IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 24.1.x, 24.2.x , 24.3.x

First Published: 2024-03-14

Last Modified: 2024-09-04

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

Preface

From Release 6.1.2 onwards, Cisco introduces support for the 64-bit Linux-based IOS XR operating system. Extensive feature parity is maintained between the 32-bit and 64-bit environments. Unless explicitly marked otherwise, the contents of this document are applicable for both the environments. For more details on Cisco IOS XR 64 bit, refer to the Release Notes for Cisco ASR 9000 Series Routers, Release 6.1.2 document.

The *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers* preface contains these sections:

Changes to This Document

Table 1: Changes to This Document

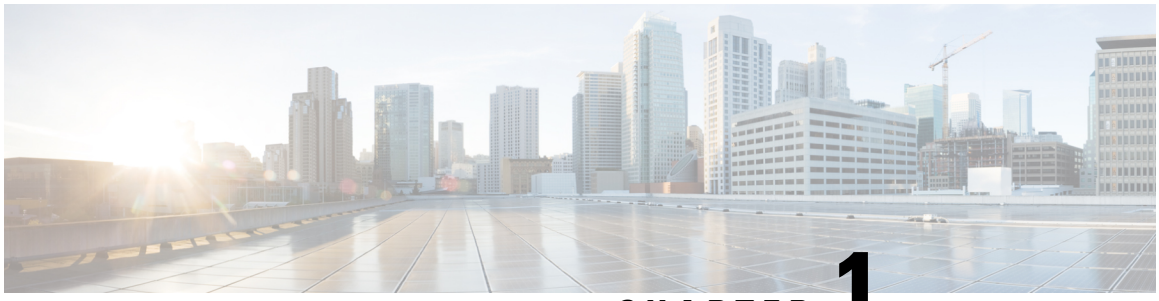
Date	Change Summary
September 2024	Republished for Release 24.3.1
June 2024	Republished for Release 24.2.1
February 2024	Initial release of this document

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed IP Addresses and Services Features

This table summarizes the new and changed feature information for the *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers*, and tells you where they are documented.

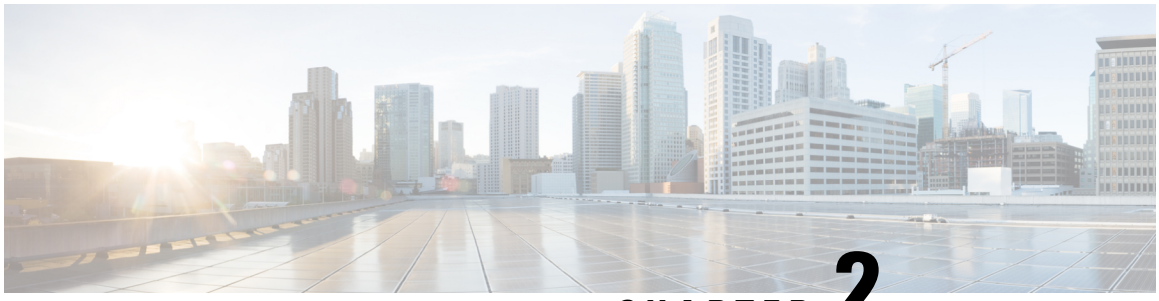
IP Addresses and Services Features Added or Modified in IOS XR Release 24.x.x

This section describes the new and changed IP addresses features for Cisco IOS XR.

IP Addresses Features Added or Modified in IOS XR Release 24.x.x

Table 2: New and Changed Features

Feature	Description	Changed in Release	Where Documented
TCP Dump File Converter	This feature was introduced.	Release 24.2.1	TCP Dump File Converter, on page 401



CHAPTER 2

YANG Data Models for IP Addressing Features

This chapter provides information about the YANG data models for IP Addressing features.

• Using YANG Data Models, on page 3

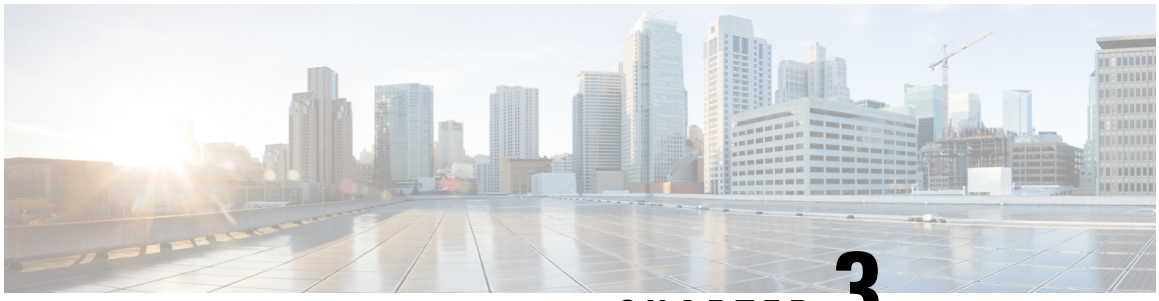
Using YANG Data Models

Cisco IOS XR supports a programmatic way of configuring and collecting operational data of a network device using YANG data models. Although configurations using CLIs are easier and human-readable, automating the configuration using model-driven programmability results in scalability.

The data models are available in the release image, and are also published in the Github repository. Navigate to the release folder of interest to view the list of supported data models and their definitions. Each data model defines a complete and cohesive model, or augments an existing data model with additional XPaths. To view a comprehensive list of the data models supported in a release, navigate to the **Available-Content.md** file in the repository.

You can also view the data model definitions using the YANG Data Models Navigator tool. This GUI-based and easy-to-use tool helps you explore the nuances of the data model and view the dependencies between various containers in the model. You can view the list of models supported across Cisco IOS XR releases and platforms, locate a specific model, view the containers and their respective lists, leaves, and leaf lists presented visually in a tree structure. This visual tree form helps you get insights into nodes that can help you automate your network.

To get started with using the data models, see the *Programmability Configuration Guide*.



CHAPTER 3

Implementing Network Stack IPv4 and IPv6

The Network Stack IPv4 and IPv6 features are used to configure and monitor Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

This module describes the new and revised tasks you need to implement Network Stack IPv4 and IPv6 on your Cisco IOS XR network.

Note For a complete description of the Network Stack IPv4 and IPv6 commands, refer to the *Network Stack IPv4 and IPv6 Commands* module of the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Feature History for Implementing Network Stack IPv4 and IPv6

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	GRE for IPv4 feature was added.
Release 4.2.1	IPv6 over IPv4 GRE Tunnel interface feature was added.
Release 5.3.1	IPv6 Virtual Addresses feature was added.
Release 5.3.2	IPv6 Path MTU Discovery support for applications using Ping protocol was introduced.

Prerequisites for Implementing Network Stack IPv4 and IPv6

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

- Check test

Restrictions for Implementing Network Stack IPv4 and IPv6

In any Cisco IOS XR software release with IPv6 support, multiple IPv6 global addresses can be configured on an interface. However, multiple IPv6 link-local addresses on an interface are not supported.

Information About Implementing Network Stack IPv4 and IPv6

To implement Network Stack IPv4 and IPv6, you need to understand the following concepts:

Network Stack IPv4 and IPv6 Exceptions

The Network Stack feature in the Cisco IOS XR software has the following exceptions:

- In Cisco IOS XR software, the **clear ipv6 neighbors** and **show ipv6 neighbors** commands include the **location** *node-id* keyword. If a location is specified, only the neighbor entries in the specified location are displayed.
- The **ipv6 nd scavenge-timeout** command sets the lifetime for neighbor entries in the stale state. When the scavenge-timer for a neighbor entry expires, the entry is cleared.
- In Cisco IOS XR software, the **show ipv4 interface** and **show ipv6 interface** commands include the **location** *node-id* keyword. If a location is specified, only the interface entries in the specified location are displayed.
- Cisco IOS XR software allows conflicting IP address entries at the time of configuration. If an IP address conflict exists between two interfaces that are active, Cisco IOS XR software brings down the interface according to the configured conflict policy, the default policy being to bring down the higher interface instance. For example, if GigabitEthernet 0/1/0/1 conflicts with GigabitEthernet 0/2/0/1, then the IPv4 protocol on GigabitEthernet 0/2/0/1 is brought down and IPv4 remains active on GigabitEthernet 0/1/0/1.

IPv4 and IPv6 Functionality

When Cisco IOS XR software is configured with both an IPv4 and an IPv6 address, the interface can send and receive data on both IPv4 and IPv6 networks.

The architecture of IPv6 has been designed to allow existing IPv4 users to make the 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 prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities provide an IPv6 addressing hierarchy that allows for more efficient

routing. IPv6 supports widely deployed routing protocols such as Open Shortest Path First (OSPF), and multiprotocol Border Gateway Protocol (BGP).

The IPv6 neighbor discovery (nd) process uses Internet Control Message Protocol (ICMP) 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.

IPv6 for Cisco IOS XR Software

IPv6, formerly named IPng (next generation) is the latest version of the Internet Protocol (IP). IP is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 was proposed when it became clear that the 32-bit addressing scheme of IP version 4 (IPv4) was inadequate to meet the demands of Internet growth. After extensive discussion, it was decided to base IPng on IP but add a much larger address space and improvements such as a simplified main header and extension headers. IPv6 is described initially in RFC 2460, I*nternet Protocol, Version 6 (IPv6) Specification* issued by the Internet Engineering Task Force (IETF). Further RFCs describe the architecture and services supported by IPv6.

