* **Example:** `Router(config-erp-inst-aps)# port1 service instance 100`	Associates APS channel information with port1.

	Command or Action	Purpose
Step 21	**end** **Example:** `Router(config-erp-inst-aps)# end`	Returns to privileged EXEC mode.

Configuring Topology Change Notification Propagation

To configure topology change notification (TCN) propagation, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet tcn-propogation G8032 to {REP | G8032}** **Example:** `Router (config)# ethernet tcn-propagation G8032 to G8032`	Allows topology change notification (TCN) propagation from a source protocol to a destination protocol. **Note** Source and destination protocols vary by platform and release.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Verifying Ethernet Ring Protection Configuration

Verifying ERP Switching Configuration

To verify an ERP switching configuration, use the **show ethernet ring g8032 configuration** command, as shown in this example:

```
Router# show ethernet ring g8032 configuration

Ethernet ring erp
 Port0: Port-channel5 (Monitor: Service Instance 5)
 Port1: Port-channel6 (Monitor: Service Instance 6)
```

```
 Exclusion-list VLAN IDs: 5-6
 Open-ring: no
 Instance 1
  Description: ERP_FOR_VLANS_1000-1299
  Profile:     erp
  RPL:         port0 RPL Owner
  Inclusion-list VLAN IDs: 1000-1299
  APS chanel
   Level: 6
   Port0: Service Instance 1000
   Port1: Service Instance 1000
  State: configuration resolved
 Instance 2
  Description: ERP_FOR_VLANS_1500-1799
  Profile:     erp
  RPL:
  Inclusion-list VLAN IDs: 1500-1799
  APS channel
   Level: 5
   Port0: Service Instance 1500
   Port1: Service Instance 1500
  State: configuration resolved
  <cr>
```

Verifying Functional State of a Ring

To verify a brief description of the functional state of the ERP instance, use the **show ethernet ring g8032 brief [***ring-name***] [instance [***instance-id* **]]** command, as shown in this example:

```
Router# show ethernet ring g8032 brief erp instance 1
R: Interface is the RPL-link
F: Interface is faulty
B: Interface is blocked
FS: Local forced switch
MS: Local manual switch

RingName                         Inst NodeType  NodeState     Port0    Port1
--------------------------------------------------------------------------------
erp                              1    Owner     Idle          R,B
```

Verifying Ring Status

To verify the status summary of a ring , use the **show ethernet ring g8032 status [***ring-name***] [instance [***instance-id* **]]** command, as shown in this example:

```
Router# show ethernet ring g8032 status erp instance 1
Ethernet ring erp instance 1 is RPL Owner node in Idle State
 Port0: Port-channel5 (Monitor: Service Instance 5)
  APS-Channel: Port-channel5
  Status: RPL, blocked
  Remote R-APS NodeId: 0000.0000.0000, BPR: 0
 Port1: Port-channel6 (Monitor: Service Instance 6)
  APS-Channel: Port-channel6
  Status: Non-RPL
  Remote R-APS NodeId: 0000.0000.0000, BPR: 0
 APS Level: 6
 Profile: erp
  WTR interval: 1 minutes
  Guard interval: 2000 milliseconds
  HoldOffTimer: 0 seconds
```

```
 Revertive mode
```

Verifying Ring Summary

To view the summary of the number of ERP instances in each state of the ERP switching process, use the **show ethernet ring g8032 summary** command, as shown in this example:

```
Router# show ethernet ring g8032 summary
Chassis Node Id: 4403.a70c.4e98

States
-----------------------------
 Init              0
 Idle              2
 Protection        0
 Manual Switch     0
 Forced Switch     0
 Pending           0
 ----------------------------
 Total             2
```

Verifying Events and Messages in a Ring

To verify the number the number of events and R-APS messages received for an ERP instance, use the **show ethernet ring g8032 statistics [** *ring-name*] **[instance [***instance-id* **]]** command, as shown in this example:

```
Router# show ethernet ring g8032 statistics erp instance 1
Statistics for Ethernet ring erp instance 1
 Local SF detected:
  Port0: 1
  Port1: 0
 FOP PM detected:
  Port0: 0
  Port1: 0

 R-APS   Port0(Tx/Rx)                    Port1(Tx/Rx)
         Last Tx time                    Last Tx time
         Last Rx time                    Last Rx time
 ----------------------------------------------------------------------------------
 NR    : 6/14                            6/13
         Wed May 14 15:46:44.391         Wed May 14 15:46:44.391
         Wed May 14 15:47:42.699         Wed May 14 15:47:42.699
 NR,RB : 157/0                           157/0
         Wed May 14 16:00:34.391         Wed May 14 16:00:34.391
         Never                           Never
 SF    : 5/4                             5/2
         Wed May 14 15:46:40.043         Wed May 14 15:46:40.043
         Wed May 14 15:46:44.639         Wed May 14 15:46:45.503
 MS    : 0/0                             0/0
         Never                           Never
         Never                           Never
 FS    : 0/0                             0/0
         Never                           Never
         Never                           Never
 EVENT : 0/0                             0/0
         Never                           Never
         Never                           Never

 State           Last entry into state time
```

```
 --------------------------------------------------------------------------------
 Init          : Wed May 14 15:46:29.903
 Idle          : Wed May 14 15:47:44.391
 Protection    : Wed May 14 15:46:30.039
 Manual Switch : Never
 Forced Switch : Never
 Pending       : Wed May 14 15:46:44.391

Router# show ethernet ring g8032 statistics erp instance 2
Statistics for Ethernet ring erp instance 2
 Local SF detected:
  Port0: 1
  Port1: 0
 FOP PM detected:
  Port0: 0
  Port1: 0

 R-APS   Port0(Tx/Rx)                    Port1(Tx/Rx)
         Last Tx time                    Last Tx time
         Last Rx time                    Last Rx time
 --------------------------------------------------------------------------------
 NR    : 6/14                            6/13
         Wed May 14 15:46:44.395         Wed May 14 15:46:44.395
         Wed May 14 15:47:42.699         Wed May 14 15:47:42.699
 NR,RB : 0/155                           0/3
         Never                           Never
         Wed May 14 16:00:42.255         Wed May 14 15:47:47.255
 SF    : 5/3                             5/1
         Wed May 14 15:46:43.191         Wed May 14 15:46:43.191
         Wed May 14 15:46:44.643         Wed May 14 15:46:43.407
 MS    : 0/0                             0/0
         Never                           Never
         Never                           Never
 FS    : 0/0                             0/0
         Never                           Never
         Never                           Never
 EVENT : 0/0                             0/0
         Never                           Never
         Never                           Never

 State           Last entry into state time
 --------------------------------------------------------------------------------
 Init          : Wed May 14 15:46:32.827
 Idle          : Wed May 14 15:47:47.255
 Protection    : Wed May 14 15:46:33.123
 Manual Switch : Never
 Forced Switch : Never
 Pending       : Wed May 14 15:46:44.395
```

Verifying Port Status of a Ring

To verify the Ethernet ring port status information for the interface, use the **show ethernet ring g8032 port status interface [***type number* **]** command, as shown in this example:

```
Router# show ethernet ring g8032 port status interface po5
Port: Port-channel5
 Ring: erp
         Block vlan list: 1-4,7-1499,1800-4095
         Unblock vlan list: 5-6,1500-1799
         REQ/ACK: 0/0
         Instance 1 is in Blocked state
         Instance 2 is in Unblocked state
```

Verifying ERP Profile Settings

To verify the settings for one or more ERP profiles, use the **show ethernet ring g8032 profile [***profile-name***]** command, as shown in this example:

```
Router# show ethernet ring g8032 profile erp
Ethernet ring profile name: erp
  WTR interval: 1 minutes
  Guard interval: 2000 milliseconds
  HoldOffTimer: 0 seconds
  Revertive mode
```

Troubleshooting Tips

The following table lists the troubleshooting tips for Configuring the ITU-T G.8032 Ethernet Ring Protection feature.

Note We recommend that you do not use these debug commands without TAC supervision.

Table 55: Troubleshooting Tips for G.8032 ERP Configuration

Command Name	Description
[no] debug ethernet ring g8032 all	Enables debugging all Ethernet Ring Protocol (ERP) messages.
[no] debug ethernet ring g8032 errors	Enables debugging ERP errors.
[no] debug ethernet ring g8032 events	Enables debugging ERP events.
[no] debug ethernet ring g8032 fsm	Enables debugging Finite State Machine (FSM) state changes for ERP instances
[no] debug ethernet ring g8032 ha	Enables debugging ERP high availability (HA) features.
[no] debug ethernet ring g8032 packets	Enables debugging ERP packets.
[no] debug ethernet ring g8032 parser	Enables debugging ERP messages related to G.8032 parser.
[no] debug ethernet ring g8032 timing	Enables debugging timing of ERP events.
[no] debug ethernet ring g8032 memmgr	Enables debugging G.8032 memory manager messages.
[no] debug ethernet ring g8032 cfgmgr	Enables debugging G.8032 configuration manager messages.
[no] debug ethernet ring g8032 ctrlmgr	Enables debugging G.8032 control manager messages.

Command Name	Description
[no] debug ethernet ring g8032 instmgr	Enables debugging G.8032 instance manager messages.
[no] debug ethernet ring g8032 pseudo-preemption	Enables debugging G.8032 pseudo-preemption messages.

Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching

Example: Configuration for Ethernet Ring Protection

The following is a sample ERP switching configuration:

```
Owner:

!
ethernet ring g8032 profile closed_ring
 timer wtr 1
 timer guard 2000
ethernet ring g8032 pp_closed
 port0 interface GigabitEthernet0/9
  monitor service instance 1
 port1 interface GigabitEthernet0/10
  monitor service instance 5
 instance 1
  profile closed_ring
  rpl port0 owner
  inclusion-list vlan-ids 1-10
  aps-channel
   level 5
   port0 service instance 10
   port1 service instance 10
!

!

Router# show run | sec cfm
asr901-platf-multi-nni-cfm
ethernet cfm ieee
ethernet cfm global
ethernet cfm domain closed_ring1 level 4
 service closed_ring1 evc closed_ring1 vlan 1 direction down
  continuity-check
  continuity-check interval 1s
  efd notify g8032
ethernet cfm domain closed_ring5 level 4
 service closed_ring5 evc closed_ring5 vlan 5 direction down
  continuity-check
  continuity-check interval 1s
  efd notify g8032

!

!
```

```
Neighbor:

Router# show run | sec ring
ethernet ring g8032 profile closed_ring
 timer wtr 1
 timer guard 2000
ethernet ring g8032 closed_ring
 port0 interface GigabitEthernet0/9
  monitor service instance 5
 port1 interface GigabitEthernet0/6
  monitor service instance 4
 instance 1
  profile closed_ring
  rpl port0 neighbor
  inclusion-list vlan-ids 1-10
  aps-channel
   level 5
   port0 service instance 10
   port1 service instance 10
 !
```

Additional References

The following sections provide references related to the Configuring ITU-T G.8032 Ethernet Ring Protection feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference Cisco ASR 901S Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 56: Feature Information for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

Feature Name	Releases	Feature Information
Configuring ITU-T G.8032 Ethernet Ring Protection Switching	15.4(2)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • G.8032 Overview, on page 896 • How to Configure ITU-T G.8032 Ethernet Ring Protection Switching, on page 904 • Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching, on page 913
Psuedo Preemption Support	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • G.8032 Overview, on page 896 • How to Configure ITU-T G.8032 Ethernet Ring Protection Switching, on page 904
CFM Filtering Hardware Offload Support	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: • G.8032 Overview, on page 896

CHAPTER 48

Configuring NAT for IP Address Conservation

This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure the inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded to the corresponding network.

NAT can be configured to advertise to the outside world only one address for the entire network. This provides additional security by effectively hiding the entire internal network behind that one address.

NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

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 NAT" 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 Configuring NAT for IP Address Conservation

- This feature is supported only on the following PIDs of the Cisco ASR 901 Router: A901-6CZ-FS-D and A901-6CZ-FS-A.

Restrictions for Configuring NAT for IP Address Conservation

The following limitations and configuration guidelines apply when configuring NAT on the Cisco ASR 901 Router:

- NAT-T is not supported.
- Dynamic NAT with pools in the same network as on the NAT interfaces.
- Port channel for NAT and Port Address Translation (PAT) are not supported.
- Simple Network Management Protocol (SNMP) MIB is not supported for NAT.
- Dynamic NAT with Extended ACL is not supported.
- This feature is available only on the new software image named *asr901sec-universalk9.mz*. (This feature is not available on the standalone software image named *asr901-universalk9.mz*. If you use asr901sec-universalk9.mz in an unsupported Cisco ASR 901 PID, the router issues a warning message and loads the software with basic features.)
- Maximum bidirectional throughput supported for ESP-NAT traffic is 250 Mbps.
- TCP-NAT traffic with frame size greater than 1496 is not supported.

Note Throughput is low with fragmentation (around 300 Kbps).

Information About Configuring NAT for IP Address Conservation

The following features are supported on the Cisco ASR 901 Routers from Cisco IOS Release 15.4(2)S onwards.

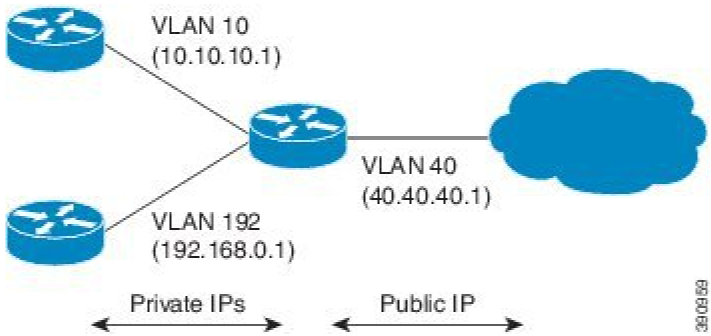
Overview

You can translate IP addresses into globally unique IP addresses when communicating outside your network.

You can configure static or dynamic inside-source address translation as follows:

- Static translation establishes a one-to-one mapping between an inside local address and an inside global address. Static translation is useful when a host on the inside has to be accessed by a fixed address from the outside.
- Dynamic translation establishes mapping between an inside local address and a pool of global addresses.

The following figure shows the translation of a source address inside a network to a source address outside the network.



You can conserve addresses in the inside global address pool by allowing a device to use one global address for many local addresses. This type of Network Address Translation (NAT) configuration is called overloading. When overloading is configured, the device maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between local addresses.

How NAT Works

A device that is configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit device between a stub domain and the backbone. When a packet leaves the domain, NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table.

If NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet to the destination.

Types of NAT

NAT operates on a router—generally connecting only two networks—and translates the private (inside local) addresses within the internal network into public (inside global) addresses before packets are forwarded to another network. This functionality gives you the option to configure NAT such that it will advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the world, giving you additional security.

The types of NAT include:

- Static address translation (static NAT)—Allows one-to-one mapping between local and global addresses.
- Dynamic address translation (dynamic NAT)—Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.
- Overloading—Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as PAT. By using overloading, thousands of users can be connected to the Internet by using only one real global IP address.

NAT Inside and Outside Addresses

The term *inside* in NAT context refers to networks owned by an organization, and which must be translated. When NAT is configured, hosts within this network will have addresses in one space (known as the local address space) that will appear to those outside the network as being in another space (known as the global address space).

Similarly, the term *outside* refers to those networks to which the stub network connects, and which are generally not under the control of an organization. Hosts in outside networks can also be subject to translation, and can thus have local and global addresses.

NAT uses the following definitions:

- Inside local address—An IP address that is assigned to a host on the inside network. The address is probably not a valid IP address assigned by the Network Information Center (NIC) or service provider.
- Inside global address—A valid IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.
- Outside local address—The IP address of an outside host as it appears to the inside network. Not necessarily a valid address, it is allocated from the address space that is routable on the inside.
- Outside global address—The IP address assigned to a host on the outside network by the owner of the host. The address is allocated from a globally routable address or network space.

Static IP Address Support

A public wireless LAN provides users of mobile computing devices with wireless connections to a public network, such as the Internet.

The NAT Static IP Address Support feature extends the capabilities of public wireless LAN providers to support users configured with a static IP address. By configuring a device to support users with a static IP address, public wireless LAN providers extend their services to a greater number of users.

Users with static IP addresses can use services of the public wireless LAN provider without changing their IP address. NAT entries are created for static IP clients, and a routable address is provided.

Supported Components

The following components are supported as part of the NAT feature:

- Static NAT and PAT
- Dynamic NAT and PAT with overload
- NAT and PAT support for Layer 3-forwarded traffic.
- Maximum number of inside and outside addresses is 10.
- Coexistence with Layer 2 and Layer 3 traffic

How to Configure NAT for IP Address Conservation

The tasks described in this section configure NAT for IP address conservation. You must configure at least one of the tasks described in this section. Based on your configuration, you may have to configure more than one task.

Configuring an Inside Source Address

Inside source addresses can be configured for static or dynamic translations. Based on your requirements, you can configure either static or dynamic translations.

Note You must configure different IP addresses for an interface on which NAT is configured and for inside addresses that are configured, by using the **ip nat inside source static** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 10`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *ip_address mask* **Example:** `Router(config-if)# ip address 10.10.10.1 255.255.255.0`	Sets a primary IP address for an interface.
Step 5	ip nat inside **Example:** `Router(config-if)# ip nat inside`	Connects the interface to the inside network, which is subject to NAT.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**ip address** *ip_address mask* **Example:** `Router(config-if)# ip address 40.40.40.1 255.255.255.0`	Sets a primary IP address for an interface.
Step 9	ip nat outside **Example:** `Router(config-if)# ip nat outside`	Connects the interface to the outside network.
Step 10	**ip nat inside source static** *ilocal-ip global-ip* **Example:** `Router(config)# ip nat inside source static 10.10.10.2 40.40.40.1`	Establishes static translation between an inside local address and an inside global address.
Step 11	end **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Dynamic Translation of Inside Source Addresses Without Overload

Dynamic translation establishes a mapping between an inside local addresses and a pool of global addresses. Dynamic translation is useful when multiple users on a private network have to access the Internet. The dynamically configured pool IP address can be used as required, and is released for use by other users when access to the Internet is no longer required.

Note Cisco ASR 901 Router does not differentiate between the dynamic translation with overload and dynamic translation without overload. By default, overloading is considered if translation exceeds the given pool.

Note When inside global or outside local addresses belong to a directly connected subnet on a NAT device, the device adds IP aliases for them so that it can answer Address Resolution Protocol (ARP) requests. However, a situation where the device answers packets that are not destined for it, possibly causing a security issue, may arise. This may happen when an incoming Internet Control Message Protocol (ICMP) packet or a UDP packet that is destined for one of the alias addresses does not have a corresponding NAT translation in the NAT table, and the device itself runs a corresponding service, for example, Network Time Protocol (NTP). Such a situation might cause minor security risks.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 10`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.1 255.255.255.0`	Sets a primary IP address for the interface.
Step 5	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Connects the interface to the inside network, that is subject to NAT.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to the global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 40.40.40.1 255.255.255.0`	Sets a primary IP address for the interface.
Step 9	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Connects the interface to the outside network.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 11	**ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}** **Example:** `Router(config)# ip nat pool net-208 50.50.50.1 50.50.50.10 netmask 255.255.255.0`	Defines a pool of global addresses to be allocated as required.
Step 12	**access-list access-list-number permit source [source-wildcard]** **Example:** `Router(config)# access-list 1 permit 10.10.10.2 0.0.0.0`	Defines a standard access list permitting those addresses that are to be translated.
Step 13	**ip nat inside source list access-list-number pool** *name* **Example:** `Router(config)# ip nat inside source list 1 pool net-208`	Establishes dynamic source translation, specifying the access list defined in 12.
Step 14	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Dynamic Translation of Inside Source Addresses with Overload

You can conserve addresses in the inside global address pool by allowing a device to use one global address for many local addresses. This type of NAT configuration is called overloading. When overloading is configured, the device maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between local addresses.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Specifies an interface type and number, and enters the interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface vlan 10`	
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.1 255.255.255.0`	Sets a primary IP address for the interface.
Step 5	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Connects the interface to the inside network, that is subject to NAT.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 40.40.40.1 255.255.255.0`	Sets a primary IP address for the interface.
Step 9	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Connects the interface to the outside network.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}** **Example:** `Router(config)# ip nat pool net-208 50.50.50.1 50.50.50.10 netmask 255.255.255.0`	Defines a pool of global addresses to be allocated as required.
Step 12	**access-list access-list-number permit source** *[source-wildcard]* **Example:** `Router(config)# access-list 1 permit 10.10.10.2 0.0.0.0`	Defines a standard access list permitting those addresses that are to be translated.

	Command or Action	Purpose
Step 13	**ip nat inside source list access-list-number pool** *name* **overload** **Example:** `Router(config)# ip nat inside source list 1 pool net-208 overload`	Establishes dynamic source translation, specifying the access list defined in 12.
Step 14	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Static PAT

To configure a static PAT, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 10`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.1 255.255.255.0`	Sets a primary IP address for an interface.
Step 5	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Connects the interface to the inside network, that is subject to NAT.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**interface** *type number* **Example:** `Router(config)# interface vlan 40`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 40.40.40.1 255.255.255.0`	Sets a primary IP address for an interface.
Step 9	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Connects the interface to the outside network.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**ip nat outside source static tcp** *local-ip local-port global-ip global-port* **Example:** `Router(config)# ip nat outside source static tcp 10.10.10.2 23 40.40.40.10 2023`	Establishes static translation for outside network. Also, enables the use of Telnet to the device from the outside.
Step 12	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying Configuration of NAT for IP Address Conservation

To verify the NAT configuration, use the **show ip nat translation** command:

```
Router# show ip nat translation
SNAT: Proto udp Inside local ip is 10.10.10.2 Inside global ip 40.40.40.10 input 1146 output
 0
DNAT: Proto tcp Outside local ip is 40.40.40.10 Outside global ip 10.10.10.2 input 8 output
 5
```

Configuration Examples for NAT for IP Address Conservation

Example: Configuring Inside Source Address

The following is a sample configuration of static NAT:

```
interface vlan10
ip address 10.10.10.1 255.255.255.0
```

```
ip nat inside
int vlan40
ip address 40.40.40.1 255.255.255.0
ip nat outside
ip nat inside source static 10.10.10.2 40.40.40.1
ip nat inside source static 192.168.1.2 40.40.40.2
```

Example: Configuring Dynamic Translation of Inside Source Addresses Without Overload

The following is a sample configuration of dynamic NAT without overload:

```
interface vlan10
ip address 10.10.10.1 255.255.255.0
ip nat inside
interface vlan192
ip address 192.168.0.1 255.255.255.0
ip nat inside
interface vlan40
ip address 40.40.40.1 255.255.255.0
ip nat outside
ip nat pool no-overload 50.50.50.10 50.50.50.10 netmask 255.255.255.0
access-list 7 permit 10.10.10.0 0.0.0.255
ip nat inside source list 7 pool no-overload
```

Example: Configuring Dynamic Translation of Inside Source Addresses with Overload

The following is a sample configuration of dynamic NAT with overload:

```
interface vlan10
ip address 10.10.10.1 255.255.255.0
ip nat inside
interface vlan192
ip address 192.168.0.1 255.255.255.0
ip nat inside
interface vlan40
ip address 40.40.40.1 255.255.255.0
ip nat outside
ip nat pool overld 50.50.50.10 50.50.50.10 netmask 255.255.255.0
access-list 7 permit 10.10.10.0 0.0.0.255
ip nat inside source list 7 pool overld overload
```

Example: Configuring Static PAT

The following is a sample configuration of static PAT:

```
interface vlan10
ip address 10.10.10.1 255.255.255.0
ip nat inside
interface vlan192
ip address 192.168.0.1 255.255.255.0
ip nat inside
interface vlan40
ip address 40.40.40.1 255.255.255.0
ip nat outside
ip nat inside source static tcp 10.10.10.2 23 40.40.40.1 2323
```

Additional References

The following sections provide references related to Configuring NAT for IP Address Conservation feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Command Reference	Cisco ASR 901 Series Aggregation Services Router Command Reference
Cisco IOS Interface and Hardware Component Commands	Cisco IOS Interface and Hardware Component Command Reference

Standards

Standard	Title
None	—

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for Configuring NAT for IP Address Conservation

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 57: Feature Information for NAT

Feature Name	Releases	Feature Information
Configuring NAT for IP Address Conservation	15.4(2)S	This feature was introduced on the Cisco ASR 901 Routers.

CHAPTER 49

Auto-IP

Auto-IP

Auto-IP

In ring topology, when a device is inserted into the ring, the neighboring node interfaces require manual reconfiguration. The auto-IP feature addresses the problem of manually reconfiguring nodes during insertion, deletion, and movement of nodes within the ring. The auto-IP feature automatically provides IP addresses to the nodes inserted into the ring. For information on how to configure Auto-IP, see the IPv4 Addressing Configuration Guide, Cisco IOS XE Release 15.3(3)S.

The Auto-IP feature is supported on the Cisco ASR 901 series routers with the following restrictions:

- Auto-IP configuration is not supported on the switch virtual interface (SVI) associated with a port channel.
- Manual intervention is mandatory for inserting and deleting nodes because auto-IP is configured on the SVI.
- Auto-IP configuration is not supported for routers that are connected by a switch. It is supported only for directly connected routers.
- Auto-IP-Ring configuration needs to be removed manually on the SVI before defaulting or removing the SVI.

CHAPTER 50

IPv6 Routing: OSPFv3 Authentication Support with IPsec

In order to ensure that Open Shortest Path First version 3 (OSPFv3) packets are not altered and re-sent to the device, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

Prerequisites for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3 in order to enable authentication and encryption.

Restrictions for IPv6 Routing: OSPFv3 Authentication Support with IPsec

The OSPF for IPv6(OSPFv3) Authentication Support with IPsec feature is not supported on the IP BASE license package. The Advanced Enterprise Services package license must be used.

Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec

OSPFv3 Authentication Support with IPsec

In order to ensure that OSPFv3 packets are not altered and re-sent to the device, causing the device to behave in a way not desired by its system administrators, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

OSPFv3 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPFv3.

In OSPFv3, authentication fields have been removed from OSPFv3 packet headers. When OSPFv3 runs on IPv6, OSPFv3 requires the IPv6 authentication header (AH) or IPv6 ESP header to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH and ESP extension headers can be used to provide authentication and confidentiality to OSPFv3.

To use the IPsec AH, you must enable the **ipv6 ospf authentication** command. To use the IPsec ESP header, you must enable the **ipv6 ospf encryption** command. The ESP header may be applied alone or in combination with the AH, and when ESP is used, both encryption and authentication are provided. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

Each interface has a secure socket state, which can be one of the following:

- NULL: Do not create a secure socket for the interface if authentication is configured for the area.
- DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition.
- GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec.
- UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec.
- CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED.
- UNCONFIGURED: Authentication is not configured on the interface.

OSPFv3 does not send or accept packets while in the DOWN state.

How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec

Configuring IPsec on OSPFv3

Once you have configured OSPFv3 and decided on your authentication, you must define the security policy on each of the devices within the group. The security policy consists of the combination of the key and the SPI. To define a security policy, you must define an SPI and a key.

You can configure an authentication or encryption policy either on an interface or for an OSPFv3 area. When you configure for an area, the security policy is applied to all of the interfaces in the area. For higher security, use a different policy on each interface.

You can configure authentication and encryption on virtual links.

Defining Authentication on an Interface

Before you begin

Before you configure IPsec on an interface, you must configure OSPFv3 on that interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode. **Note** You should configure the OSPFv3 authentication of the VLAN interface, instead of the physical interface. See the below example: `Device(config)# interface VLAN 60`

	Command or Action	Purpose

Step 4	Do one of the following:
	• **ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**}{ *key-encryption-type key*} | **null**
	• **ipv6 ospf authentication** {**null** | **ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] [*key*]}
	Example:
	`Device(config-if)# ospfv3 authentication md5 0 27576134094768132473302031209727`
	Example:
	Or
	`Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`
		Specifies the authentication type for an interface.

Defining Authentication in an OSPFv3 Area

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router ospf** *process-id* **Example:** `Device(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**area** *area-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* **Example:** `Device(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	Enables authentication in an OSPFv3 area.

Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Example: Defining Authentication on an Interface

The following example shows how to define authentication on Ethernet interface 0/0:

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

Example: Defining Authentication in an OSPFv3 Area

The following example shows how to define authentication on OSPFv3 area 0:

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

Additional References for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*
IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec	"*Configuring OSPF* " module in *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

Technical Assistance

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

Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec

CHAPTER 51

Policy-Based Routing

Policy-based routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed to which device next. You might enable policy-based routing if you want certain packets to be routed some way other than the obvious shortest path. Possible applications for policy-based routing are to provide equal access, protocol-sensitive routing, source-sensitive routing, routing based on interactive versus batch traffic, and routing based on dedicated links. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

To enable policy-based routing, you must identify which route map to use for policy-based routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met.