Larger IPv6 Address Space

The primary motivation for IPv6 is the need to meet the anticipated future demand for globally unique IP addresses. Applications such as mobile Internet-enabled devices (such as personal digital assistants [PDAs], telephones, and cars), home-area networks (HANs), and wireless data services are driving the demand for globally unique IP addresses. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides more than enough globally unique IP addresses for every networked device on the planet. By being globally unique, IPv6 addresses inherently enable global reachability and end-to-end security for networked devices, functionality that is crucial to the applications and services that are driving the demand for the addresses. Additionally, the flexibility of the IPv6 address space reduces the need for private addresses and the use of Network Address Translation (NAT); therefore, IPv6 enables new application protocols that do not require special processing by border routers at the edge of networks.

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:

2001:0DB8:7654:3210:FEDC:BA98:7654:3210

2001:0DB8:0:0:8:800:200C:417A

It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, two colons (::) can 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 3: Compressed IPv6 Address Formats, on page 8 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 interfaces, 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 3: Compressed IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	2001:0:0:0:0DB8:800:200C:417A	1080::0DB8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
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 3: Compressed IPv6 Address Formats, on page 8 may be 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 3: Compressed IPv6 Address Formats, on page 8 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* argument must be in the form documented in RFC 2373, in which 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 compose the prefix (the network portion of the address). For example, 2001:0DB8:8086:6502::/32 is a valid IPv6 prefix.

IPv6 Address Type: Unicast

An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address. Cisco IOS XR software supports the following IPv6 unicast address types:

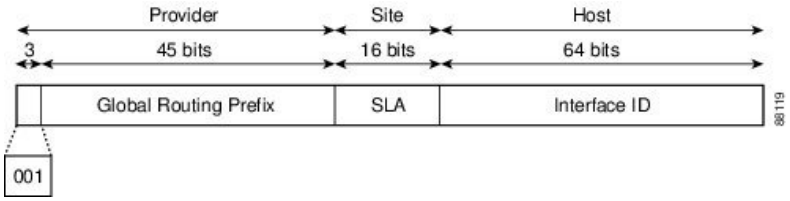
- Global aggregatable address
- Site-local address (proposal to remove by IETF)
- Link-local address
- IPv4-compatible IPv6 address

Aggregatable Global Address

An aggregatable global address is an IPv6 address from the aggregatable global unicast prefix. The structure of aggregatable global unicast addresses enables strict aggregation of routing prefixes that limits the number of routing table entries in the global routing table. Aggregatable global addresses are used on links that are aggregated upward through organizations, and eventually to the Internet service providers (ISPs).

Aggregatable global IPv6 addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Except for addresses that start with binary 000, all global unicast addresses have a 64-bit interface ID. The current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Figure 1: Aggregatable Global Address Format, on page 9shows the structure of an aggregatable global address.

Figure 1: Aggregatable Global Address Format



Addresses with a prefix of 2000::/3 (001) through E000::/3 (111) are required to have 64-bit interface identifiers in the extended universal identifier (EUI)-64 format. The Internet Assigned Numbers Authority (IANA) allocates the IPv6 address space in the range of 2000::/16 to regional registries.

The aggregatable global address typically consists of a 48-bit global routing prefix and a 16-bit subnet ID or Site-Level Aggregator (SLA). In the IPv6 aggregatable global unicast address format document (RFC 2374), the global routing prefix included two other hierarchically structured fields named Top-Level Aggregator (TLA) and Next-Level Aggregator (NLA).The IETF decided to remove the TLS and NLA fields from the RFCs, because these fields are policy-based. Some existing IPv6 networks deployed before the change might still be using networks based on the older architecture.

A 16-bit subnet field called the subnet ID could be used by individual organizations to create their own local addressing hierarchy and to identify subnets. A subnet ID is similar to a subnet in IPv4, except that an organization with an IPv6 subnet ID can support up to 65,535 individual subnets.

An interface ID is used to identify interfaces on a link. The interface ID must be unique to the link. It may also be unique over a broader scope. In many cases, an interface ID is the same as or based on the link-layer address of an interface. Interface IDs used in aggregatable global unicast and other IPv6 address types must be 64 bits long and constructed in the modified EUI-64 format.

Interface IDs are constructed in the modified EUI-64 format in one of the following ways:

- For all IEEE 802 interface types (for example, Ethernet interfaces and FDDI interfaces), the first three octets (24 bits) are taken from the Organizationally Unique Identifier (OUI) of the 48-bit link-layer address (MAC address) of the interface, the fourth and fifth octets (16 bits) are a fixed hexadecimal value of FFFE, and the last three octets (24 bits) are taken from the last three octets of the MAC address. The construction of the interface ID is completed by setting the Universal/Local (U/L) bit—the seventh bit of the first octet—to a value of 0 or 1. A value of 0 indicates a locally administered identifier; a value of 1 indicates a globally unique IPv6 interface identifier.
- For all other interface types (for example, serial, loopback, ATM, Frame Relay, and tunnel interface types—except tunnel interfaces used with IPv6 overlay tunnels), the interface ID is constructed in the same way as the interface ID for IEEE 802 interface types; however, the first MAC address from the

pool of MAC addresses in the router is used to construct the identifier (because the interface does not have a MAC address).

- For tunnel interface types that are used with IPv6 overlay tunnels, the interface ID is the IPv4 address assigned to the tunnel interface with all zeros in the high-order 32 bits of the identifier.

Note For interfaces using Point-to-Point Protocol (PPP), given that the interfaces at both ends of the connection might have the same MAC address, the interface identifiers used at both ends of the connection are negotiated (picked randomly and, if necessary, reconstructed) until both identifiers are unique. The first MAC address in the router is used to construct the identifier for interfaces using PPP.

If no IEEE 802 interface types are in the router, link-local IPv6 addresses are generated on the interfaces in the router in the following sequence:

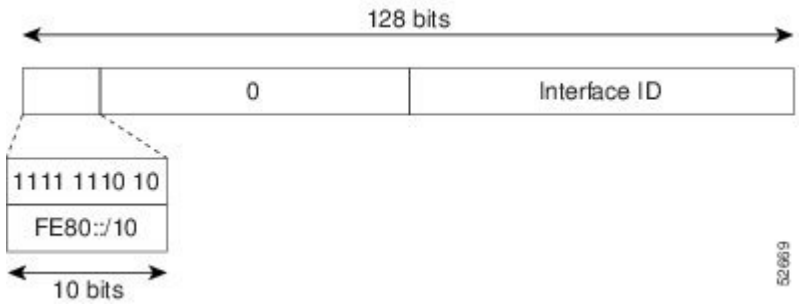
1. The router is queried for MAC addresses (from the pool of MAC addresses in the router).
2. If no MAC address is available, the serial number of the Route Processor (RP) or line card (LC) is used to form the link-local address.

Link-Local Address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need site-local or globally unique addresses to communicate. Figure 2: Link-Local Address Format, on page 10shows the structure of a link-local address.

IPv6 routers must not forward packets that have link-local source or destination addresses to other links.

Figure 2: Link-Local Address Format

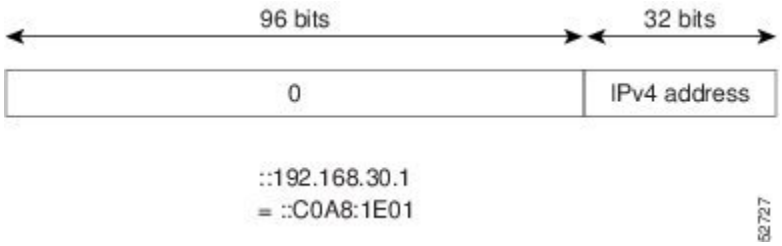


IPv4-Compatible IPv6 Address

An IPv4-compatible IPv6 address is an IPv6 unicast address that has zeros in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The format of an IPv4-compatible IPv6 address is 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D. The entire 128-bit IPv4-compatible IPv6 address is used as the IPv6 address of a node and the IPv4 address embedded in the low-order 32 bits is used as the IPv4 address of the node. IPv4-compatible IPv6 addresses are assigned to nodes that support both the IPv4 and IPv6 protocol

stacks and are used in automatic tunnels. Figure 3: IPv4-Compatible IPv6 Address Format, on page 11 shows the structure of an IPv4-compatible IPv6 address and a few acceptable formats for the address.