To enable policy-based routing on an interface, indicate which route map the device should use by using the **ip policy route-map** *map-tag* command in interface configuration mode

To define the route map to be used for policy-based routing, use the **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] global configuration command.

Only **set ip next-hop** command can be used under route-map configuration mode when you configure policy-based routing.

To define the criteria by which packets are examined to learn if they will be policy-based routed, use the **match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*] command in route map configuration mode. No match clause in the route map indicates all packets.

Note Mediatrace will show statistics of incorrect interfaces with policy-based routing (PBR) if the PBR does not interact with CEF.

Note Management implications: Since the policy based routing alters the conventional path (learnt through routing protocols) the traffic would have taken, the policies should be defined in a deterministic manner to keep the network manageable without impacting running services or applications. For example, the policy based routing can alter the path for the control traffic and affect protocols like OSPF, multicast, etc. Hence the policies need to be defined considering these aspects.

- Restrictions on the Policy-Based Routing, on page 940
- How to Configure Policy-Based Routing, on page 940

Restrictions on the Policy-Based Routing

- ACL and PBR are not supported together on the same SVI. Only one of the access-group (permit or deny access list) or IP policy route-map can be configured on the same SVI.
- IPv6 PBR is not supported.
- FRR is not supported with PBR.
- PBR is supported only on the SVI interfaces. It is not supported on Physical ports, EFPs, and EVCs.
- Single route-map entry is supported for each **ip policy route-map** command usage instances. Multiple route-map sequence entries for the same route-map are not supported (route-map with multiple sequence of route-map-entries).
- Only the access list is supported as match clause. Prefix list and other match clauses are not supported.
- Only one ACL is supported for route-map entry match statement.
- Only one match statement is supported for each route-map entry.
- Only **set ip next-hop** command is supported for the route-map entry. The **set ip next-hop recursive** command is not supported. Consequently, the next-hop which is going to be MPLS path is not supported. Other set commands including **set ip vrf**, **set ip precedence** etc. are not supported.
- PBR is applicable for ingress traffic only and is not applicable for locally generated packets.
- IPv6 traffic filter and IPv4 PBR are not supported together on the same interface.
- One ACL can be associated to only one SVI interface (either through "IPv4 Policy Route-map" or through "IPv4 Access group") on one device.
- We recommend a maximum of 50 ACE rules in one access-List for all access-lists being used for PBR (route-map).

How to Configure Policy-Based Routing

Configuring ACLs

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list extended** *access-list-tag* **Example:** `Router(config)# ip access-list extended ACL1`	Defines an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations.
Step 4	**permit ip** *source-addr source-wildcard* **any** **Example:** `Router(config-ext-nacl)# permit ip 192.168.3.0 0.0.0.255 any`	Set conditions in named IP access list that permit packets. **Note** The 'deny' rules of access-list are ignored when the access-list is used for PBR purposes in a route-map.
Step 5	**end** **Example:** `Router(config-ext-nacl)# end`	Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure a Route-Map

Configuring Route-Map

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]	Defines the conditions for redistributing routes from one routing protocol into another routing

	Command or Action	Purpose
	Example: `Router(config)# route-map PBR1 permit 10`	protocol or enables policy-based routing and enters route-map configuration mode.
Step 4	**match ip address** *access-list-tag* **Example:** `Router(config-route-map)# match ip address ACL1`	Define the criteria by which packets are examined to learn if they will be policy-based routed.
Step 5	**set ip next-hop** *ip-address* **Example:** `Router(config-route-map)# set ip next-hop 30.30.30.3`	Specifies where to output packets that pass a match clause of a route map for policy routing.
Step 6	**end** **Example:** `Router(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

What to do next

Configure the IP Policy association (on SVI)

Configuring the IP Policy association (on SVI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vlan 100`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 100.0.0.2 255.255.255.0`	Defines the IP address for the interface.
Step 5	**ip policy route-map** *route-map-tag* **Example:** `Router(config-if)# ip policy route-map PBR1`	Identifies a route map to use for policy routing on an interface..
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the PBR Configuration

To display the interfaces where PBR is enabled, use the show ip policy command as shown in the following example:

```
Router# show ip policy

Interface Route map
Vlan10 RMAP1
```

To display the route-map sequence configuration, use the show route-map command as shown in the following example:

```
Router# show route-map MAP1

route-map MAP1, permit, sequence 10
  Match clauses:
    ip address (access-lists): 100
  Set clauses:
    ip next-hop 192.168.40.1
  Policy routing matches: 0 packets, 0 bytes
```

Configuration Example for the Policy-Based Routing

```
Building configuration...

Current configuration : 13748 bytes
!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
!
interface GigabitEthernet0/8
 no ip address
 negotiation auto
```

```
 no qos-config scheduling-mode min-bw-guarantee
 service instance 70 ethernet
  encapsulation dot1q 70
  rewrite ingress tag pop 1 symmetric
  bridge-domain 70
 !
 !
 !
!
interface Vlan221
 ip address 192.168.221.1 255.255.255.0
 ip policy route-map MAP1
 ip ospf 100 area 0
!
interface Vlan222
 ip address 192.168.222.1 255.255.255.0
 ip policy route-map MAP2
 ip ospf 100 area 0
!
interface Vlan246
!
router ospf 500
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 500
 network 192.168.40.0 0.0.0.255 area 500
 network 192.168.50.0 0.0.0.255 area 500
 network 192.168.60.0 0.0.0.255 area 500
 network 192.168.70.0 0.0.0.255 area 500
!
router ospf 100
!
router ospf 5090
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.77.224.1
!
access-list 100 permit ip host 12.12.12.1 host 20.20.20.1
access-list 200 permit ip host 11.11.111.1 host 10.10.10.1
!
route-map MAP1 permit 10
 match ip address 100
 set ip next-hop 192.168.40.1
!
route-map MAP2 permit 10
 match ip address 200
 set ip next-hop 192.168.50.1
!
tftp-server flash:asr901-universalk9-mz.5jan_mcp_hsrp
!
control-plane
!
environment monitor
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
exception crashinfo buffersize 128
!
```

```
!
end
```

Additional References

Related Documents

Related Topic	Document Title
IP routing protocol-independent commands	Cisco IOS IP Routing: Protocol-Independent Command Reference

Technical Assistance

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

Feature Information for Policy-Based Routing

The following table provides release information about the feature or features described in this module. This table 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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 58: Feature Information for Policy-Based Routing

Feature Name	Releases	Feature Information
Policy-Based Routing	Cisco IOS Release 15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 52

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

GRE encapsulates a payload, that is, an inner packet that needs to be delivered to a destination network inside an outer IP packet. GRE tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. Other IP routers along the way do not parse the payload (the inner packet); they only parse the outer IP packet as they forward it towards the GRE tunnel endpoint. Upon reaching the tunnel endpoint, GRE encapsulation is removed and the payload is forwarded to it’s ultimate destination.

IPv6 over IPv4 GRE Tunnels

IPv6 traffic can be carried over IPv4 GRE tunnels using the standard GRE tunneling technique that is designed to provide the services to implement any standard point-to-point encapsulation scheme. As in IPv6 manually configured tunnels, GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol but, in this case, carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol.

Note In Cisco ASR 901 Series Routers, for the IPv6 traffic over GRE, IPv4 is used as transport protocol.

GRE Tunnel Keepalive

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

QoS Tunnel Marking for GRE Tunnels

The QoS Tunnel Marking for GRE Tunnels feature introduces the capability to define and control the quality of service (QoS) for outbound customer traffic on the IP node or router (both encapsulation and decapsulation) in a service provider network.

If the service policy is not associated with the GRE tunnel, the QoS information from original header is copied to the outer header of a GRE tunneled packet.

If the service policy is associated with the GRE tunnel, the QoS information in the outer IPv4 header of a GRE tunneled packet is set as per the configured service-policy and table-map rules. If table-map rules are not configured for some QoS values, the outer header uses the value 0 for QoS fields in the outer IPv4 header.

Restrictions

The following are NOT claimed to be supported, though the configuration is accepted silently.

- Termination of GRE with outer IPv6 header.
- Multiple GRE encapsulations and GRE terminations.
- GRE encapsulation followed by MPLS encapsulation.
- GRE encapsulation followed by MPLS label lookup.
- MPLS encapsulation followed by GRE encapsulation.
- GRE termination followed by MPLS label lookup.
- MPLS label lookup followed by GRE termination.
- Support of VRF (MPLS) over tunnels.
- Multicast GRE (MGRE).
- MTU configuration over L3 interfaces is defined with the additional tunnel header length. This is because of GRE tunnel using the L3 interface for reachability.
- Shaping and Policing support over GRE Tunnel Interface (logical interface).
- Load-sharing is supported only for a maximum of two GRE tunnels.
- GRE tunnels with same source and destination are not supported.
- GRE over MLPP/PPP is not supported.

- Both IPSec and GRE on the single node are not supported. That is, the following are not supported on the single ASR901 node
  - GRE encapsulation followed by IPsec encryption.
  - IPsec decryption followed by GRE encapsulation.

Note You should remove and reapply the policy-map associated to an interface after any dynamic change or modification to the table-map.

Configuring a GRE Tunnel

Perform this task to configure a GRE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface Tunnel 100`	Enters tunnel interface configuration mode. number is the number associated with the tunnel interface.
Step 4	**tunnel ttl** *hop-count* **Example:** `Router(config-if)# tunnel ttl 5`	(Optional) Configures the Time-to-Live (TTL) hop-count value for a tunnel interface. The default TTL value is 255. It can be changed using this command, which allows you to set the TTL value for the outer IP header of the GRE tunnel packets.
Step 5	**ipv4 address** *ipv4-address subnet-mask* **Example:** `Router(config-if)# ip address 1.1.1.2 255.255.255.252`	Specifies the IPv4 address and subnet mask for the interface.
Step 6	**tunnel source** *type source-ip-address* **Example:** `Router(config-if)# tunnel source 11.1.1.2`	Specifies the source of the tunnel interface.

	Command or Action	Purpose
Step 7	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 10.1.1.1`	Defines the tunnel destination.
Step 8	**keepalive** [*period* [**retries**]] **Example:** `Router(config-if)# keepalive 10 3`	(Optional) Defines the keepalive period (default is 10 seconds) and the number of times that the device continues to send keepalive packets without a response before bringing the interface down.

What to do next

Repeat the steps on a different router to complete the tunnel configuration.

Ensure that tunnel destination should be reachable from source. And tunnel src, tunnel destination on encapsulation and decapsulation should match as illustrated below.

Encapsulation

```
Tunnel src 11.1.1.2
Tunnel dest 10.1.1.1
```

Decapsulation

```
Tunnel src 10.1.1.1
Tunnel dest 11.1.1.2
```

Configuring a GRE Tunnel for IPv6

Perform this task to configure a GRE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding on the router.

	Command or Action	Purpose
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 5	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables Cisco Express Forwarding for IPv6.
Step 6	**interface tunnel** *number* **Example:** `Router(config)# interface Tunnel 100`	Enters tunnel interface configuration mode. number is the number associated with the tunnel interface.
Step 7	**tunnel ttl** *hop-count* **Example:** `Router(config-if)# tunnel ttl 5`	(Optional) Configures the Time-to-Live (TTL) hop-count value for a tunnel interface. The default TTL value is 255. It can be changed using this command, which allows you to set the TTL value for the outer IP header of the GRE tunnel packets.
Step 8	**ipv4 address** *ipv4-address subnet-mask* **Example:** `Router(config-if)# ip address 1.1.1.2 255.255.255.252`	Specifies the IPv4 address and subnet mask for the interface.
Step 9	**tunnel source** *type source-ip-address* **Example:** `Router(config-if)# tunnel source 11.1.1.2`	Specifies the source of the tunnel interface.
Step 10	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 10.1.1.1`	Defines the tunnel destination.
Step 11	**keepalive** [*period* [**retries**]] **Example:** `Router(config-if)# keepalive 10 3`	(Optional) Defines the keepalive period (default is 10 seconds) and the number of times that the device continues to send keepalive packets without a response before bringing the interface down.
Step 12	**ipv6 address** *ipv6-address subnet-mask* **Example:** `Router(config-if)# ipv6 address 35:35:35::1/64`	Specifies the IPv6 address and subnet mask for the interface.

	Command or Action	Purpose
Step 13	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Specifies IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

What to do next

Repeat the steps on a different router to complete the tunnel configuration.

Ensure that tunnel destination should be reachable from source. And tunnel src, tunnel destination on encapsulation and decapsulation should match as illustrated below. For IPv6 also, the tunnel source and destination (outer transport) should only be IPv4.

Encapsulation

```
Tunnel src 11.1.1.2
Tunnel dest 10.1.1.1
```

Decapsulation

```
Tunnel src 10.1.1.1
Tunnel dest 11.1.1.2
```

Configuring VRF Lite over GRE Tunnel

Configuring VRF-lite in Global Configuration Mode

Perform this task to configure VRF-lite in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition vpn_1`	Configures a virtual routing and forwarding (VRF) routing table instance and enter VRF configuration mode.
Step 4	**address-family ipv4 unicast** **Example:**	Specifies the IPv4 address family, and enters address family configuration mode.

	Command or Action	Purpose
	`Router(config-vrf)# address-family ipv4 unicast`	

Configuring VRF-lite for IPv6

Perform this task to configure VRF-lite for IPv6.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables Cisco Express Forwarding for IPv6.
Step 5	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition vpn_1`	Configures a virtual routing and forwarding (VRF) routing table instance and enter VRF configuration mode.
Step 6	**address-family ipv6 unicast** **Example:** `Router(config-vrf)# address-family ipv6 unicast`	Specifies the IPv6 address family, and enters address family configuration mode.

Configuring VRF Lite in SVI Configuration Mode

Perform this task to configure VRF Lite in SVI configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-number* **Example:** `Router(config)# interface vlan 17`	Enters SVI interface configuration mode. *vlan-number* is the number associated with the tunnel interface.
Step 4	**vrf forwarding** *name* **Example:** `Router(config-if)# vrf forwarding vpn_1`	Associate a VRF with a peer.

Configuring VRF Lite over GRE Tunnel

Perform this task to configure VRF lite over GRE tunnel. The core network should be under the same VRF as the tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface Tunnel 0`	Enters tunnel interface configuration mode. *number* is the number associated with the tunnel interface.
Step 4	**vrf forwarding** *name* **Example:** `Router(config-if)# vrf forwarding vpn_1`	Associate a VRF with a peer.
Step 5	**tunnel vrf** *name* **Example:** `Router(config-if)# tunnel vrf vpn_1`	Associates a VRF instance with a specific tunnel destination.

Adding Static Route to the Tunnel

Perform this task to add a static route to the GRE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip route vrf** *vpn-name ipv4-address subnet-mask* **tunnel** *number* **Example:** `Router(config)# ip route vrf vpn_1 19.19.19.1 255.255.255.0 tunnel 0`	Establishes static routes for a Virtual Private Network (VPN) routing and forwarding (VRF) instance. **Note** Ensure that VRF enabled prefixes are not present in the global routing table.

Configuring GRE QoS Table Map Support

To configure GRE QoS Table Map support, you need to configure the following:

- Ingress policy-map: It is used to associated to a GigabitEthernet interface as an in-bound policy.
- Table Map.
- Egress policy-map: It is used to associated to a GRE as an outbound policy.

Configuring Service-Policy

Procedure

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

	Command or Action	Purpose
Step 3	**class-map match-any***class-map-name* **Example:** `Router(config)# class-map match-any dscp_class`	Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode.
Step 4	**match dscp** *dscp-value* **Example:** `Router(config-cmap)# match dscp 38`	Identifies a specific quality of service (QoS) group value as a match criterion.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Enters global configuration mode.
Step 6	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy_dscp`	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
Step 7	**class** *class-name* **Example:** `Router(config-pmap)# class dscp_class`	Associates a map class with the policy-map.
Step 8	**set qos-group** *group-id* **Example:** `Router(config-pmap)# set qos-group 5`	Configures a quality of service (QoS) group identifier (ID) that can be used later to classify packets.
Step 9	**exit** **Example:** `Router(config-pmap)# exit`	Enters global configuration mode.
Step 10	**interface GigabitEthernet** *number* **Example:** `Router(config)# interface GigabitEthernet 0/1`	Enters gigabitethernet interface configuration mode. number is the number associated with the interface. Here the Marked Traffic is coming from the host.
Step 11	**service-policy input** *policy-map* **Example:** `Router(config-if)# service-policy input policy_dscp`	Attaches the policy map to a gigabitethernet interface as an inbound.

What to do next

Configure a Table-Map

Configuring a Table-Map

Perform this task to configure a table-map.

Before you begin

Before configuring table-map, ensure that there is an ingress policy, and then remark using the table-map.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**table-map** *table-map-name* **Example:** `Router(config)# table-map TABLE3`	Configures a mapping table for mapping and converting one packet-marking value to another. **Note** The Cisco ASR 901 router supports DSCP to QoS and QoS to DSCP. However, it is not supported directly from DSCP to DSCP and the same is also applicable for precedence values.
Step 4	**map from** *value* **to** *value* **Example:** `Router(config-tablemap)# map from 5 to 7`	Maps 'From' value to 'To' value. This step is remarking from qos-group (5) to dscp value (7).

What to do next

Create a policy-map to associate to the GRE tunnel.

Configuring a Policy-Map

Perform this task to configure a policy-map.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map POLICY3`	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
Step 4	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Associate a class-default with policy-map.
Step 5	**set dscp** *qos-group***table** *table-map-name* **Example:** `Router(config-pmap-c)# set dscp qos-group table TABLE3`	Marks a packet by setting the QoS group value in the type of service (ToS) byte. This step is associating the table-map to policy-map.

Associating Service Policy to the GRE Tunnel

Perform this task to associate a service policy to the GRE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface Tunnel 0`	Enters tunnel interface configuration mode. *number* is the number associated with the tunnel interface.
Step 4	**service-policy output** *name* **Example:** `Router(config-if)# service-policy output POLICY3`	Associate a policy map to GRE tunnel as an outbound service-policy. **Note** To verify the remarking matching counters, configure a policy-map in intermediate router and associate it to the ingress port.

Verifying the GRE Configuration

Use the show commands given in the following examples to verify the GRE configuration.

To display the contents of the tunnel interface, use the **show running-config** command.

```
Router# show running-config interface tunnel 0

Building configuration...

Current configuration : 160 bytes
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.252
 keepalive 10 3
 tunnel source 1.1.1.1
 tunnel destination 2.2.2.2
 service-policy output policy2
end
```

To display the usability status of interfaces configured for IP, use the **show ip interface** command.

```
Router# show ip interface brief | include Tunnel

Tunnel2               35.35.35.1      YES NVRAM  up                    up
Tunnel10              45.45.45.1      YES NVRAM  up                    up
```

To display the configuration of a tunnel interface, use the **show interface tunnel** command.

```
Router# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec), retries 3
  Tunnel linestate evaluation up
  Tunnel source 1.1.1.1, destination 2.2.2.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 01:13:28, output 00:00:08, output hang never
  Last clearing of "show interface" counters 01:13:48
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     15 packets input, 1416 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
     442 packets output, 21216 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
```

```
     0 output buffer failures, 0 output buffers swapped out
```

To display the contents of the gigabitethernet interface, use the **show running-config** command.

```
Router# show running-config interface gigabitEthernet 0/11

Building configuration...

Current configuration : 384 bytes
!
interface GigabitEthernet0/11
 no ip address
 negotiation auto
 no qos-config scheduling-mode min-bw-guarantee
 service-policy input policy1
 service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
  bridge-domain 101
 !
end
```

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command.

```
Router# show policy-map interface g0/11

 GigabitEthernet0/11

  Service-policy input: policy1

    Class-map: class1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match:  dscp af43 (38)
      QoS Set
        qos-group 5
          Packets marked 0
        No marking statistics available for this class

    Class-map: class_2 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match:  dscp af33 (30)
      QoS Set
        qos-group 3
          Packets marked 0
        No marking statistics available for this class

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

To display the configuration of a specified table map or all table maps, use the **show table-map** command.

```
Router# show table-map

 Table Map table_1
 from 5 to 7
 default copy

 Table Map new_table
 default copy

 Table Map table3
 from 0 to 7
 from 5 to 1
 default copy
```

Configuration Examples for GRE

Configuration Example for IPv4 GRE

```
Router# show running-configuration

Building configuration...

Current configuration : 3334 bytes
!
!
!
multilink bundle-name authenticated
!
table-map table_1
 map from  5 to 7
 default copy
table-map new_table
 default copy
!
l3-over-l2 flush buffers
asr901-storm-control-bpdu 1000
!
!
!
class-map match-all class_2
 match dscp af33
class-map match-all class1
 match dscp af43
!
policy-map invalid
 class class-default
  set dscp qos-group table table_1
policy-map policy1
 class class1
  set qos-group 5
 class class_2
  set qos-group 3
policy-map policy2
 class class-default
  set dscp qos-group table new_table
!
!
!
```

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.252
 keepalive 10 3
 tunnel source 1.1.1.1
 tunnel destination 2.2.2.2
 service-policy output policy2
!
interface GigabitEthernet0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 negotiation auto
 service instance 34 ethernet
  encapsulation dot1q 34
  rewrite ingress tag pop 1 symmetric
  bridge-domain 34
 !
!
!
interface GigabitEthernet0/11
 no ip address
 negotiation auto
 no qos-config scheduling-mode min-bw-guarantee
 service-policy input policy1
 service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
  bridge-domain 101
 !
!
interface FastEthernet0/0
 ip address 7.44.23.31 255.255.0.0
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan34
 ip address 1.1.1.1 255.255.255.252
!
interface Vlan100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan101
 ip address 172.16.1.1 255.255.255.0
!
ip default-gateway 7.44.0.1
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 2.2.2.0 255.255.255.252 1.1.1.2
```

```
ip route 172.16.2.0 255.255.255.0 Tunnel0
ip route 192.168.2.0 255.255.255.0 Tunnel0
!
!
!
!
control-plane
!
environment monitor
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
exception crashinfo buffersize 128
!
!
end
```