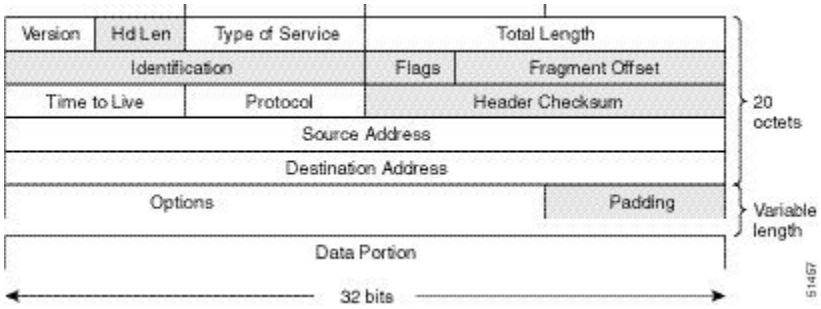
Figure 3: IPv4-Compatible IPv6 Address Format



Simplified IPv6 Packet Header

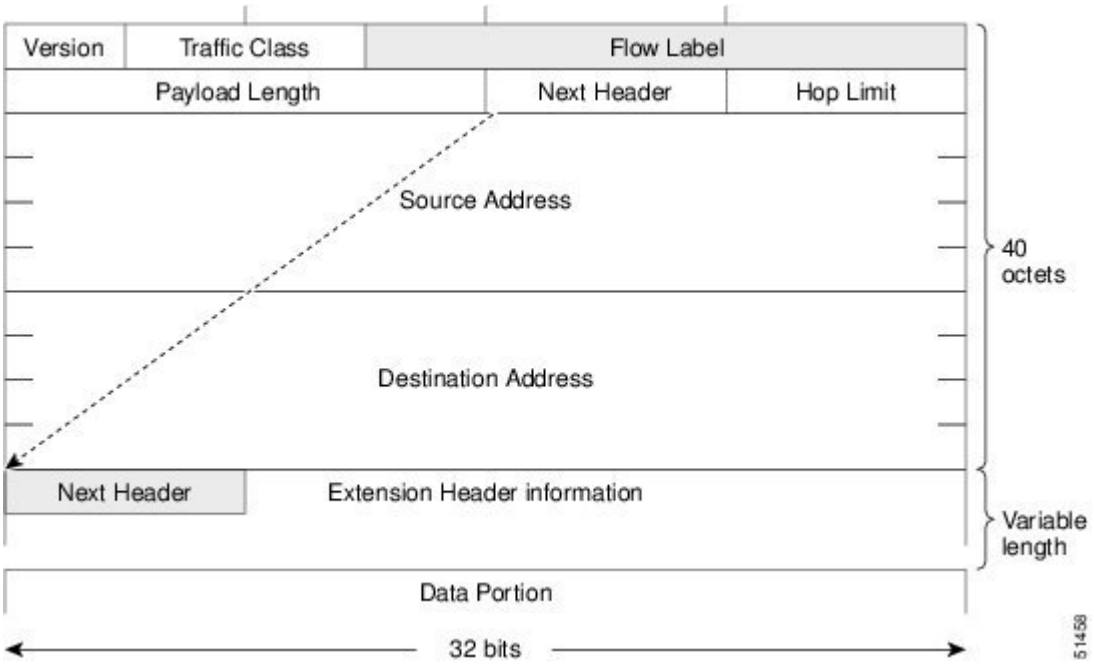
The basic IPv4 packet header has 12 fields with a total size of 20 octets (160 bits). The 12 fields may be followed by an Options field, which is followed by a data portion that is usually the transport-layer packet. The variable length of the Options field adds to the total size of the IPv4 packet header. The shaded fields of the IPv4 packet header are not included in the IPv6 packet header. (See Figure 4: IPv4 Packet Header Format, on page 11)

Figure 4: IPv4 Packet Header Format



The basic IPv6 packet header has 8 fields with a total size of 40 octets (320 bits). (See Figure 5: IPv6 Packet Header Format, on page 12.) Fields were removed from the IPv6 header because, in IPv6, fragmentation is not handled by routers and checksums at the network layer are not used. Instead, fragmentation in IPv6 is handled by the source of a packet and checksums at the data link layer and transport layer are used. (In IPv4, the User Datagram Protocol (UDP) transport layer uses an optional checksum. In IPv6, use of the UDP checksum is required to check the integrity of the inner packet.) Additionally, the basic IPv6 packet header and Options field are aligned to 64 bits, which can facilitate the processing of IPv6 packets.

Figure 5: IPv6 Packet Header Format



This table lists the fields in the basic IPv6 packet header.

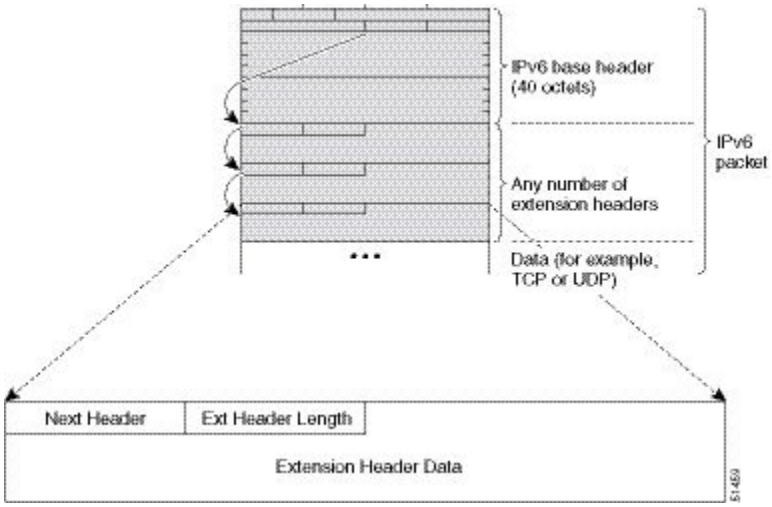
Table 4: Basic IPv6 Packet Header Fields

Field	Description
Version	Similar to the Version field in the IPv4 packet header, except that the field lists number 6 for IPv6 instead of number 4 for IPv4.
Traffic Class	Similar to the Type of Service field in the IPv4 packet header. The Traffic Class field tags packets with a traffic class that is used in differentiated services.
Flow Label	A new field in the IPv6 packet header. The Flow Label field tags packets with a specific flow that differentiates the packets at the network layer.
Payload Length	Similar to the Total Length field in the IPv4 packet header. The Payload Length field indicates the total length of the data portion of the packet.
Next Header	Similar to the Protocol field in the IPv4 packet header. The value of the Next Header field determines the type of information following the basic IPv6 header. The type of information following the basic IPv6 header can be a transport-layer packet, for example, a TCP or UDP packet, or an Extension Header, as shown in Figure 6: IPv6 Extension Header Format, on page 13.
Hop Limit	Similar to the Time to Live field in the IPv4 packet header. The value of the Hop Limit field specifies the maximum number of routers that an IPv6 packet can pass through before the packet is considered invalid. Each router decrements the value by one. Because no checksum is in the IPv6 header, the router can decrement the value without needing to recalculate the checksum, which saves processing resources.

Field	Description
Source Address	Similar to the Source Address field in the IPv4 packet header, except that the field contains a 128-bit source address for IPv6 instead of a 32-bit source address for IPv4.
Destination Address	Similar to the Destination Address field in the IPv4 packet header, except that the field contains a 128-bit destination address for IPv6 instead of a 32-bit destination address for IPv4.

Following the eight fields of the basic IPv6 packet header are optional extension headers and the data portion of the packet. If present, each extension header is aligned to 64 bits. There is no fixed number of extension headers in an IPv6 packet. Together, the extension headers form a chain of headers. Each extension header is identified by the Next Header field of the previous header. Typically, the final extension header has a Next Header field of a transport-layer protocol, such as TCP or UDP. Figure 6: IPv6 Extension Header Format, on page 13shows the IPv6 extension header format.

Figure 6: IPv6 Extension Header Format



This table lists the extension header types and their Next Header field values.

Table 5: IPv6 Extension Header Types

Header Type	Next Header Value	Description
Hop-by-hop options header	0	This header is processed by all hops in the path of a packet. When present, the hop-by-hop options header always follows immediately after the basic IPv6 packet header.
Destination options header	60	The destination options header can follow any hop-by-hop options header, in which case the destination options header is processed at the final destination and also at each visited address specified by a routing header. Alternatively, the destination options header can follow any Encapsulating Security Payload (ESP) header, in which case the destination options header is processed only at the final destination.

Header Type	Next Header Value	Description
Routing header	43	The routing header is used for source routing.
Fragment header	44	The fragment header is used when a source must fragment a packet that is larger than the maximum transmission unit (MTU) for the path between itself and a destination. The Fragment header is used in each fragmented packet.
Authentication header and ESP header	51 50	The Authentication header and the ESP header are used within IP Security Protocol (IPSec) to provide authentication, integrity, and confidentiality of a packet. These headers are identical for both IPv4 and IPv6.
Upper-layer header	6 (TCP) 17 (UDP)	The upper-layer (transport) headers are the typical headers used inside a packet to transport the data. The two main transport protocols are TCP and UDP.
Mobility header	To be done by IANA	Extension headers used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings.

Path MTU Discovery for IPv6

As in IPv4, path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, however, fragmentation is handled by the source of a packet when the path MTU of one link along a given data path is not large enough to accommodate the size of the packets. Having IPv6 hosts handle packet fragmentation saves IPv6 router processing resources and helps IPv6 networks run more efficiently.

In IPv4, the minimum link MTU is 68 octets, which means that the MTU size of every link along a given data path must support an MTU size of at least 68 octets. In IPv6, the minimum link MTU is 1280 octets. We recommend using an MTU value of 1500 octets for IPv6 links.

Note Path MTU discovery is supported only for applications using TCP and Ping protocol.

To enable path MTU discovery in IPv6 for applications using the Ping protocol, the path MTU command must be enabled. To do so, run the following command in global configuration mode:

```
RP/0/RSP0/CPU0:router(config)# ipv6 path-mtu enable
```

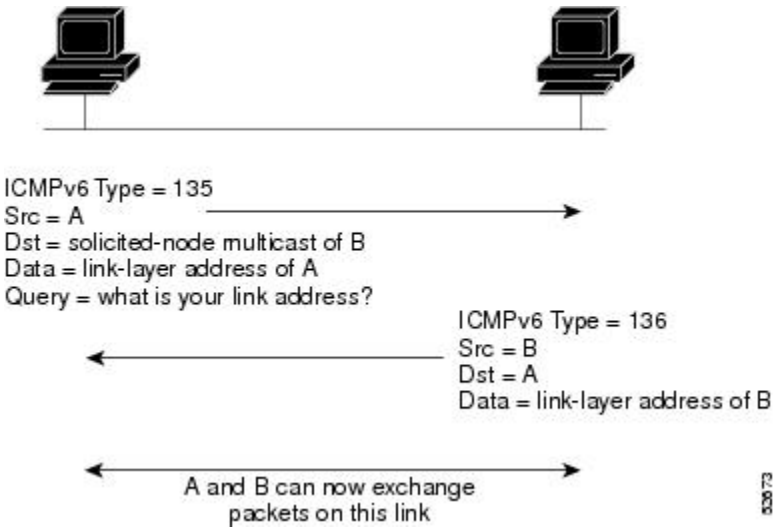
IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMP 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.