Configuration Example for IPv6 GRE

```
Router# show running-configuration

Building configuration...

Current configuration : 3398 bytes
!
! Last configuration change at 16:02:49 IST Wed Mar 4 2015
!
version 15.5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname Pura-2035
!
boot-start-marker
boot-end-marker
!
!
no logging console
!
no aaa new-model
clock timezone IST 5 30
ip cef
!
!
!
!
no ip domain lookup

ipv6 unicast-routing
ipv6 cef
!
!
mpls label protocol ldp
multilink bundle-name authenticated
l3-over-l2 flush buffers
asr901-storm-control-bpdu 1000
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
license udi pid A901-4C-F-D sn CAT1711U0TZ
license boot level AdvancedMetroIPAccess
!
!
lldp run
!
class-map match-any class_1
match dscp 6
class-map match-any class_2
match dscp 7
!
policy-map policy_2
class class_1
class class_2
!
!
!
!
interface Loopback35
ip address 35.1.1.1 255.255.255.255
ip ospf 1 area 0
!
interface Tunnel100
ip address 100.1.1.2 255.255.255.252
ipv6 address 35:35:35::2/64
keepalive 10 3
tunnel source 34.34.34.2
tunnel destination 34.34.34.1
!
interface GigabitEthernet0/0
no ip address
negotiation auto
service instance 34 ethernet
  encapsulation dot1q 34
  rewrite ingress tag pop 1 symmetric
  bridge-domain 34
!
!
interface GigabitEthernet0/1
no ip address
negotiation auto
!
interface GigabitEthernet0/2
no ip address
negotiation auto
!
interface GigabitEthernet0/3
no ip address
negotiation auto
!
interface GigabitEthernet0/4
no ip address
media-type auto-select
negotiation auto
!
interface GigabitEthernet0/5
no ip address
media-type auto-select
negotiation auto
!
interface GigabitEthernet0/6
no ip address
```

```
negotiation auto
!
interface GigabitEthernet0/7
no ip address
media-type auto-select
negotiation auto
!
interface GigabitEthernet0/8
no ip address
negotiation auto
qos-config scheduling-mode min-bw-guarantee
!
interface GigabitEthernet0/9
no ip address
negotiation auto
qos-config scheduling-mode min-bw-guarantee
!
interface GigabitEthernet0/10
no ip address
negotiation auto
no qos-config scheduling-mode min-bw-guarantee
service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
!
interface GigabitEthernet0/11
no ip address
negotiation auto
no qos-config scheduling-mode min-bw-guarantee
!
interface FastEthernet0/0
ip address 7.44.23.30 255.255.0.0
!
interface Vlan1
no ip address
!
interface Vlan34
ip address 34.34.34.2 255.255.255.252
ip ospf 1 area 0
!
interface Vlan100
no ip address
ipv6 address 2002::1/64
!
router ospf 1
router-id 35.1.1.1
!
ip default-gateway 7.44.0.1
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 route 2001::/64 Tunnel100
!
!
!
control-plane
!
environment monitor
!
```

```
line con 0
exec-timeout 0 0
line vty 0 4
login
!
exception crashinfo buffersize 128
!
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference

Standards and RFCs

Standard/RFC	Title
RFC2784	Generic Routing Encapsulation (GRE)

MIBs

MIB	MIBs Link
TUNNEL-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Generic Routing Encapsulation

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 59: Feature Information for Generic Routing Encapsulation

Feature Name	Releases	Feature Information
Generic Routing Encapsulation	15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 53

Call Home

The Call Home feature can deliver messages containing information on configuration, inventory, syslog, snapshot, environmental, and crash events. It provides these messages as either email-based or web-based messages. Multiple message formats are available, allowing for compatibility with pager services, standard email, or XML-based automated parsing applications. This feature can deliver messages to multiple recipients, referred to as Call Home destination profiles, each with configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco Smart Call Home server. The predefined profile defines both the email address and the HTTP(S) URL; the transport method configured in the profile determines whether the email address or the HTTP(S) URL is used.

Benefits of Using Call Home

The Call Home feature offers the following benefits:

- Multiple message-format options
    - Short Text—Suitable for pagers or printed reports.
    - Long Text—Full formatted message information suitable for human reading.
    - XML—Machine-readable format using XML. The XML format enables communication with Cisco Smart Call Home server for automatic processing.
- Multiple concurrent message destinations
- Multiple message categories including configuration, inventory, syslog, snapshot, environment, and crash events
- Filtering of messages by severity and pattern matching
- Scheduling of periodic message sending

Obtaining Smart Call Home Services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Call Home messages and provides background information and recommendations. For critical issues, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router
- Your email address
- Your Cisco.com username

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information is sent.

When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html.

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No identifying information is sent.

How to Configure Call Home

Prerequisites for Call Home

The Call Home feature provides email-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard email, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, email notification to a network operations center, XML delivery to a support website, and use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

Information to consider before you configure Call Home:

- Contact email address (required for full registration with Smart Call Home, optional if Call Home is enabled in anonymous mode), phone number (optional), and street address information (optional) should be configured so that the receiver can determine the origin of messages received.
- At least one destination profile (predefined or user-defined) must be configured. The destination profile you use depends on whether the receiving entity is a pager, an email address, or an automated service such as Cisco Smart Call Home.
    - If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.
    - Configuring the trustpoint CA is not required for HTTPS server connection since the trustpool feature enabled by default.
- Router must have IP connectivity to an email server or the destination HTTP(S) server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full SCH service.

Configuring Smart Call Home (Single Command)

To enable all Call Home basic configurations using a single command, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** *name* **port** *port-number* **Example:** `Router(config)# call-home reporting contact-email-addr email@company.com`	Enables all Call Home basic configurations using a single command. **Note** HTTP proxy option allows you to make use of your own proxy server to buffer and secure internet connections from your devices. **Note** After successfully enabling Call Home either in anonymous or full registration mode using the call-home reporting command, an inventory message is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent.

Enabling and Disabling Call Home

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**service call-home** **Example:** `Router(config)# service call-home`	Enables Call Home service on a device.

	Command or Action	Purpose
Step 3	**no service call-home** **Example:** `Router(config)# no service call-home`	Disables the Call Home feature.

Configuring Contact Information

Each router must include a contact email address (except if Call Home is enabled in anonymous mode). You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**contact-email-addr** *contact-email-addr* **Example:** `Router(cfg-call-home)# contact-email-addr username@example.com`	Designates your email address. Enter up to 200 characters in email address format with no spaces.
Step 4	**phone-number** + *phone-number* **Example:** `Router(cfg-call-home)# phone-number +1-800-555-4567`	(Optional) Assigns your phone number. **Note** The number must begin with a plus (+) prefix and may contain only dashes (-) and numbers. Enter up to 17 characters. If you include spaces, you must enclose your entry in quotes (“”).
Step 5	**street-address** *street-address* **Example:** `Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345“`	(Optional) Assigns your street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).

	Command or Action	Purpose
Step 6	**customer-id** *text* **Example:** `Router(cfg-call-home)# customer-id Customer1234`	(Optional) Identifies customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).
Step 7	**site-id** *text* **Example:** `Router(cfg-call-home)# site-id Site1ManhattanNY`	(Optional) Identifies customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).
Step 8	**contract-id** *text* **Example:** `Router(cfg-call-home)# contract-id Company1234`	(Optional) Identifies your contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).

Configuring Destination Profiles

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can create and define a new destination profile or copy and use the predefined destination profile. If you define a new destination profile, you must assign a profile name.

Note If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.

You can configure the following attributes for a destination profile:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive. You cannot use all as a profile name.
- Transport method—Transport mechanism, either email or HTTP (including HTTPS), for delivery of alerts.
  - For both the CiscoTAC-1 profile and user-defined destination profiles, email is the default, and you can enable either or both transport mechanisms. If you disable both methods, email is enabled.
  - For the predefined CiscoTAC-1 profile, you can enable either transport mechanism, but not both.
- Destination address—The actual address related to the transport method by which the alert should be sent.
- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined CiscoTAC-1 profile, only XML is allowed.
- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 bytes. The default is 3,145,728 bytes.

- Reporting data—You can choose which data to report for a profile. You can enable reporting of Smart Call Home data or Smart Licensing data, or both. Only one active profile is allowed to report Smart Licensing data at a time.
- Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.

Creating a New Destination Profile

To create and configure a new destination profile, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**profile** *name* **Example:** `Router(config-call-home)# profile profile1`	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	**destination transport-method** {**email** | **http**} **Example:** `Router(cfg-call-home-profile)# destination transport-method email`	(Optional) Enables the message transport method. The no option disables the method.
Step 5	**destination address** {**email** *email-address* | **http** *url*} **Example:** `Router(cfg-call-home-profile)# destination address email myaddress@example.com`	Configures the destination email address or URL to which Call Home messages are sent.
Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**} **Example:** `Router(cfg-call-home-profile)# destination preferred-msg-format xml`	(Optional) Configures a preferred message format. The default is XML.

	Command or Action	Purpose
Step 7	**destination message-size-limit** *bytes* **Example:** `Router(cfg-call-home-profile)# destination message-size-limit 3145728`	(Optional) Configures a maximum destination message size for the destination profile.
Step 8	**active** **Example:** `Router(cfg-call-home-profile)# active`	Enables the destination profile. By default, the profile is enabled when it is created.
Step 9	**reporting** {**all** | **smart-call-home-data** | **smart-licensing-data**} **Example:** `Router(cfg-call-home-profile)# reporting smart-call-home-data`	Configures the type of data to report for a profile. You can select either to report Smart Call Home data or Smart Licensing data. Selecting the **all** option reports data for both types of data.

Copying a Destination Profile

To create a new destination profile by copying an existing profile, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**copy profile** *source-profile target-profile* **Example:** `Router(cfg-call-home)# copy profile profile1 profile2`	Creates a new destination profile with the same configuration settings as the existing destination profile.

Setting Profiles to Anonymous Mode

To set an anonymous profile, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**profile** *name* **Example:** `Router(cfg-call-home) profile CiscoTAC-1`	Enables profile configuration mode.
Step 4	**anonymous-reporting-only** **Example:** `Router(cfg-call-home-profile)# anonymous-reporting-only`	Sets the profile to anonymous mode. **Note** By default, the profile sends a full report of all types of events subscribed in the profile. When anonymous-reporting-only is set, only crash, inventory, and test messages are sent.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts supported in all routers. Different types of Call Home alerts are grouped into different alert groups depending on their type. The following alert groups are available:

- Environmental
- Configuration
- Inventory
- Syslog
- Crash
- Snapshot

Note A Call Home alert is sent only to destination profiles that have subscribed to the alert group containing that Call Home alert. In addition, the alert group must be enabled.

Note As an alternative to subscribing to individual alert groups, you can subscribe to all alert groups by entering the subscribe-to-alert-group all command. However, entering this command causes a large number of syslog messages to generate. We recommend subscribing to alert groups individually, using appropriate severity levels and patterns when possible.

To subscribe a destination profile to one or more alert groups, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**} **Example:** `Router(cfg-call-home)# alert-group all`	Enables the specified alert group. Use the keyword all to enable all alert groups. By default, all alert groups are enabled.
Step 4	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters Call Home destination profile configuration submode for the specified destination profile.
Step 5	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *daily hh:mm* | **weekly** *daily hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00`	Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification, as described in the "Periodic Notification" section.
Step 6	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *daily hh:mm* | **weekly** *daily hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00`	Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification, as described in the "Periodic Notification" section.
Step 7	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** |	Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be

	Command or Action	Purpose
	major | **minor** | **warning** | **notification** | **normal** | **debugging**}] [**pattern** *string*] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major`	configured to filter messages based on severity, as described in the "Message Severity Threshold" section. You can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (""). You can specify up to five patterns for each destination profile.
Step 8	**subscribe-to-alert-group crash** **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group crash`	Subscribes to the Crash alert group in user profile. By default, the CiscoTAC-1 profile subscribes to the Crash alert group and cannot be unsubscribed.
Step 9	**subscribe-to-alert-group snapshot** [**periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *daily hh:mm* | **weekly** *day hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00`	Subscribes this destination profile to the Snapshot alert group. The Snapshot alert group can be configured for periodic notification, as described in the "Periodic Notification" section. By default, the Snapshot alert group has no command to run. You can add commands into the alert group, as described in the "Configuring Snapshot Command List" section. In doing so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.

Periodic Notification

When you subscribe a destination profile to the Configuration, Inventory, or Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The sending period can be one of the following:

- Daily—Specifies the time of day to send, using an hour:minute format hh:mm, with a 24-hour clock (for example, 14:30).
- Weekly—Specifies the day of the week and time of day in the format day hh:mm, where the day of the week is spelled out (for example, Monday).
- Monthly—Specifies the numeric date, from 1 to 31, and the time of day, in the format date hh:mm.
- Interval—Specifies the interval at which the periodic message is sent, from 1 to 60 minutes.
- Hourly—Specifies the minute of the hour at which the periodic message is sent, from 0 to 59 minutes.

Note Hourly and by interval periodic notifications are available for the Snapshot alert group only.

Message Severity Threshold

When you subscribe a destination profile to the Syslog alert group, you can set a threshold for the sending of alert group messages based on the level of severity of the message. Any message with a value lower than the destination profile specified threshold is not sent to the destination.

The severity threshold is configured using the keywords in the following table and ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). Other alert groups do not allow setting a threshold for severity.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 60: Severity and Syslog Level Mapping

Level	Keyword	Syslog Level	Description
9	catastrophic	—	Network-wide catastrophic failure.
8	disaster	—	Significant network impact.
7	fatal	Emergency (0)	System is unusable.
6	critical	Alert (1)	Critical conditions, immediate attention needed.
5	major	Critical (2)	Major conditions.
4	minor	Error (3)	Minor conditions.
3	warning	Warning (4)	Warning conditions.
2	notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	normal	Information (6)	Normal event signifying return to normal state.

Configuring Snapshot Command List

To configure the snapshot command list, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**alert-group-config snapshot** **Example:** `Router(cfg-call-home)# alert-group-config snapshot`	Enters snapshot configuration mode.
Step 4	**add-command** *command string* **Example:** `Router(cfg-call-home-snapshot)# add-command "show version"`	Adds the command to the Snapshot alert group. The no or default command will remove the corresponding command.

Configuring General email Options

To use the email message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) email server address. You can configure the from and reply-to email addresses, and you can specify up to four backup email servers.

Note the following guidelines when configuring general email options:

- Backup email servers can be defined by repeating the mail-server command using different priority numbers.
- The mail-server priority number parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.

	Command or Action	Purpose
Step 3	**mail-server** *name* **priority** *number* **Example:** `Router(cfg-call-home)# mail-server stmp.example.com priority 1`	Assigns an email server address and its relative priority among configured email servers.
Step 4	**sender from** *email-address* **Example:** `Router(cfg-call-home)# sender from username@example.com`	(Optional) Assigns the email address that appears in the from field in Call Home email messages. If no address is specified, the contact email address is used.
Step 5	**sender reply-to** *email-address* **Example:** `Router(cfg-call-home)# sender reply-to username@example.com`	(Optional) Assigns the email address that appears in the reply-to field in Call Home email messages.
Step 6	**source-interface** *interface-name* **Example:** `Router(cfg-call-home)# source-interface loopback1`	Assigns the source interface name to send call-home messages. **Note** For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.
Step 7	**source-ip-address** *ipv4/ipv6-address* **Example:** `Router(cfg-call-home)# source-ip-address 209.165.200.226`	Assigns source IP address to send call-home messages.
Step 8	**vrf** *vrf-name* **Example:** `Router(cfg-call-home)# vrf vpn1`	(Optional) Specifies the VRF instance to send call-home email messages. If no vrf is specified, the global routing table is used. **Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

Specifying Rate Limit for Sending Call Home Messages

To specify the rate limit for sending Call Home messages, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**rate-limit** *number* **Example:** `Router(cfg-call-home)# rate-limit 40`	Specifies a limit on the number of messages sent per minute.

Specifying HTTP Proxy Server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**http-proxy** *name* **port** *port-number* **Example:** `Router(cfg-call-home)# http-proxy 1.1.1.1 port 1`	Specifies the proxy server for the HTTP request.

Enabling AAA Authorization to Run IOS Commands for Call Home Messages

To enable AAA authorization to run IOS commands that enable the collection of output for a Call Home message, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**aaa-authorization** **Example:** `Router(cfg-call-home)# aaa-authorization`	Enables AAA authorization.
Step 4	**aaa-authorization** [**username** *username*] **Example:** `Router(cfg-call-home)# aaa-authorization username user`	Specifies the username for authorization.

Configuring Syslog Throttle

To enable or disable Call Home syslog message throttling and avoid sending repetitive Call Home syslog messages, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**syslog-throttling** **Example:** `Router(cfg-call-home)# syslog-throttling`	Enables or disables Call Home syslog message throttling and avoids sending repetitive Call Home syslog messages. The same syslog entry will only trigger call-home message after 24 hours. By default, syslog message throttling is enabled. **Note**

	Command or Action	Purpose
		Debug level syslogs like debug trace are not throttled.

Configuring Call Home Data Privacy

The data-privacy command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. Currently, show command output is not being scrubbed except for configuration messages in the show running-config all and show startup-config data.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 3	**data-privacy** {**level** { **normal** | **high**} | **host-name**} **Example:** `Router(cfg-call-home)# data-privacy level high`	Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal. **Note** Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.

Sending Call Home Communications Manually

Sending a Call Home Test Message Manually

You can use the call-home test command to send a user-defined Call Home test message.

To manually send a Call Home test message, perform the following step:

Procedure

	Command or Action	Purpose
Step 1	**call-home test** [*test-message*] **profile** *name* **Example:** `Router# call-home test profile profile1`	Sends a test message to the specified destination profile. The user-defined test message text is optional but must be enclosed in quotes (“”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Sending Call Home Alert Group Messages Manually

You can use the call-home send command to manually send a specific alert group message.

Note the following guidelines when manually sending a Call Home alert group message:

- Only the snapshot, crash, configuration, and inventory alert groups can be sent manually. Syslog alert groups cannot be sent manually.
- When you manually trigger a snapshot, configuration, or inventory alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile’s active status, subscription status, or severity setting.
- When you manually trigger a snapshot, configuration, or inventory alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.
- You can trigger only one alert-group at a time for a given profile.

To manually trigger Call Home alert group messages, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**call-home send alert-group snapshot** [**profile** *name*] **Example:** `Router# call-home send alert-group snapshot profile profile1`	Sends a snapshot alert group message to one destination profile if specified or to all subscribed destination profiles.
Step 2	**call-home send alert-group crash** [**profile** *name*] **Example:** `Router# call-home send alert-group crash profile profile1`	Sends a crash alert group message to one destination profile if specified or to all subscribed destination profiles.
Step 3	**call-home send alert-group configuration** [**profile** *name*] **Example:**	Sends a configuration alert group message to one destination profile if specified or to all subscribed destination profiles.

	Command or Action	Purpose
	`Router# call-home send alert-group configuration profile profile1`	
Step 4	**call-home send alert-group inventory** [**profile** *name*] **Example:** `Router# call-home send alert-group inventory profile profile1`	Sends an inventory alert group message to one destination profile if specified or to all subscribed destination profiles.

Submitting Call Home Analysis and Report Requests

You can use the call-home request command to submit information about your system to Cisco to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note the following guidelines when manually sending Call Home analysis and report requests:

- If a profile name is specified, the request is sent to the profile. If no profile is specified, the request is sent to the CiscoTAC-1 profile. The recipient profile does not need to be enabled for the call-home request.
- When requesting "registration-info", the profile must have URL destination configured. Call home needs to talk with Smart Call Home server to get those information, then display them on device. So the URL destination pointing to Smart Call Home server or Transport Gateway should be configured in the profile already.
- The ccoid user-id is the registered identifier of the Smart Call Home user. In "registration-info" case, if the user-id is not specified, the command only gets device's registration status, otherwise it will get more detailed information about the device from Smart Call Home server, like entitlement and contract information. In other case, if the user-id is specified, the response is sent to the email address of the registered user. If no user-id is specified, the response is sent to the contact email address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:
  - config-sanity—Information on best practices as related to the current running configuration.
  - bugs-list—Known bugs in the running version and in the currently applied features.
  - command-reference—Reference links to all commands in the running configuration.
  - product-advisory—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.
  - registration-info—Device status information from Smart Call Home server. It may include device registration status, contract information, contact information and last message update time, etc.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**call-home request output-analysis** *show-command* [**profile** *name*] [**ccoid** *user-id*] **Example:** `Router# call-home request output-analysis "show diag" profile TG`	Sends the output of the specified show command for analysis. The show command must be contained in quotes ("").
Step 2	**call-home request** {**config-sanity** | **bugs-list** | **registration-info** |**command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*] **Example:** `Router# call-home request config-sanity profile TG`	Sends the output of a predetermined set of commands such as the show running-config all , show version or show module commands, for analysis. In addition, the call home request product-advisory subcommand includes all inventory alert group commands. The keyword specified after request specifies the type of report requested.

Manually Sending Command Output Message for One Command or a Command List

You can use the call-home send command to execute an IOS command or a list of IOS commands and send the command output through HTTP or email protocol.

Note the following guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes ("").
- If the email option is selected using the "email" keyword and an email address is specified, the command output is sent to that address.
- If neither the email nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the "email" nor the "http" keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the email.
- If the HTTP option is specified and neither URL nor profile is specified, the CiscoTAC-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. The user must specify either the destination email address or an SR number but they can also specify both.

To execute a command and send the command output, perform the following step:

Procedure

	Command or Action	Purpose

Step 1	**call-home send** {*cli command* | *cli list*} [[**email** [*email -address* | **profile***profile-name*] | [**http** [*url* | **profile***profile-name*] **destination-email-address** *forward-email-address*]]**msg-format** {**long-text** | **xml**} [**tac-service-request** *SR#*]
	Example:
	`Router# call-home send “show version;show running-config;show inventory” email support@example.com msg-format xml`
	`!The following example shows how to send the output of a command to a user-specified email address:`
	`Router# call-home send “show diag” email support@example.com`
	`!The following example shows the command output sent in long-text format to attach@cisco.com, with the SR number specified:`
	`Router# call-home send “show version; show run” tac-service-request 123456`
	`!The following example shows the command output sent in XML message format to callhome@cisco.com:`
	`Router# call-home send “show version; show run” email callhome@cisco.com msg-format xml`
		Executes the CLI or CLI list and sends output via email or HTTP.

Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customers networks.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that the following conditions are met:

- You must assign one or more DSs to the device.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files.

Diagnostic Signatures Overview

Diagnostic signatures (DS) for the Call Home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DSs provide the ability to define more types of events and trigger types than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic Signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify their integrity, reliability, and security.

The structure of a DS file can be one of the following formats:

- Metadata-based simple signature that specifies the event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI. The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats above.

The following basic information is contained in a DS file:

- ID (unique number): unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription): unique description of the DS file that can be used in lists for selection.
- Description: long description about the signature.
- Revision: version number, which increments when the DS content is updated.
- Event & Action: defines the event to be detected and the action to be performed after the event happens.

Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download. Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Workflow

The diagnostic signature feature is enabled by default in Cisco software. The following is the workflow for using diagnostic signatures:

1. Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
2. The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded. On the Cisco ASR 901 Series Routers, the DS file is stored in the flash:/directory.
4. The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.
5. The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature Events and Actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed after the event happens, such as collecting s how command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature Event Detection

Event detection in a DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, and call home are the supported event types, where “immediate” indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- The Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two ore more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if syslog or IPSLA are triggered.

Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an event occurs. The action type indicates the kind of action that will be initiated in response to a certain event. Variables are elements within a DS that are used to customize the files.

DS actions are categorized into the following four types:

- call-home
- command
- emailto
- script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses “diagnostic-signature” as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

Diagnostic Signature Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the environment variable-name variable-value command in call-home diagnostic-signature configuration mode. Use the show call-home diagnostic-signature command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the call-home diagnostic-signature install ds-id command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring the Call Home Service for Diagnostic Signatures

Configure the Call Home Service feature to set attributes such as the contact email address where notifications related with diagnostic signatures (DS) are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and we recommend using it. If used, you only need to change the destination transport-method to the http setting.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**service call-home** **Example:** `Router(config)# service call-home`	Enables Call Home service on a device.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 4	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)# contact-email-addr userid@example.com`	(Optional) Assigns an email address to be used for Call Home customer contact.
Step 5	**mail-server** {*ipv4-address* | *name*} **priority** *number* **Example:** `Router(cfg-call-home)# mail-server 10.1.1.1 priority 4`	(Optional) Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call Home. This command is only used when sending email is part of the actions defined in any DS.
Step 6	**profile** *profile-name* **Example:** `Router(cfg-call-home)# profile user1`	Configures a destination profile for Call Home and enters call-home profile configuration mode.

	Command or Action	Purpose
Step 7	**destination transport-method** {**email** | **http**} **Example:** `Router(cfg-call-home-profile)# destination transport-method http`	Specifies a transport method for a destination profile in the Call Home. **Note** To configure diagnostic signatures, you must use the http option.
Step 8	**destination transport-method** {**email** *address* | **http** *url*} **Example:** `Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Configures the address type and location to which call-home messages are sent. **Note** To configure diagnostic signatures, you must use the http option.
Step 9	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **month** *day hh:mm* | **weekly** *day hh:mm*}] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Configures a destination profile to send messages for the Inventory alert group for Call Home. **Note** This command is used only for the periodic downloading of DS files.

What to do next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configuring Diagnostic Signatures

Configure the Call Home feature to set attributes for the Call Home profile. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

Procedure

	Command or Action	Purpose
Step 1	**call-home** **Example:** `Router(config)# call-home`	Enters the Call Home configuration submode.
Step 2	**diagnostic-signature** **Example:** `Router(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 3	**profile** *ds-profile-name* **Example:**	Specifies the destination profile on a device that DS uses.

	Command or Action	Purpose
	`Router(cfg-call-home-diag-sign)# profile user1`	
Step 4	**environment** *ds _ env-var-name ds-env-var-value* **Example:** `Router(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.
Step 5	**end** **Example:** `Router(cfg-call-home-diag-sign)# end`	Exits call-home diagnostic signature mode and returns to privileged EXEC mode.
Step 6	**call-home diagnostic-signature** {{**deinstall** | **download** } {*ds-id* | **all** } | **install** *ds-id*} **Example:** `Router# call-home diagnostic-signature download 6030`	Downloads, installs, and uninstalls diagnostic signature files on a device.

Displaying Call Home Configuration Information

You can use variations of the **`show call-home`** command to display Call Home configuration information.

- **`show call-home`**
- **`show call-home detail`**
- **`show call-home alert-group`**
- **`show call-home mail-server status`**
- **`show call-home profile`**
- **`show call-home statistics`**
- **`show call-home diagnostic-signature`**
- **`show call-home diagnostic-signature statistics`**
- **`show call-home smart-licensing`**
- **`show call-home smart-licensing statistics`**

Examples

The following examples show sample output when using different options of the **show call-home** command.

Call Home Information in Summary

```
Router# show call-home
```

```
Current call home settings:
    call home feature : enable
    call home message's from address: username@cisco.com
    call home message's reply-to address: username@cisco.com

    vrf for call-home messages: Not yet set up

    contact person's email address: user@cisco.com

    contact person's phone number: +1-800-555-4567
    street address: 1234
    customer ID: 1234
    contract ID: cisco1234
    site ID: manhattan

    source ip address: 209.165.200.226
    source interface: Not yet set up
    Mail-server[1]: Address: stmp.example.com Priority: 1
    Mail-server[2]: Address: 10.1.1.1 Priority: 4
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: profile1 (status: ACTIVE)

    Smart licensing messages: disabled

    aaa-authorization: enable
    aaa-authorization username: usr1

    data-privacy: normal and hostname
    syslog throttling: enable

    Rate-limit: 40 message(s) per minute

    Snapshot command[0]: show version

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- ------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: CiscoTAC-1
    Profile Name: profile1
    Profile Name: profile2
```

Call Home Information in Detail

```
Router# show call-home detail

Current call home settings:
    call home feature : enable
    call home message's from address: username@cisco.com
    call home message's reply-to address: username@cisco.com

    vrf for call-home messages: Not yet set up

    contact person's email address: user@cisco.com
```

```
    contact person's phone number: +1-800-555-4567
    street address: 1234
    customer ID: 1234
    contract ID: cisco1234
    site ID: manhattan

    source ip address: 209.165.200.226
    source interface: Not yet set up
    Mail-server[1]: Address: stmp.example.com Priority: 1
    Mail-server[2]: Address: 10.1.1.1 Priority: 4
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: profile1 (status: ACTIVE)

    Smart licensing messages: disabled

    aaa-authorization: enable
    aaa-authorization username: usr1

    data-privacy: normal and hostname
    syslog throttling: enable

    Rate-limit: 40 message(s) per minute

    Snapshot command[0]: show version

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCESe
rvice

    Periodic configuration info message is scheduled every 27 day of the month a
t 11:53

    Periodic inventory info message is scheduled every 27 day of the month at 11

38

   Alert-group               Severity
   ------------------------  ------------
   crash                     debug
   environment               minor
   inventory                 normal
```

```
   Syslog-Pattern            Severity
   ------------------------  ------------
   .*                        major

rofile Name: profile1
   Profile status: ACTIVE
   Profile mode: Full Reporting
   Reporting Data: Smart Call Home
   Preferred Message Format: xml
   Message Size Limit: 3145700 Bytes
   Transport Method: email and http
   Email address(es): addrss@cisco.com
   HTTP  address(es): Not yet set up

   Periodic configuration info message is scheduled daily at 08:12

   Periodic inventory info message is scheduled every 1 day of the month at 12:
0

   Periodic snapshot info message is scheduled daily at 12:00

   Alert-group               Severity
   ------------------------  ------------
   crash                     debug
   inventory                 normal

   Syslog-Pattern            Severity
   ------------------------  ------------
   .*                        major

rofile Name: profile2
   Profile status: ACTIVE
   Profile mode: Anonymous Reporting Only
   Reporting Data: Smart Call Home
   Preferred Message Format: xml
   Message Size Limit: 3145700 Bytes
   Transport Method: email
   Email address(es): addrss@cisco.com
   HTTP  address(es): Not yet set up

   Alert-group               Severity
```

Available Call Home Alert Groups

```
Router# show call-home alert-group

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
```

Email Server Status Information

```
Router# show call-home mail-server status
```

Information for All Destination Profiles

```
Router# show call-home profile all

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCESe
rvice

    Periodic configuration info message is scheduled every 27 day of the month a
t 11:53

    Periodic inventory info message is scheduled every 27 day of the month at 11
:38

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Profile Name: profile1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145700 Bytes
    Transport Method: email
    Email address(es): addrss@cisco.com
    HTTP  address(es): Not yet set up

    Periodic configuration info message is scheduled daily at 08:12

    Periodic inventory info message is scheduled every 1 day of the month at 12:
00

    Periodic snapshot info message is scheduled daily at 12:00

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Profile Name: profile2
    Profile status: ACTIVE
    Profile mode: Anonymous Reporting Only
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145700 Bytes
    Transport Method: email
    Email address(es): addrss@cisco.com
```

```
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    N/A                       N/A

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
```

Information for a User-Defined Destination Profile

```
Router# show call-home profile profile1

Profile Name: profile1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145700 Bytes
    Transport Method: email and http
    Email address(es): addrss@cisco.com
    HTTP  address(es): Not yet set up

    Periodic configuration info message is scheduled daily at 08:12

    Periodic inventory info message is scheduled every 1 day of the month at 12:
00

    Periodic snapshot info message is scheduled daily at 12:00

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

Call Home Statistics

```
Router# show call-home statistics

Message Types    Total                Email                HTTP
-------------    -------------------- -------------------- ------------------
Total Success    0                    0                    0
    Config       0                    0                    0
    Crash        0                    0                    0
    Environment  0                    0                    0
    Inventory    0                    0                    0
    Snapshot     0                    0                    0
    SysLog       0                    0                    0
    Test         0                    0                    0
    Request      0                    0                    0
    Send-CLI     0                    0                    0
    SCH          0                    0                    0

Total In-Queue   0                    0                    0
    Config       0                    0                    0
    Crash        0                    0                    0
```

```
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
    SCH         0                    0                    0

Total Failed    2                    2                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     1                    1                    0
    Send-CLI    1                    1                    0
    SCH         0                    0                    0

Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
    SCH         0                    0                    0

Last call-home message sent time: n/a
```

Call Home Diagnostic Signature

```
Router# show call-home diagnostic-signature

Current diagnostic-signature settings:
 Diagnostic-signature: enabled
 Profile: profile1 (status: ACTIVE)
 Environment variable:
           ds_env1: evrval

Downloaded DSes:
                                                              Last Update
DS ID    DS Name                         Revision Status     (GMT+00:00)
-------- ------------------------------- -------- ---------- -------------------
6030     ActCH                           1.0      registered 2014-12-19 15:08:13
```

Call Home Diagnostic Signature Statistics

```
Router# show call-home diagnostic-signature statistics

                                          Triggered/     Average Run  Max Run
DS ID     DS Name                         Max/Deinstall  Time(sec)    Time(sec)
--------  ------------------------------- -------------  -----------  ---------
6030      ActCH                           0/0/N          0.000        0.000
```

Call Home Licensing Smart-Licensing

```
Router# show call-home smart-licensing

Current smart-licensing settings:
 Smart-licensing: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
```

Call Home Diagnostic Smart-Licensing Statistics

```
Router# show call-home smart-licensing statistics

Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.

Msg Subtype      Success Failed Inqueue Dropped Last-sent (GMT+08:00)
----------------------------------------------------------------------
REGISTRATION     33      0      0       0       2014-03-12 10:08:08
ACKNOWLEDGEMENT  1       0      0       0       2014-03-12 10:08:13
ENTITLEMENT      1       0      0       0       2014-03-12 10:08:21
```

Default Settings

The following table lists the default Call Home settings.