IPv6 Neighbor Solicitation Message

A value of 135 in the Type field of the ICMP packet header identifies a neighbor solicitation message. Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link. (See Figure 7: IPv6 Neighbor Discovery—Neighbor Solicitation Message, on page 15.) When a node wants to determine the link-layer address of another node, the source address in a neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The destination address in the neighbor solicitation message is the solicited-node multicast address that corresponds to the IPv6 address of the destination node. The neighbor solicitation message also includes the link-layer address of the source node.

Figure 7: IPv6 Neighbor Discovery—Neighbor Solicitation Message



After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message, which has a value of 136 in the Type field of the ICMP packet header, on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node (more specifically, the IPv6 address of the node interface) sending the neighbor advertisement message. The destination address in the neighbor advertisement message 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 can communicate.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verifying the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. Neighbor unreachability detection identifies the failure of a neighbor or the failure of the forward path to the neighbor, and is used for all paths between hosts and neighboring nodes (hosts or routers). Neighbor unreachability detection is performed for neighbors to which only unicast packets are being sent and is not performed for neighbors to which multicast packets are being sent.

A neighbor is considered reachable when a positive acknowledgment is returned from the neighbor (indicating that packets previously sent to the neighbor have been received and processed). A positive acknowledgment—from an upper-layer protocol (such as TCP)—indicates that a connection is making forward progress (reaching its destination) or that a neighbor advertisement message in response to a neighbor solicitation message has been received. If packets are reaching the peer, they are also reaching the next-hop neighbor of the source. Therefore, forward progress is also a confirmation that the next-hop neighbor is reachable.

For destinations that are not on the local link, forward progress implies that the first-hop router is reachable. When acknowledgments from an upper-layer protocol are not available, a node probes the neighbor using unicast neighbor solicitation messages to verify that the forward path is still working. The return of a solicited neighbor advertisement message from the neighbor is a positive acknowledgment that the forward path is still working. (Neighbor advertisement messages that have the solicited flag set to a value of 1 are sent only in response to a neighbor solicitation message.) Unsolicited messages confirm only the one-way path from the source to the destination node; solicited neighbor advertisement messages indicate that a path is working in both directions.

Note A neighbor advertisement message that has the solicited flag set to a value of 0 must not be considered as a positive acknowledgment that the forward path is still working.

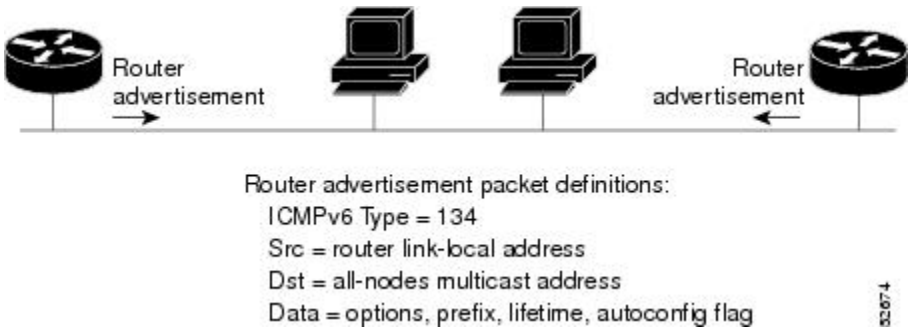
Neighbor solicitation messages are also used in the stateless autoconfiguration process to verify the uniqueness of unicast IPv6 addresses before the addresses are assigned to an interface. Duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface. (The new address remains in a tentative state while duplicate address detection is performed.) Specifically, a node sends a neighbor solicitation message with an unspecified source address and a tentative link-local address in the body of the message. If another node is already using that address, the node returns a neighbor advertisement message that contains the tentative link-local address. If another node is simultaneously verifying the uniqueness of the same address, that node also returns a neighbor solicitation message. If no neighbor advertisement messages are received in response to the neighbor solicitation message and no neighbor solicitation messages are received from other nodes that are attempting to verify the same tentative address, the node that sent the original neighbor solicitation message considers the tentative link-local address to be unique and assigns the address to the interface.

Every IPv6 unicast address (global or link-local) must be checked for uniqueness on the link; however, until the uniqueness of the link-local address is verified, duplicate address detection is not performed on any other IPv6 addresses associated with the link-local address. The Cisco implementation of duplicate address detection in the Cisco IOS XR software does not check the uniqueness of anycast or global addresses that are generated from 64-bit interface identifiers.

IPv6 Router Advertisement Message

Router advertisement (RA) messages, which have a value of 134 in the Type field of the ICMP packet header, are periodically sent out each configured interface of an IPv6 router. The router advertisement messages are sent to the all-nodes multicast address. (See Figure 8: IPv6 Neighbor Discovery—Router Advertisement Message, on page 17.)

Figure 8: IPv6 Neighbor Discovery—Router Advertisement Message



Router advertisement messages typically include the following information:

- One or more onlink IPv6 prefixes that nodes on the local link can use to automatically configure their IPv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or statefull) that can be completed
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time, in seconds, that the router should be used as a default router)
- Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates

Router advertisements are also sent in response to router solicitation messages. 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 router advertisement message. Given that router solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in router solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When a router advertisement is sent in response to a router solicitation, the destination address in the router advertisement message is the unicast address of the source of the router solicitation message.

The following router advertisement message parameters can be configured:

- The time interval between periodic router advertisement messages
- The “router lifetime” value, which indicates the usefulness of a router as the default router (for use by all nodes on a given link)
- The network prefixes in use on a given link
- The time interval between neighbor solicitation message retransmissions (on a given link)
- The amount of time a node considers a neighbor reachable (for use by all nodes on a given link)

The configured parameters are specific to an interface. The sending of router advertisement messages (with default values) is automatically enabled on Ethernet and FDDI interfaces. For other interface types, the sending of router advertisement messages must be manually configured by using the **no ipv6 nd suppress-ra** command

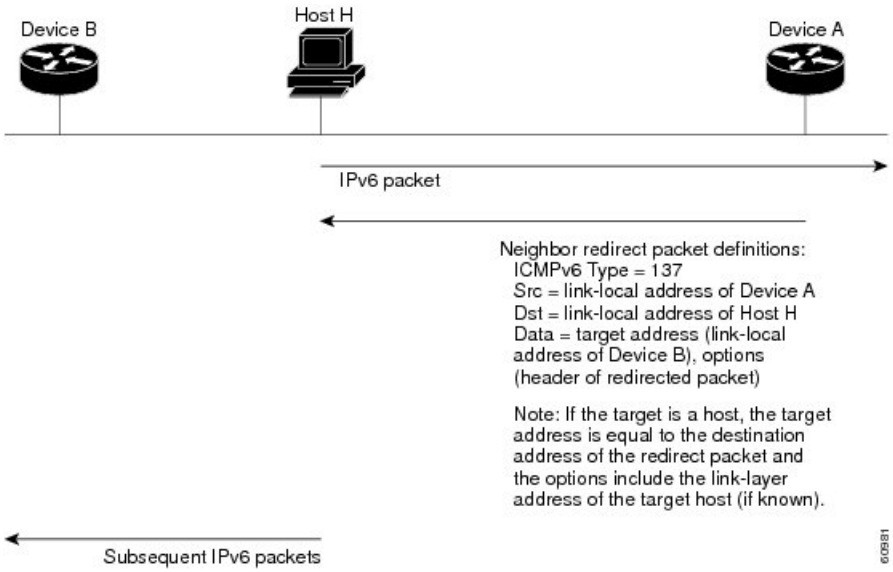
in interface configuration mode. The sending of router advertisement messages can be disabled on individual interfaces by using the **ipv6 nd suppress-ra** command in interface configuration mode.

Note For stateless autoconfiguration to work properly, the advertised prefix length in router advertisement messages must always be 64 bits.

IPv6 Neighbor Redirect Message

A value of 137 in the Type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Routers send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination. (See Figure 9: IPv6 Neighbor Discovery—Neighbor Redirect Message , on page 18.)

Figure 9: IPv6 Neighbor Discovery—Neighbor Redirect Message



Note A router must be able to determine the link-local address for each of its neighboring routers to ensure that the target address (the final destination) in a redirect message identifies the neighbor router by its link-local address. For static routing, the address of the next-hop router should be specified using the link-local address of the router; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring routers.

After forwarding a packet, a router should send a redirect message to the source of the packet under the following circumstances:

- The destination address of the packet is not a multicast address.
- The packet was not addressed to the router.
- The packet is about to be sent out the interface on which it was received.
- The router determines that a better first-hop node for the packet resides on the same link as the source of the packet.

- The source address of the packet is a global IPv6 address of a neighbor on the same link, or a link-local address.