Parameters	Default
Call Home feature status	Disabled
User-defined profile status	Active
Predefined CiscoTAC-1 profile status	Inactive
Transport method	email
Message format type	XML
Alert group status	Enabled
Call Home message severity threshold	Debug
Message rate limit for messages per minute	20
AAA authorization	Disabled
Call Home syslog message throttling	Enabled
Data privacy level	Normal

Alert Group Trigger Events and Commands

Call Home trigger events are grouped into alert groups, with each alert group assigned commands to execute when an event occurs. The command output is included in the transmitted message. The following lists the trigger events included in each alert group, including the severity level of each event and the executed commands for the alert group.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Crash	SYSTEM_CRASH	—	—	Events related to system crash. Commands executed: • show version • show logging • show region • show stack
—	TRACEBACK	—	—	Detects software traceback events. Commands executed: • show version • show logging • show region • show stack
Configuration	—	—	—	User-generated request for configuration or configuration change event. Commands executed: • show inventory • show running-config all • show startup-config • show version • show platform diag

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Inventory	—	—	—	User-generated request for inventory event. Commands executed: • show version • show inventory oid • show diag • show interfaces • show process cpu sorted • show process cpu history • show buffers • show memory statistics • show cdp neighbors • show ip arp • show ip route • show data-corruption • show file systems
Syslog	—	Syslog	—	User-generated Syslog event. Commands executed: • show logging • show inventory
Environment	—	—	—	Events related to power, fan, and environment sensing elements such as temperature alarms. Commands executed: • show logging • show inventory • show environment

Message Contents

The following tables display the content formats of alert group messages:

Table 61: Format for a Short Text Message

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to a system message

Table 62: Common Fields for All Long Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML only)
Time stamp	Date and time stamp of event in ISO time notation: YYYY-MM-DD HH:MM:SS GMT+HH:MM	CallHome/EventTime
Message name	Name of message.	For short text message only
Message type	Specifically "Call Home".	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Specifically "reactive". Optional because default is "reactive".	For long-text message only
Severity level	Severity level of message	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only
Device ID	Unique device identifier (UDI) for end device generating message. This field should be empty if the message is nonspecific to a fabric switch. The format is type @ Sid @ seria l. • type is the product model number from backplane IDPROM. • @ is a separator character. • Sid is C, identifying the serial ID as a chassis serial number. • serial is the number identified by the Sid field. Example: CISCO3845@C@12345678	CallHome/CustomerData/ContractData/DeviceId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML only)
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/ContractId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ContractData/SiteId
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. The format is type @ Sid @ seria l.	For long text message only
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the host name of the device.	CallHome/CustomerData/SystemInfo/NameName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/SystemInfo/Contact
Contact email	email address of person identified as contact for this unit.	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/SystemInfo/ ContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	Model name of the router. This is the "specific model as part of a product family name.	CallHome/Device/Cisco_Chassis/Model
Serial number	Chassis serial number of the unit.	CallHome/Device/Cisco_Chassis/SerialNumber
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name="sysObjectID"
System description	System description for the managed element.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name="sysDescr"

Table 63: Inserted Fields Specific to a Particular Alert Group Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML only)
Command output name	Exact name of the issued command.	/aml/Attachments/Attachment/Name
Attachment type	Attachment type. Usually “inline”.	/aml/Attachments/Attachment@type
MIME type	Normally “text” or “plain” or encoding type.	/aml/Attachments/Attachment/Data@encoding
Command output text	Output of command automatically executed.	/mml/attachments/attachment/atdata

Sample Syslog Alert Notification in XML Format

Sample Syslog alert notification in XML format.


```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path> <aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>

<aml-session:MessageId>M8:9S1NMSF22DW:51AEAC68</aml-session:MessageId> </aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2013-06-05 03:11:36 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CSR1000v</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G9:9S1NMSF22DW:51AEAC68</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2013-06-05 03:11:36 GMT+00:00</ch:EventTime> <ch:MessageDescription>
*Jun 5 03:11:36.041: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event> <ch:Type>syslog</ch:Type> <ch:SubType></ch:SubType> <ch:Brand>Cisco
Systems</ch:Brand>
<ch:Series>CSR1000v Cloud Services Router</ch:Series> </ch:Event> <ch:CustomerData>
<ch:UserData>
```

```
<ch:Email>weijuhua@cisco.com</ch:Email>
</ch:UserData>
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope"> <soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path> <aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>

<aml-session:MessageId>M8:9S1NMSF22DW:51AEAC68</aml-session:MessageId> </aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block"> <aml-block:Header>

<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2013-06-05 03:11:36 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CSR1000v</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G9:9S1NMSF22DW:51AEAC68</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2013-06-05 03:11:36 GMT+00:00</ch:EventTime>
<ch:MessageDescription>
*Jun 5 03:11:36.041: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event> <ch:Type>syslog</ch:Type> <ch:SubType></ch:SubType> <ch:Brand>Cisco
Systems</ch:Brand>
<ch:Series>CSR1000v Cloud Services Router</ch:Series> </ch:Event> <ch:CustomerData>
<ch:UserData>
<ch:Email>weijuhua@cisco.com</ch:Email>
</ch:UserData>
```


Configuration Example for Call Home

```
Router#show running-config
Building configuration...

Current configuration : 3007 bytes
!
! Last configuration change at 16:03:42 UTC Fri Dec 19 2014
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
!
hostname Router
!
boot-start-marker
```

```
boot-end-marker
!
!
!
no aaa new-model
call-home
 contact-email-addr username@cisco.com
 contract-id "cisco1234"
 customer-id "1234"
 mail-server stmp.example.com priority 1
 phone-number "+1-800-555-4567"
 rate-limit 40
 sender from username@cisco.com
 sender reply-to username@cisco.com
 site-id "manhattan"
 source-ip-address "209.165.200.226"
 street-address "1234"
 aaa-authorization username "usr1"
 aaa-authorization
 alert-group-config snapshot
  add-command "show version"
 data-privacy hostname
 profile "profile1"
  destination message-size-limit 3145700
  destination address email addrss@cisco.com
  subscribe-to-alert-group crash
  subscribe-to-alert-group syslog severity major pattern .*
  subscribe-to-alert-group configuration periodic daily 8:12
  subscribe-to-alert-group inventory periodic monthly 1 12:00
  subscribe-to-alert-group snapshot periodic daily 12:00

ip cef
!
!
!
!

no ipv6 cef
!
!
!
end

Router#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference

Standards and RFCs

Standard/RFC	Title
None	

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Call Home

The following table lists the features in this module and provides links to specific configuration information.

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 following table 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 64: Feature Information for Call Home

Feature Name	Releases	Feature Information
Call Home	15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 54

PTP Debugging over GRE Tunnel

The Precision Time Protocol (PTP) debugging over GRE tunnel feature enables the transport of PTP debugging information and PTP packets originated from this device through a GRE tunnel.

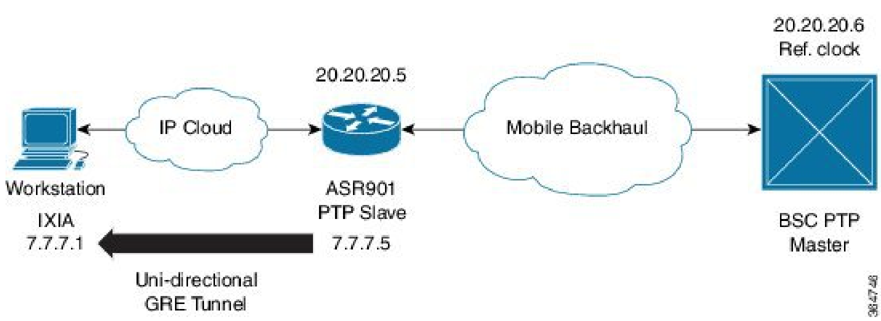
Information About PTP Debugging over GRE Tunnel

PTP debugging over GRE tunnel feature encapsulates the debugging dumps into the IP/UDP packets. The packets are transferred from the PTP slave device to a remote site device or IXIA through a GRE tunnel. The PTP packets received on the remote site are captured in a packet capture (PCAP) file, which is then used for analysis.

The following figure shows the sample Unidirectional tunnel with slave device topology.

Note This feature should be used only for debugging purposes and in a maintenance window.

Figure 57: Topology: Unidirectional Tunnel with Slave Device



Prerequisites

- Identify a remote site node, which is reachable through an IP path.
- Ensure that the GRE tunnel configured on the PTP slave device is not carrying any data traffic at the time of PTP debugging.
- Ensure that the tunnel configuration is not changed during PTP debugging.
- Ensure that the PTP debugging dumps are enabled.

Restrictions

- The PTP debugging over GRE tunnel feature is supported only for debugging.
- Only Unidirectional GRE tunnel is supported.
- This feature does *not* support the capture of PTP packets received from the peer on this device. It only supports the capture of PTP packets generated by this device.
- This feature does *not* support the changes in tunnel configuration during execution.

Guidelines

- Unidirectional GRE tunnel should be set up manually by the user from the PTP client node to the remote site node or IXIA where the packets are captured.
- Manual configuration of GRE tunnel is required by the user.
- The PTP packets are captured only for a 30 minutes duration in packet capture (PCAP) file. The debugging is disabled after 30 minutes.
- After the successful capture of PTP packets, tunnel configuration must be manually removed from the slave device.

Configuring GRE Tunnel on Slave Device

Perform this task to configure GRE tunnel on the slave device.

Note This feature configures a unidirectional GRE tunnel. The other end of the tunnel is not configured with any GRE tunnel configuration; however, that other end must be reachable through a pure IP path (no MPLS).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface Tunnel 10`	Enters tunnel interface configuration mode. number is the number associated with the tunnel interface.
Step 4	**ipv4 address** *ipv4-address subnet-mask* **Example:** `Router(config-if)# ip address 45.45.45.1 255.255.255.0`	Specifies the IPv4 address and subnet mask for the interface.
Step 5	**tunnel source** *type source-ip-address* **Example:** `Router(config-if)# tunnel source 7.7.7.5`	Specifies the source of the tunnel interface.
Step 6	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 7.7.7.10`	Defines the tunnel destination.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuring PTP Debugging over GRE Tunnel

Perform the following steps to configure PTP debugging over GRE tunnel.

Procedure

Step 1 Enable PTP debugging dumps on the ASR901 PTP slave device using BCM shell commands. (Contact Cisco TAC to enable these commands.)

Step 2 Enable PTP debugging over GRE tunnel feature using the **debug platform ptp interface tunnel** command.

Step 3 Allow the packet capture to run for 30 minutes. After 30 minutes, disable the feature. (You can disable the PTP debugging over GRE tunnel feature using the **no debug platform ptp interface tunnel** command.)

Note
Generic debug commands like **debug all** and **undebug all** do not have any effect on this feature. You can only use the **debug platform ptp interface tunnel** command to enable the PTP debugging over GRE tunnel feature.

CHAPTER 55

Overview

Smart Licensing is the next generation enterprise license model for all Cisco software products. It simplifies the Cisco software experience and helps you to understand how Cisco software is used across your network.

Information About Smart Licensing

Smart Licensing is software based licensing end-to-end platform that consists of several tools and processes to authorize customers the usage and reporting of the Cisco products. The Smart Licensing feature is aimed at giving users an experience of a single, standardized licensing solution for all Cisco products. The users are not required to install licenses on the devices.

The feature has the capability to capture the customers order and communicates with Cisco Cloud License Service through Smart Call Home transport media to complete the products registration and authorization on desired performance and technology level.

The usage information from all products owned by a customer is kept in a single central database and used by Cisco for usage based pre/post-paid billing. The customers have the visibility into their current software usage across their entire network at any given time.

Benefits

- Seamless software experience encompassing purchasing, licensing management, reporting, and reconciliation/ renewal/ billing.
- Reduce cycle time with activation and registration that are automatic, instead of manual.
- Obtain visibility of software consumption (what's purchased and what's deployed) across your network.

- New streamlined way of viewing and managing software licenses. Make changes within minutes, instead of days or weeks.
- New cloud-based solution architecture and tools, in line with where the industry is headed.
- Eliminates the need for return materials authorization (RMA) or re-hosting action.

Supported Software Models and PIDs

The Smart Licensing platform supports the following flexible software consumption models:

- Own Up-Front (perpetual)
- Upgrade and Support over Time
- Subscription
- Utility (pay as you go)

Supported PIDs

The following PIDs are supported with Smart Licensing.

Chassis PID	License Feature	License PID
A901-12C-FT-D A901-12C-F-D	IPBase AdvancedMetroIPAccess 1588BC	SL-A901-B SL-A901-A SL-A901-T
A901-4C-FT-D A901-4C-F-D	IPBase AdvancedMetroIPAccess 1588BC Gige4CuUpgrade Gige4SfpUpgrade	SL-A901-B SL-A901-A SL-A901-T FLS-A901-4T FLS-A901-4S
A901-6CZ-FT-D A901-6CZ-F-D A901-6CZ-FT-A A901-6CZ-F-A	IPBase AdvancedMetroIPAccess 1588BC 10gigUpgrade Gige4portflexi	SL-A901-B SL-A901-A SL-A901-T FLS-A901-2Z FLS-A901-4
A901S-4SG-F-D A901S-3SG-F-D A901S-2SG-F-D A901S-2SG-F-AH A901S-3SG-F-AH	IPBase AdvancedMetroIPAccess	SL-A901-B SL-A901-A

Chassis PID	License Feature	License PID
A901-6CZ-FS-D A901-6CZ-FS-A	IPBase AdvancedMetroIPAccess 1588BC Ipsecnatpat	SL-A901-B SL-A901-A SL-A901-T FLS-A901-I

How to Configure Cisco Smart Licensing

Enabling Smart Licensing

This procedure enables Smart Licensing on the device.

Before you begin

- Ensure that Smart Call Home feature is enabled before using Smart Licensing.

  Review the sample configuration of Smart Call-Home feature provided in the Example: Smart Call Home, on page 1026 section.
- Call-home uses HTTPS to transport the licensing messages to Cisco back end license cloud.
- After disabling Smart Licensing feature, you should reload the router. Failing to do so may result in unpredictable behavior.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**license smart enable** **Example:** `Router# license smart enable`	Activates Smart Licensing on the device. **Note** When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. **Note** Use the no form of the command to disable smart licensing.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router# exit`	Exits the global configuration mode.

Registering the Device

In this task, the device supplies token id to the Cisco back-end and receives an ID that is valid for 365 days. This certificate is saved and automatically used for all future communications with Cisco. This only needs to be done once per device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**license smart register idtoken** *idtoken* **Example:** `Router# license smart register idtoken 123`	Registers the device with the back-end server. Token id can be obtained from your virtual a/c in the Smart Licensing server.
Step 3	**license smart deregister** **Example:** `Router# license smart deregister`	Deregisters the device from the backend server. **Note** When you use this command, the device is deregistered from the licensing cloud. All Smart Licensing entitlements and certificates on the platform are removed and appropriate notifications are sent to the platform and features that were using the entitlements. If you want to use smart licensing again, you should run the **license smart register** command again with a token. Tokens are valid for 1-365 days (user-specified)..
Step 4	**license smart renew**[**ID** | **auth**] **Example:** `Router# license smart renew ID`	(Optional) Manually renews the ID certification or authorization.

Authorizing the Device

When the device is registered, the agent stores the entitlement requests and checks with the backend to check for usage authorization. Authorization responses are valid for 90 days. After the expiry of the term, the device should get reauthorized from the backend again.

Verifying Smart Licensing Configuration

Use the following show commands to verify the Smart Licensing configuration.

To display all the license information, use the **show license all** command as shown in the example below:

```
Router# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: Default Virtual Account
  Initial Registration: SUCCEEDED on Feb 16 23:32:44 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Aug 15 23:32:43 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: AUTHORIZED on Feb 18 11:07:03 2015 UTC
  Last Communication Attempt: SUCCEEDED on Feb 18 11:07:03 2015 UTC
  Next Communication Attempt: Mar 20 11:07:03 2015 UTC
  Communication Deadline: May 19 05:32:22 2015 UTC