Use the **ipv6 icmp error-interval** global configuration command to limit the rate at which the router generates all IPv6 ICMP error messages, including neighbor redirect messages, which ultimately reduces link-layer congestion.

Note A router must not update its routing tables after receiving a neighbor redirect message, and hosts must not originate neighbor redirect messages.

Preventing IPv6 ND Packet Drops Using CoS Values

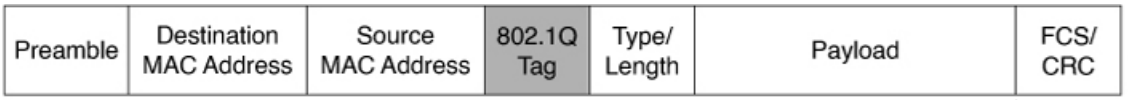
Table 6: Feature History Table

Feature name	Release Information	Feature Description
Preventing IPv6 ND Packet Drops Using CoS (Class of Service) Values	Release 7.3.1	Network policies configured on downstream routers override the CoS value of IPv6 ND packets; the default of the CoS value is CoS 7. You can now explicitly set a CoS value for IPv6 ND packets and prevent them being dropped at service provider networks. The ipv6 nd command includes a new option to enable CoS value setting.

IEEE 802.1Q Tagging and CoS

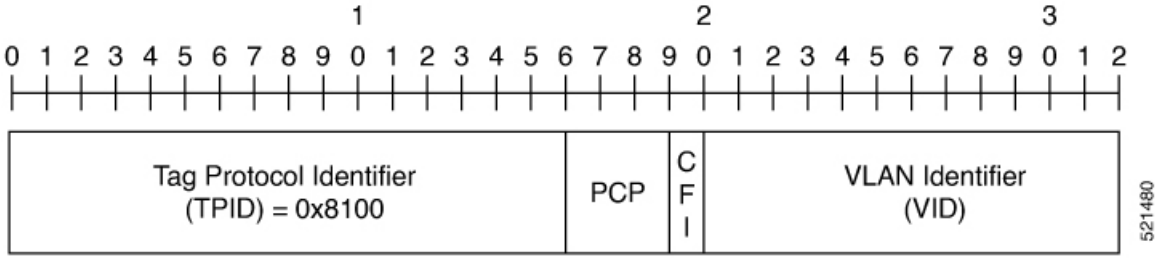
The IEEE 802.1Q specification provides a standards-based mechanism to define VLAN tagging and class of service (CoS) across Ethernet networks. This is accomplished through an additional 4-byte tag, which carries VLAN and frame prioritization information, inserted within the header of a Layer 2 Ethernet frame, as shown in this figure:

Figure 10: Ethernet Frame with IEEE 802.1Q Tag



The 802.1Q Tag has a specific format, consisting of four fixed-length fields. This figure illustrates the 802.1Q tag format:

Figure 11: IEEE 802.1Q Tag Format



In the IEEE 802.1Q Tag Format, the Priority Code Point (PCP) is a 3-bit field that indicates the frame priority level. PCP is defined within the IEEE 802.1p standard and defines eight levels of priority, referred to as CoS values. A common practice is to map different classes of traffic into different CoS values as they are sent across VLANs. Based on these traffic classes, separate queues within network devices that send and receive frames implement traffic prioritization.

Table 1 illustrates the mapping of the CoS value to the bit field. CoS values range from 0 for best-effort packets to 7 for high-priority (network control) packets.

Table 7: CoS Value to PCP Bit Field Mapping

COS Value	Bit Field	Application
CoS 7	111	Reserved (network control)
CoS 6	110	Internetwork control
CoS 5	101	Voice
CoS 4	100	Video Conferencing
CoS 3	011	Call Signaling
CoS 2	010	High Priority packets
CoS 1	001	Medium Priority packets
CoS 0	000	Best-Effort packets

Configuring CoS to override Network Policies

By default, Neighbor Discovery (ND) packets are assigned a CoS value of 7. However, network policies configured in downstream routers can override the CoS value. Therefore, ND packets are dropped. To prevent such overrides, you can explicitly set the CoS value so that ND packets are not dropped by downstream devices.

If you have a network policy configured on a router that drops IPv6 ND packets with the CoS value of 3, make sure that you set the CoS value of IPv6 ND packets to any other value. This ensures that the ND packet are not dropped.

Configuration Example: Set a CoS Value of 2 to prevent ND Packets from dropping

```
/* Enter the global configuration mode. */
Router# configure
```

```
/* Enter the IPv6 ND configuration mode and Configure the IPv6 ND CoS value as 1. */
Router(config)# ipv6 nd cos 1
Router(config)# commit
```

Note For packets that have inner and outer Ethernet frame headers, separate CoS values cannot be set. In the above example, a CoS value of 2 is applied for both inner and outer Ethernet frame headers.

Verification Example

You can use the **show run | inc cos** command to find out the CoS value configured for IPv6 ND packets.

```
Router# show run | inc cos
Thu Feb 18 11:36:22.667 UTC
Building configuration...
ipv6 nd cos 2
```

ICMP for IPv6

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 like 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. 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. MLD is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.

A value of 58 in the Next Header field of the basic IPv6 packet header identifies an IPv6 ICMP packet. ICMP packets in IPv6 are like a transport-layer packet in the sense that the ICMP packet follows all the extension headers and is the last piece of information in the IPv6 packet. Within IPv6 ICMP packets, the ICMPv6 Type and ICMPv6 Code fields identify IPv6 ICMP packet specifics, such as the ICMP message type. The value in the Checksum field is derived (computed by the sender and checked by the receiver) from the fields in the IPv6 ICMP packet and the IPv6 pseudoheader. The ICMPv6 Data field contains error or diagnostic information relevant to IP packet processing.

Address Repository Manager

IPv4 and IPv6 Address Repository Manager (IPARM) enforces the uniqueness of global IP addresses configured in the system, and provides global IP address information dissemination to processes on route processors (RPs) and line cards (LCs) using the IP address consumer application program interfaces (APIs), which includes unnumbered interface information.

Address Conflict Resolution

There are two parts to conflict resolution; the conflict database and the conflict set definition.

Conflict Database

IPARM maintains a global conflict database. IP addresses that conflict with each other are maintained in lists called conflict sets. These conflict sets make up the global conflict database.

A set of IP addresses are said to be part of a conflict set if at least one prefix in the set conflicts with every other IP address belonging to the same set. For example, the following four addresses are part of a single conflict set.

address 1: 10.1.1.1/16

address 2: 10.2.1.1/16

address 3: 10.3.1.1/16

address 4: 10.4.1.1/8

When a conflicting IP address is added to a conflict set, an algorithm runs through the set to determine the highest precedence address within the set.

This conflict policy algorithm is deterministic, that is, the user can tell which addresses on the interface are enabled or disabled. The address on the interface that is enabled is declared as the highest precedence ip address for that conflict set.

The conflict policy algorithm determines the highest precedence ip address within the set.

Multiple IP Addresses

The IPARM conflict handling algorithm allows multiple IP addresses to be enabled within a set. Multiple addresses could potentially be highest precedence IP addresses.

interface GigabitEthernet 0/2/0/0: 10.1.1.1/16

interface GigabitEthernet 0/3/0/0: 10.1.1.2/8

interface GigabitEthernet 0/4/0/0: 10.2.1.1/16

The IP address on GigabitEthernet 0/2/0/0 is declared as highest precedence as per the lowest rack/slot policy and is enabled. However, because the address on interface GigabitEthernet 0/4/0/0 does not conflict with the current highest precedence IP address, the address on GigabitEthernet 0/4/0/0 is enabled as well.

Recursive Resolution of Conflict Sets

In the example below, the address on the interface in GigabitEthernet 0/2/0/0 has the highest precedence because it is the lowest rack/slot. However, now the addresses on GigabitEthernet 0/4/0/0 and GigabitEthernet 0/5/0/0 also do not conflict with the highest precedence IP addresses on GigabitEthernet 0/2/0/0. However, the addresses on GigabitEthernet 0/4/0/0 and GigabitEthernet 0/5/0/0 conflict with each other. The conflict resolution software tries to keep the interface that is enabled as the one that needs to stay enabled. If both interfaces are disabled, the software enables the address based on the current conflict policy. Because GigabitEthernet 0/4/0/0 is on a lower rack/slot, it is enabled.

interface GigabitEthernet 0/2/0/0: 10.1.1.1/16

interface GigabitEthernet 0/3/0/0: 10.1.1.2/8

interface GigabitEthernet 0/4/0/0: 10.2.1.1/16

interface GigabitEthernet 0/5/0/0: 10.2.1.2/16

Route-Tag Support for Connected Routes

The Route-Tag Support for Connected Routes feature that attaches a tag with all IPv4 and IPv6 addresses of an interface. The tag is propagated from the IPv4 and IPv6 management agents (MA) to the IPv4 and IPv6 address repository managers (ARM) to routing protocols, thus enabling the user to control the redistribution

of connected routes by looking at the route tags, by using routing policy language (RPL) scripts. This prevents the redistribution of some interfaces, by checking for route tags in a route policy.

The route tag feature is already available for static routes and connected routes (interfaces) wherein the route tags are matched to policies and redistribution can be prevented.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. Do one of the following:
   - **ipv4 address** *ipv4-address mask* [**secondary**]
4. route-tag *[route-tag value]*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1`	Enters interface configuration mode.
Step 3	Do one of the following: • **ipv4 address** *ipv4-address mask* [**secondary**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.0.0.0`	Specifies a primary (or secondary) IPv4 address address for an interface.

Step 4	route-tag *[route-tag value]*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.0.0.0`
	`route-tag`
	` 100`
		Specifies that the configured address has a route tag to be associated with it. The range for the route-tag value is 1 to 4294967295.

Step 5	**commit**	

IPv4 Inline Fragmentation

When the size of an IPv4 packet leaving the interface (egress) of a router is greater than the MTU value of the interface, the packet gets fragmented before exiting the router.

IPv4 fragmentation is performed on IPv4 packets only when the following conditions are met:

- The `no-DF` bit is set in the header.
- The IPv4 packet is leaving the interface (direction must be egress).
- The egress interface is not configured in a VLAN.
- All egress features are disabled on the egress interface.

When all the preceding conditions are met, the router runs the fragmentation algorithm and fragments the IPv4 packets before sending them out of the egress interface.

How to Implement Network Stack IPv4 and IPv6

This section contains the following procedures:

Assigning IPv4 Addresses to Network Interfaces

This task assigns IPv4 addresses to individual network interfaces.

IPv4 Addresses

A basic and required task for configuring IP is to assign IPv4 addresses to network interfaces. Doing so enables the interfaces and allows communication with hosts on those interfaces using IPv4. An IP address identifies a location to which IP datagrams can be sent. An interface can have one primary IP address and multiple (up to 500) secondary addresses. Packets generated by the software always use the primary IPv4 address. Therefore, all networking devices on a segment should share the same primary network number.

Associated with this task are decisions about subnetting and masking the IP addresses. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a *subnet mask*.

Note Cisco supports only network masks that use contiguous bits that are flush left against the network field.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 address** *ipv4-address mask* [**secondary**]
4. **commit**
5. show ipv4 interface

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1`	Enters interface configuration mode.

Step 3	**ipv4 address** *ipv4-address mask* [**secondary**]
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.0.0.0`
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27/8`
		Specifies a primary or secondary IPv4 address for an interface.
		• The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address.
		• The network mask can be indicated as a slash (/) and a number- a prefix length. 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). A slash must precede the decimal value, and there is no space between the IP address and the slash.

Step 4	**commit**	
Step 5	show ipv4 interface **Example:** `RP/0/RSP0/CPU0:router# show ipv4 interface`	(Optional) Displays the usability status of interfaces configured for IPv4.

IPv4 Virtual Addresses

Configuring an IPv4 virtual address enables you to access the router from a single virtual address with a management network, without the prior knowledge of which route processor (RP) is active. An IPv4 virtual address persists across RP failover situations. For this to happen, the virtual IPv4 address must share a common IPv4 subnet with a Management Ethernet interface on both RPs.

The **vrf** keyword supports virtual addresses on a per-VRF basis.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management applications allow the transport processes (TCP, UDP, raw_ip) to select a suitable source address. The transport processes, in turn, consult the FIB for selecting a suitable source address. If a Management Ethernet's IP address is selected as the source address and if the **use-as-src-addr** keyword is configured, then the transport substitutes the Management Ethernet's IP address with a relevant virtual IP address. This functionality works

across RP switchovers. If the **use-as-src-addr** is not configured, then the source-address selected by transports can change after a failover and the NMS software may not be able to manage this situation.

Note Protocol configuration such as tacacs source-interface, snmp-server trap-source, ntp source, logging source-interface do not use the virtual management IP address as their source by default. Use the **ipv4 virtual address use-as-src-addr** command to ensure that the protocol uses the virtual IPv4 address as its source address. Alternatively, you can also configure a loopback address with the designated or desired IPv4 address and set that as the source for protocols such as TACACS+ via the **tacacs source-interface** command.

Configuring IPv6 Addressing

This task assigns IPv6 addresses to individual router interfaces and enable the forwarding of IPv6 traffic globally on the router. By default, IPv6 addresses are not configured.

Note The *ipv6-prefix* argument in the **ipv6 address** command must be in the form documented in RFC 2373 in which the address is specified in hexadecimal using 16-bit values between colons.

The **/prefix-length** argument in the **ipv6 address** command 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) A slash must precede the decimal value.

The *ipv6-address* argument in the **ipv6 address link-local** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

IPv6 Virtual Addresses

Configuring an IPv6 virtual address enables you to access the router from a single virtual address with a management network, without the prior knowledge of which route processor (RP) is active. An IPv6 virtual address persists across RP failover situations. For this to happen, the virtual IPv6 address must share a common IPv6 subnet with a Management Ethernet interface on both RPs.

The **vrf** keyword supports virtual addresses on a per-VRF basis.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management applications allow the transport processes (TCP, UDP, raw_ip) to select a suitable source address. The transport processes, in turn, consult the FIB for selecting a suitable source address. If a Management Ethernet's IP address is selected as the source address and if the **use-as-src-addr** keyword is configured, then the transport substitutes the Management Ethernet's IP address with a relevant virtual IP address. This functionality works across RP switchovers. If the **use-as-src-addr** is not configured, then the source-address selected by transports can change after a failover and the NMS software may not be able to manage this situation.

Note Protocol configuration such as tacacs source-interface, snmp-server trap-source, ntp source, logging source-interface do not use the virtual management IP address as their source by default. Use the **ipv6 virtual address use-as-src-addr** command to ensure that the protocol uses the virtual IPv6 address as its source address. Alternatively, you can also configure a loopback address with the designated or desired IPv6 address and set that as the source for protocols such as TACACS+ via the **tacacs source-interface** command.

Assigning Multiple IP Addresses to Network Interfaces

This task assigns multiple IP addresses to network interfaces.

Secondary IPv4 Addresses

The Cisco IOS XR software supports multiple IP addresses per interface.

You can specify a maximum of 500 secondary addresses. Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There might not be enough host addresses for a particular network segment. For example, suppose your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you must have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges, and were not subnetted. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can easily be made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. You can create a single network from subnets that are physically separated by another network by using a secondary address. In these instances, the first network is *extended*, or layered on top of the second network. Note that a subnet cannot appear on more than one active interface of the router at a time.

Note If any router on a network segment uses a secondary IPv4 address, all other routers on that same segment must also use a secondary address from the same network or subnet.

Caution Inconsistent use of secondary addresses on a network segment can quickly cause routing loops.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 address** *ipv4-address mask* [**secondary**]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/3`	Enters interface configuration mode.
Step 3	**ipv4 address** *ipv4-address mask* [**secondary**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0 secondary`	Specifies that the configured address is a secondary IPv4 address.
Step 4	**commit**	

Configuring IPv4 and IPv6 Protocol Stacks

This task configures an interface in a Cisco networking device to support both the IPv4 and IPv6 protocol stacks.

When an interface in a Cisco networking device is configured with both an IPv4 and an IPv6 address, the interface forwards both IPv4 and IPv6 traffic—the interface can send and receive data on both IPv4 and IPv6 networks.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 address** *ip-address mask* [**secondary**]
4. **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:**	Specifies the interface type and number, and enters interface configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1`	
Step 3	**ipv4 address** *ip-address mask* [**secondary**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.99.1 255.255.255.0`	Specifies a primary or secondary IPv4 address for an interface.
Step 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:c18:1::3/64`	Specifies the IPv6 address assigned to the interface and enables IPv6 processing on the interface. • A slash mark (/) must precede the *prefix-length* , and there is no space between the *ipv6-prefix* and slash mark.
Step 5	**commit**	

Enabling IPv4 Processing on an Unnumbered Interface

This task enables IPv4 processing on an unnumbered interface.

IPv4 Processing on an Unnumbered Interface

This section describes the process of enabling an IPv4 point-to-point interface without assigning an explicit IP address to the interface. Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the interface you specified as the source address of the IP packet. It also uses the specified interface address in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, and Frame Relay encapsulations can be unnumbered. Serial interfaces using Frame Relay encapsulation can also be unnumbered, but the interface must be a point-to-point subinterface.
- You cannot use the **ping** EXEC command to determine whether the interface is up, because the interface has no IP address. The Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- You cannot support IP security options on an unnumbered interface.
- If you have configured GRE tunnel as IPv4 unnumberered interface then you must also configure a static route. The tunnel cannot reach the peer address if there is no static route configured. Here is the configuration example:

```
interface Loopback 100
ipv4 address 192.0.2.1 255.255.255.252

interface tunnel-ip 100
ipv4 unnumbered Loopback 100
tunnel source 192.0.2.10
keepalive
tunnel destination 192.0.2.11
```

```
router static
address-family ipv4 unicast
  192.0.2.2/32 tunnel-ip 100
```

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered, which allows you to conform with RFC 1195, which states that IP addresses are not required on each interface.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 unnumbered** *interface-type interface-instance*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1`	Enters interface configuration mode.
Step 3	**ipv4 unnumbered** *interface-type interface-instance* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5`	Enables IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface. • The interface you specify must be the name of another interface in the router that has an IP address, not another unnumbered interface. • The interface you specify by the *interface-type* and *interface-instance* arguments must be enabled (listed as "up" in the **show interfaces** command display).
Step 4	**commit**	

Configuring ICMP Rate Limiting

This task explains how to configure IPv4 or IPv6 ICMP rate limiting.

IPv4 ICMP Rate Limiting

The IPv4 ICMP rate limiting feature limits the rate that IPv4 ICMP destination unreachable messages are generated. The Cisco IOS XR software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **DF** keyword is not configured, the **icmp ipv4 rate-limit unreachable** command sets the time values for DF

destination unreachable messages. If the **DF** keyword is configured, its time values remain independent from those of general destination unreachable messages.