License Usage
==============

(asr901_AdvancedMetro):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

(asr901_Gige4SfpUpgra):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

(asr901_Gige4CuUpgrad):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:A901-4C-F-D,SN:CAT1747U2BF
```

```
Agent Version
=============
Smart Agent for Licensing: 1.2.1_throttle/5
Component Versions: SA:(1_2_1_throttle)1.1.0, SI:(rel20)1.0.0, CH:(rel4)1.0.15,
PK:(rel16)1.0.6
```

To display the license status information, use the **show license status** command as shown in the example below:

```
Router# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: Default Virtual Account
  Initial Registration: SUCCEEDED on Feb 16 23:32:44 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Aug 15 23:32:42 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: AUTHORIZED on Feb 18 11:07:03 2015 UTC
  Last Communication Attempt: SUCCEEDED on Feb 18 11:07:03 2015 UTC
  Next Communication Attempt: Mar 20 11:07:02 2015 UTC
  Communication Deadline: May 19 05:32:21 2015 UTC
```

To display the license summary information, use the **show license summary** command as shown in the example below:

```
Router# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: Default Virtual Account
  Last Renewal Attempt: None
  Next Renewal Attempt: Aug 15 23:32:43 2015 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Mar 20 11:07:03 2015 UTC

License Usage:
               License       Entitlement tag    Count Status
  ---------------------------------------------------------------
                      (asr901_AdvancedMetro) 1        AUTHORIZED
                      (asr901_Gige4SfpUpgra) 1        AUTHORIZED
                      (asr901_Gige4CuUpgrad) 1        AUTHORIZED


Router#sh license tec
Router#sh license tech su
Router#sh license tech support
Smart Licensing Tech Support info

Smart Licensing Status
======================
```

```
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: Default Virtual Account
  Initial Registration: SUCCEEDED on Feb 16 23:32:44 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Aug 15 23:32:43 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: AUTHORIZED on Feb 18 11:07:03 2015 UTC
  Last Communication Attempt: SUCCEEDED on Feb 18 11:07:03 2015 UTC
  Next Communication Attempt: Mar 20 11:07:03 2015 UTC
  Communication Deadline: May 19 05:32:22 2015 UTC

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 48 minutes, 21 seconds

License Usage
=============
Handle: 1
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-08.com.cisco.asr901_AdvancedMetroIPAccess,1.0_14ff6adc-3428-47c8-8785-6d50c8625f55

    Description: <empty>
    Count: 1
    Version: 1.0
    Status: AUTHORIZED(3)
    Status time: Feb 18 11:06:44 2015 UTC
    Request Time: Jan  2 00:00:01 2006 UTC

Handle: 2
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-08.com.cisco.asr901_Gige4SfpUpgrade,1.0_e915366f-c9af-4dd9-b540-305725da8fb6
    Description: <empty>
    Count: 1
    Version: 1.0
    Status: AUTHORIZED(3)
    Status time: Feb 18 11:06:44 2015 UTC
    Request Time: Feb 18 11:05:50 2015 UTC

Handle: 3
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-08.com.cisco.asr901_Gige4CuUpgrade,1.0_038900ea-4249-42c1-90c8-76b737a6dabf
    Description: <empty>
    Count: 1
    Version: 1.0
    Status: AUTHORIZED(3)
    Status time: Feb 18 11:06:44 2015 UTC
    Request Time: Feb 18 11:05:50 2015 UTC

Product Information
===================
UDI: PID:A901-4C-F-D,SN:CAT1747U2BF

Agent Version
=============
Smart Agent for Licensing: 1.2.1_throttle/5
```

```
Component Versions: SA:(1_2_1_throttle)1.1.0, SI:(rel20)1.0.0, CH:(rel4)1.0.15,
PK:(rel16)1.0.6

Upcoming Scheduled Jobs
=======================
Current time: Feb 18 11:08:31 2015 UTC
IdCert Expiration Warning: Dec 18 17:57:45 2015 UTC (303 days, 6 hours, 49 minutes, 14
seconds remaining)
Daily: Feb 19 11:05:49 2015 UTC (23 hours, 57 minutes, 18 seconds remaining)
Certificate Renewal: Aug 15 23:32:43 2015 UTC (178 days, 12 hours, 24 minutes, 12 seconds
remaining)
Certificate Expiration Check: Feb 16 17:57:45 2016 UTC (363 days, 6 hours, 49 minutes, 14
seconds remaining)
Authorization Renewal: Mar 20 11:07:03 2015 UTC (29 days, 23 hours, 58 minutes, 32 seconds
 remaining)
Authorization Expiration Check: May 19 05:32:22 2015 UTC (89 days, 18 hours, 23 minutes,
51 seconds remaining)
Init Flag Check: Not Available

License Certificates
====================
Production Cert: False
PIID: d0dba898-674b-4420-96e6-6186abc54afb
Licensing Certificated:
    Id certificate Info:
        Start Date: Feb 16 17:57:46 2015 UTC
        Expiry Date: Feb 16 17:57:46 2016 UTC
        Version Number: 3
        Serial Number: 130921
        Common Name: 1E4712A4FFD650C29359701C8DB6ECF02CB9048A::1,2

    Signing certificate Info:
        Start Date: Jun 14 20:18:52 2013 UTC
        Expiry Date: Apr 24 21:55:42 2033 UTC
        Version Number: 3
        Serial Number: 3
        Common Name: MMI Signer

    Sub CA Info:
        Start Date: Apr 24 22:19:15 2013 UTC
        Expiry Date: Apr 24 21:55:42 2033 UTC
        Version Number: 3
        Serial Number: 2
        Common Name: Smart Licensing CA - DEV


HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless

Other Info
==========
Software ID: regid.2014-08.com.cisco.ASR901,1.0_63ef356d-26bc-431b-8ef2-792054f1a118
Agent State: authorized
TS enable: True
Transport: Callhome
Locale: en_US.UTF-8
Debug flags: 0x0
Privacy Send Hostname: True
```

```
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 4
sizeof(time_t): 4
sizeof(size_t): 4
Endian: Big
routingReadyByEvent: True
systemInitByEvent: True
WaitForHaRole: False
standbyIsHot: False
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: False
debugFlags: 0
```

To display the license udi information, use the **show license udi** command as shown in the example below:

```
Router# show license udi

UDI: PID:A901-4C-F-D,SN:CAT1747U2BF
```

To display the license usage information, use the **show license usage** command as shown in the example below:

```
Router# show license usage

License Authorization:
  Status: AUTHORIZED on Feb 18 11:07:03 2015 UTC

(asr901_AdvancedMetro):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

(asr901_Gige4SfpUpgra):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

(asr901_Gige4CuUpgrad):
  Description:
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

Configuration Examples for Smart Licensing

```
Router> show running-config

Building configuration...

Current configuration : 3216 bytes
```

```
!
! No configuration change since last restart
!
version 15.5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
!
hostname 10G_ASR901_2015
!
boot-start-marker
boot system tftp://10.105.33.135//auto/tftp-blr-users4/byashasw/mcp_2014-12-17-a
sr901
boot-end-marker
!
!
!card type command needed for slot/vwic-slot 0/0
no logging console
!
no aaa new-model
clock timezone IST 5 30
call-home
 contact-email-addr byashasw@cisco.com
 mail-server 72.163.4.161 priority 1
 sender from Yasha_CH@cisco.com
 profile "CiscoTAC-1"
  active
  no reporting smart-licensing-data
  destination transport-method http
  no destination transport-method email
  destination address http http://10.22.183.117:8080/ddce/services/DDCEService
  no destination address http https://tools.cisco.com/its/service/oddce/services
/DDCEService
 profile "User_Profile"
  reporting smart-licensing-data
  destination transport-method http
  destination address http http://10.22.183.117:8080/ddce/services/DDCEService
ip cef
!
!
!
!

no ipv6 cef
!
!
!
!
!
!
!
multilink bundle-name authenticated
l3-over-l2 flush buffers
asr901-storm-control-bpdu 1000
!
!
spanning-tree mode pvst
spanning-tree extend system-id
license udi pid A901-6CZ-FT-A sn CAT1625U0EL
!
!
!
```

```
!
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 !
interface GigabitEthernet0/8
 no ip address
 shutdown
 negotiation auto
 qos-config scheduling-mode min-bw-guarantee
!
interface GigabitEthernet0/9
 no ip address
 shutdown
 negotiation auto
 qos-config scheduling-mode min-bw-guarantee
!
interface GigabitEthernet0/10
 no ip address
 shutdown
 negotiation auto
 qos-config scheduling-mode min-bw-guarantee
!
interface GigabitEthernet0/11
 no ip address
 shutdown
 negotiation auto
 qos-config scheduling-mode min-bw-guarantee
!
interface TenGigabitEthernet0/0
 no ip address
 shutdown
!
interface TenGigabitEthernet0/1
 no ip address
 shutdown
 no negotiation auto
!
interface FastEthernet0/0
 ip address 10.64.99.202 255.255.255.128
!
interface Vlan1
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip http client source-interface FastEthernet0/0
ip route 0.0.0.0 0.0.0.0 202.153.144.25
ip route 0.0.0.0 0.0.0.0 10.64.99.1
```

```
ip route 0.0.0.0 0.0.0.0 10.64.99.129
ip route 10.105.33.0 255.255.255.0 10.64.99.129
!
!
!
!
control-plane
!
environment monitor
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
exception crashinfo buffersize 128
!
!
end
```

Example: Smart Call Home

Sample configuration example for Smart Call Home is provided below:

```
! Enabling call-home service
Router# config terminal
Router(config)#service call-home
Router(config)#call-home
! Configuring call-home profile. HTTP transport method is used for smart license reporting.
Router(cfg-call-home)#contact-email-addr user@cisco.com
Router(cfg-call-home)#profile CiscoTAC-1
Router(cfg-call-home-profile)#active
Router(cfg-call-home-profile)#destination transport-method http
!CiscoTAC-1 profile cannot enable more than one transport method. HTTP transport has been
enabled and email transport disabled.
Router(cfg-call-home-profile)#destination address http
http://10.22.183.117:8080/ddce/services/DDCEService
Router(cfg-call-home-profile)#reporting smart-licensing-data
Router(cfg-call-home-profile)#end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco License Manager Application	User Guide for Cisco License Manager

Standards and RFCs

Standard/RFC	Title

MIBs

MIB	MIBs Link
CISCO-LICENSE-MGMT-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Cisco Smart Licensing

The following table provides release information about the feature or features described in this module. This table 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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 65: Feature Information for Cisco Smart Licensing

Feature Name	Releases	Feature Information
Cisco Smart Licensing	Cisco IOS Release 15.5(2)S	This feature was introduced on the Cisco ASR 901 Series Routers.

CHAPTER 56

MAC Layer 2 Access Control Lists

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACLs) provide the capability to filter packets at a fine granularity. MAC ACLs are ACLs that filter traffic using information in the layer 2 header of each packet.

Layer 2 MAC ACLs allow the permission or denial of the packets based on the MAC source and destination addresses. This module describes how to implement MAC ACLs.

Prerequisites for MAC Layer 2 Access Control Lists

- Knowledge of how service instances are configured.
- Knowledge of extended MAC ACLs and how they are configured.

Restrictions for MAC Layer 2 Access Control Lists

The following limitations and configuration guidelines apply when configuring MAC Layer 2 ACLs:

- MAC ACL is only supported on the port level.
- Classification based on QoS ACL is not supported for MAC ACL.
- MAC ACLs apply to only ingress traffic.
- MAC ACL is not supported on EVC.
- MAC ACL is not supported on VLAN interface.
- MAC ACL occupies the layer 2 ACL slice based on the availability of the Ingress Field Processor (IFP) slice.
- MAC ACL is supported on 1G and 10G interfaces.
- MAC ACL is supported on Gigabit Ethernet interface and its bundle derivatives.

- MAC ACL is not supported on Multilink Point-to-Point (MLPPP) interface.
- MAC ACL and IP ACLs are not supported together on an interface.
- Named MAC ACLs are only supported.
- MAC ACLs share many fundamental concepts including the configurations and limitations with IP ACLs.
- A maximum of 128 entries can be configured per MAC ACL slice.

How to Configure MAC Layer 2 Access Control Lists

Creating a Layer 2 ACL

Perform this task to create a Layer 2 ACL with a single ACE.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mac-access-list extended** *name* **Example:** `Device(config)# mac-access-list extended test-12-acl`	Defines an extended MAC ACL and enters mac access list control configuration mode.
Step 4	**permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**}} **Example:** `Device(config-ext-macl)# permit host 00aa.00bb.00cc host 00aa.00bb.00dd`	Allows forwarding of layer 2 traffic if the conditions are matched. Creates an ACE for the ACL.

Configuring MAC Layer 2 ACL on an Interface

Perform this task to configure the MAC layer 2 ACL on an interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**# mac-access-list extended** *name* **Example:** `Device(config)# mac-access list extended test-12-acl`	Defines an extended MAC ACL and enters mac access control list configuration mode.
Step 4	**permit** {*host src-mac* | *src-mac mask* **any**} {*host dest-mac* | *dest-mac mask* **any**} **Example:** `Device(config-ext-macl)# permit host 00aa.bbcc.ddeb host 00bb.bbcc.ddeb`	Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.
Step 5	**deny any any** **Example:** `Device(config-ext-macl)# deny any any`	Prevents forwarding of Layer 2 traffic except for the allowed ACEs.
Step 6	**exit** **Example:** `Device(config-ext-macl)# exit`	Exits the current command mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/0`	Specifies the interface.
Step 8	**mac access-group** *access-list-name* **in** **Example:** `Device(config-if-srv)# mac access-group test-12-acl in`	Applies a MAC ACL to control incoming traffic on the interface.

Configuration Examples for Layer 2 MAC Access Control Lists

```
!
permit host 0001.0001.0001 host 0002.0002.0002 sequence 10
deny   any any sequence 20
permit any any sequence 30
.
.
.
.
!
interface GigabitEthernet0/0
no ip address
negotiation auto
mac access-group scale in
end
```

Verification of configuration

Use the following command to verify the configuration of MAC layer 2 ACL:

```
#sh access-lists macacl
Extended MAC access list macacl
permit host 0001.0001.0001 host 0002.0002.0002 sequence 10
deny   any any sequence 20
permit any any sequence 30
```

Use the following command to verify the configuration of MAC layer 2 ACL on an interface:

```
#sh run int g0/0
Building configuration...
Current configuration : 106 bytes
!
interface GigabitEthernet0/0
no ip address
negotiation auto
mac access-group scale in
end
```

INDEX

A

B

C