IPv6 ICMP Rate Limiting

The IPv6 ICMP rate limiting feature implements a token bucket algorithm for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The initial implementation of IPv6 ICMP rate limiting defined a fixed interval between error messages, but some applications, such as traceroute, often require replies to a group of requests sent in rapid succession. The fixed interval between error messages is not flexible enough to work with applications such as traceroute and can cause the application to fail. Implementing a token bucket scheme allows a number of tokens—representing the ability to send one error message each—to be stored in a virtual bucket. The maximum number of tokens allowed in the bucket can be specified, and for every error message to be sent, one token is removed from the bucket. If a series of error messages is generated, error messages can be sent until the bucket is empty. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket. The token bucket algorithm does not increase the average rate limiting time interval, and it is more flexible than the fixed time interval scheme.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
   - **icmp ipv4 rate-limit unreachable** [**DF**] *milliseconds*
   - **ipv6 icmp error-interval** *milliseconds* [*bucketsize*]
3. **commit**
4. Do one of the following:
   - **show ipv4 traffic** [**brief**]
   - **show ipv6 traffic** [**brief**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	Do one of the following:
	• **icmp ipv4 rate-limit unreachable** [**DF**] *milliseconds*
	• **ipv6 icmp error-interval** *milliseconds* [*bucketsize*]
	Example:
	`RP/0/RSP0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 1000`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 icmp error-interval 50 20`
		Limits the rate that IPv4 ICMP destination unreachable messages are generated.
		• The **DF** keyword limits the rate at which ICMP destination unreachable messages are sent when code 4 fragmentation is needed and Data Fragmentation (DF) is set, as specified in the IP header of the ICMP destination unreachable message.
		• The *milliseconds* argument specifies the time period between the sending of ICMP destination unreachable messages.
		or

	Command or Action	Purpose
		Configures the interval and bucket size for IPv6 ICMP error messages. • The *milliseconds* argument specifies the interval between tokens being added to the bucket. • The optional *bucketsize* argument defines the maximum number of tokens stored in the bucket.
Step 3	**commit**	

Step 4	Do one of the following:
	• **show ipv4 traffic** [**brief**]
	• **show ipv6 traffic** [**brief**]
	Example:
	`RP/0/RSP0/CPU0:router# show ipv4 traffic`
	or
	`RP/0/RSP0/CPU0:router# show ipv6 traffic`
		(Optional) Displays statistics about IPv4 traffic, including ICMP unreachable information.
		• Use the **brief** keyword to display only IPv4 and ICMPv4 traffic statistics.
		or
		(Optional) Displays statistics about IPv6 traffic, including IPv6 ICMP rate-limited counters.
		• Use the **brief** keyword to display only IPv6 and ICMPv6 traffic statistics.

Configuring IPARM Conflict Resolution

This task sets the IP Address Repository Manager (IPARM) address conflict resolution parameters.

Static Policy Resolution

The static policy resolution configuration prevents new address configurations from affecting interfaces that are currently running.

Note When you configure duplicate IP addresses of interfaces on a device and also configure the command ipv4 conflict-policy static, the duplicate interface remains down. However, this configuration is applicable only on ethernet interfaces and not on Point-to-Point (PPP) interfaces and Cisco ASR 9000 Series SPA Interface Processor-700 (SIP-700).

SUMMARY STEPS

1. **configure**
2. {**ipv4** | **ipv6**} **conflict-policy static**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	{**ipv4** | **ipv6**} **conflict-policy static**
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 conflict-policy static`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 conflict-policy static`
		Sets the conflict policy to static, that is, prevents new interface addresses from affecting the currently running interface.

Step 3	**commit**	

Longest Prefix Address Conflict Resolution

This conflict resolution policy attempts to give highest precedence to the IP address that has the longest prefix length.

SUMMARY STEPS

1. **configure**
2. **{ ipv4** | **ipv6 } conflict-policy longest-prefix**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**{ ipv4** | **ipv6 } conflict-policy longest-prefix**
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 conflict-policy longest-prefix`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 conflict-policy longest-prefix`
		Sets the conflict policy to longest prefix, that is, all addresses within the conflict set that don't conflict with the longest prefix address of the currently running interface are allowed to run as well.

Step 3	**commit**	

Highest IP Address Conflict Resolution

This conflict resolution policy attempts to give highest precedence to the IP address that has the highest value.

SUMMARY STEPS

1. **configure**
2. **{ ipv4 | ipv6 } conflict-policy highest-ip**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**{ ipv4 | ipv6 } conflict-policy highest-ip**
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 conflict-policy highest-ip`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 conflict-policy highest-ip`
		Sets the conflict policy to the highest IP value, that is, the IP address with the highest value gets precedence.

Step 3	**commit**	

Generic Routing Encapsulation

The Generic Routing Encapsulation (GRE) tunneling protocol provides a simple, and generic approach for transporting packets of one protocol over another protocol by means of encapsulation. The packet that needs to be transported is first encapsulated in a GRE header, which is further encapsulated in another protocol like IPv4 or IPv6; and the packet is then forwarded to the destination.

A typical GRE-encapsulated packet includes:

- The delivery header
- The GRE header
- The payload packet

A payload packet is a packet that a system encapsulates and delivers to a destination. The payload is first encapsulated in a GRE packet. The resulting GRE packet can then be encapsulated in another outer protocol and then forwarded. This outer protocol is called the delivery protocol.

Note

- When IPv4 is being carried as the GRE payload, the Protocol Type field must be set to 0x800.
- When IPv6 is being carried as the GRE payload, the Protocol Type field must be set to 0x86DD.

IPv4/IPv6 Forwarding over GRE Tunnels

Packets that are tunneled over GRE tunnels enter the router as normal IP packets. The packets are forwarded (routed) using the destination address of the IP packet. In the case of Equal Cost Multi Path (ECMP) scenarios, an output interface-adjacency is selected, based on a platform-specific L3 load balance (LB) hash. Once the egress physical interface is known, the packet is sent out of that interface, after it is first encapsulated with GRE header followed by the L2 rewrite header of the physical interface. After the GRE encapsulated packet reaches the remote tunnel endpoint router, the GRE packet is decapsulated. The destination address lookup of the outer IP header (this is the same as the tunnel destination address) will find a local address (receive) entry on the ingress line card.

The first step in GRE decapsulation is to qualify the tunnel endpoint, before admitting the GRE packet into the router, based on the combination of tunnel source (the same as source IP address of outer IP header) and tunnel destination (the same as destination IP address of outer IP header). If the received packet fails tunnel admittance qualification check, the packet is dropped by the decapsulation router. On successful tunnel admittance check, the decapsulation strips the outer IP and GRE header off the packet, then starts processing the inner payload packet as a regular packet.

When a tunnel endpoint decapsulates a GRE packet, which has an IPv4/IPv6 packet as the payload, the destination address in the IPv4/IPv6 payload packet header is used to forward the packet, and the TTL of the payload packet is decremented. Care should be taken when forwarding such a packet. If the destination address of the payload packet is the encapsulator of the packet (that is the other end of the tunnel), looping can occur. In such a case, the packet must be discarded.

IPv6 forwarding over GRE tunnels

IPv6 forwarding over GRE is accomplished by IPv6 forwarding over IPv4 GRE tunnels. The functionality is similar to the IPv4 forwarding over GRE tunnels (as described above). In the case of IPv6, the FIM (Forward Information Base) module needs to confirm if the forwarding chain is correctly setup both in slowpath and hardware to send the IPv6 packet as a payload of IPv4 GRE encapsulated packet.

TCP MSS Adjustment

The TCP Maximum Segment Size (MSS) Adjustment feature allows the configuration of Maximum Segment Size (MSS) on transient packets that traverse a router. TCP MSS Adjustment is used on a GRE tunnel interface or VLAN sub-interface on a physical Ethernet interface on ASR 9000 Enhanced Ethernet Line Card to enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established. It needs to be configurable, for a single tunnel interface or VLAN sub-interface, to a specific value.

This feature is supported for transit IPv4 and IPv6 packets only. It applies to both ingress and egress traffic on interfaces where the TCP MSS adjustment is configured. In this release, a configuration of **ipv4 tcp-mss-adjust enable** or **ipv6 tcp-mss-adjust enable** or both commands on an interface will have the same

effect. It applies to all TCP SYNC packets encapsulated in an IPv4 or IPv6 frame, coming in and going out of the interface.

Configuring TCP MSS for IPv4 packets

This task describes how to enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv4 packets.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 tcp-mss-adjust enable**
4. **commit**
5. **exit**
6. **hw-module location** *type interface-path-id* **tcp-mss-adjust np** *number* **value** *number*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0.100`	Enters interface configuration mode and configures an interface.
Step 3	**ipv4 tcp-mss-adjust enable** **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 tcp-mss-adjust enable`	Enable the modification of TCP Maximum Segment Size (MSS) in TCP handshake on the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv4 packets.
Step 4	**commit**	
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits interface configuration mode and returns to configuration mode.
Step 6	**hw-module location** *type interface-path-id* **tcp-mss-adjust np** *number* **value** *number* **Example:**	Configure the TCP MSS value. Only one value per network processor (NP) can be configured.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# hw-module location 0/0/CPU0 tcp-mss-adjust np 1 value 1300`	
Step 7	**commit**	

Configuring TCP MSS for IPv6 packets

This task describes how to enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv6 packets.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv6 tcp-mss-adjust enable**
4. **commit**
5. **exit**
6. **hw-module location** *type interface-path-id* **tcp-mss-adjust np** *number* **value** *number*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0.100`	Enters interface configuration mode and configures an interface.
Step 3	**ipv6 tcp-mss-adjust enable** **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv6 tcp-mss-adjust enable`	Enable the modification of TCP Maximum Segment Size (MSS) in TCP handshake on the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv4 packets.
Step 4	**commit**	
Step 5	**exit** **Example:**	Exits interface configuration mode and returns to configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-if)# exit`	
Step 6	**hw-module location** *type interface-path-id* **tcp-mss-adjust np** *number* **value** *number* **Example:** `RP/0/RSP0/CPU0:router(config)# hw-module location 0/0/CPU0 tcp-mss-adjust np 1 value 1300`	Configure the TCP MSS value. Only one value per network processor (NP) can be configured.
Step 7	**commit**	

Configuration Examples for Implementing Network Stack IPv4 and IPv6

This section provides the following configuration examples:

Assigning an Unnumbered Interface: Example

In the following example, the second interface (GigabitEthernet 0/1/0/1) is given the address of loopback interface 0. The loopback interface is unnumbered.

```
interface loopback 0
 ipv4 address 192.168.0.5 255.255.255.0
interface gigabitethernet 0/1/0/1
 ipv4 unnumbered loopback 0
```

Additional References

The following sections provide references related to implementing Network Stack IPv4 and IPv6.

Related Documents

Related Topic	Document Title
Address resolution configuration tasks	*Configuring ARP* module in this publication.
Mapping host names to IP addresses	*Host Services and Applications Commands* module in the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
Network stack IPv4 and IPv6 commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Network Stack IPv4 and IPv6 Commands* section in the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

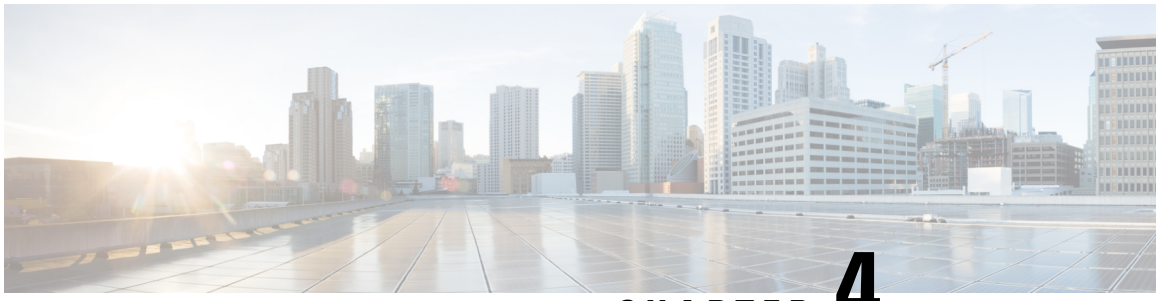
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 4

Implementing ARP

Address resolution is the process of mapping network addresses to Media Access Control (MAC) addresses. This process is accomplished using the Address Resolution Protocol (ARP). This module describes how to configure ARP processes on the Cisco ASR 9000 Series Aggregation Services Router.

Note For a complete description of the ARP commands listed in this module, refer to the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Feature History for Configuring ARP

Release	Modification
Release 3.7.2	This feature was introduced.

Prerequisites for Configuring ARP

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for Configuring ARP

The following restrictions apply to configuring ARP :

- Reverse Address Resolution Protocol (RARP) is not supported.

- Due to a hardware limitation in the Ethernet SPA interfaces installed on all routers, when a packet contains a wrong destination address, the corresponding SPA drops the packet even if the ingress packet count is already incremented in the output of the **show interfaces** command.

The following additional restrictions apply when configuring the Direct Attached Gateway Redundancy (DAGR) feature on Cisco ASR 9000 Series Routers:

- IPv6 is not supported.
- Ethernet bundles are not supported.
- Non-Ethernet interfaces are not supported.
- Hitless ARP Process Restart is not supported.
- Hitless RSP Failover is not supported.

Information About Configuring ARP

To configure ARP, you must understand the following concepts:

IP Addressing Overview

A device in the IP can have both a local address (which uniquely identifies the device on its local segment or LAN) and a network address (which identifies the network to which the device belongs). The local address is more properly known as a *data link address*, because it is contained in the data link layer (Layer 2 of the OSI model) part of the packet header and is read by data-link devices (bridges and all device interfaces, for example). The more technically inclined person will refer to local addresses as *MAC addresses*, because the MAC sublayer within the data link layer processes addresses for the layer.

To communicate with a device on Ethernet, for example, Cisco IOS XR software first must determine the 48-bit MAC or local data-link address of that device. The process of determining the local data-link address from an IP address is called *address resolution*.

Address Resolution on a Single LAN

The following process describes address resolution when the source and destination devices are attached to the same LAN:

1. End System A broadcasts an ARP request onto the LAN, attempting to learn the MAC address of End System B.
2. The broadcast is received and processed by all devices on the LAN, including End System B.
3. Only End System B replies to the ARP request. It sends an ARP reply containing its MAC address to End System A.
4. End System A receives the reply and saves the MAC address of End System B in its ARP cache. (The ARP cache is where network addresses are associated with MAC addresses.)
5. Whenever End System A needs to communicate with End System B, it checks the ARP cache, finds the MAC address of System B, and sends the frame directly, without needing to first use an ARP request.

Address Resolution When Interconnected by a Router

The following process describes address resolution when the source and destination devices are attached to different LANs that are interconnected by a router (only if proxy-arp is turned on):

1. End System Y broadcasts an ARP request onto the LAN, attempting to learn the MAC address of End System Z.
2. The broadcast is received and processed by all devices on the LAN, including Router X.
3. Router X checks its routing table and finds that End System Z is located on a different LAN.
4. Router X therefore acts as a proxy for End System Z. It replies to the ARP request from End System Y, sending an ARP reply containing its own MAC address as if it belonged to End System Z.
5. End System Y receives the ARP reply and saves the MAC address of Router X in its ARP cache, in the entry for End System Z.
6. When End System Y needs to communicate with End System Z, it checks the ARP cache, finds the MAC address of Router X, and sends the frame directly, without using ARP requests.
7. Router X receives the traffic from End System Y and forwards it to End System Z on the other LAN.

ARP and Proxy ARP

Two forms of address resolution are supported by Cisco IOS XR software: Address Resolution Protocol (ARP) and proxy ARP, as defined in RFC 826 and RFC 1027, respectively. Cisco IOS XR software also supports a form of ARP called local proxy ARP.

ARP is used to associate IP addresses with media or MAC addresses. Taking an IP address as input, ARP determines the associated media address. After a media or MAC address is determined, the IP address or media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network.

When proxy ARP is disabled, the networking device responds to ARP requests received on an interface only if one of the following conditions is met:

- The target IP address in the ARP request is the same as the interface IP address on which the request is received.
- The target IP address in the ARP request has a statically configured ARP alias.

When proxy ARP is enabled, the networking device also responds to ARP requests that meet all the following conditions:

- The target IP address is not on the same physical network (LAN) on which the request is received.
- The networking device has one or more routes to the target IP address.
- All of the routes to the target IP address go through interfaces other than the one on which the request is received.

When local proxy ARP is enabled, the networking device responds to ARP requests that meet all the following conditions:

- The target IP address in the ARP request, the IP address of the ARP source, and the IP address of the interface on which the ARP request is received are on the same Layer 3 network.
- The next hop for the target IP address is through the same interface as the request is received.

Typically, local proxy ARP is used to resolve MAC addresses to IP addresses in the same Layer 3 network such as, private VLANs that are Layer 2-separated. Local proxy ARP supports all types of interfaces supported by ARP and unnumbered interfaces.

ARP Cache Entries

ARP establishes correspondences between network addresses (an IP address, for example) and Ethernet hardware addresses. A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

You can also add a static (permanent) entry to the ARP cache that persists until expressly removed.

From Release 6.5.1 onwards, the supported ARP scale has been increased from 128K to 256K entries per LC CPU. This increase in scale improves performance while multiple ARP operations are being processed on the device.

Direct Attached Gateway Redundancy

Direct Attached Gateway Redundancy (DAGR) allows third-party redundancy schemes on connected devices to use gratuitous ARP as a failover signal, enabling the ARP process to advertise an new type of route in the Routing Information Base (RIB). These routes are distributed by Open Shortest Path First (OSPF).

Sometimes part of an IP network requires redundancy without routing protocols. A prime example is in the mobile environment, where devices such as base station controllers and multimedia gateways are deployed in redundant pairs, with aggressive failover requirements (subsecond or less), but typically do not have the capability to use native Layer 3 protocols such as OSPF or Intermediate System-to-Intermediate System (IS-IS) protocol to manage this redundancy. Instead, these devices assume they are connected to adjacent IP devices over an Ethernet switch, and manage their redundancy at Layer 2, using proprietary mechanisms similar to Virtual Router Redundancy Protocol (VRRP). This requires a resilient Ethernet switching capability, and depends on mechanisms such as MAC learning and MAC flooding.

DAGR is a feature that enables many of these devices to connect directly to Cisco ASR 9000 Series Routers without an intervening Ethernet switch. DAGR enables the subsecond failover requirements to be met using a Layer 3 solution. No MAC learning, flooding, or switching is required.

Note Since mobile devices' 1:1 Layer 2 redundancy mechanisms are proprietary, they do not necessarily conform to any standard. So although most IP mobile equipment is compatible with DAGR, interoperability does require qualification, due to the possibly proprietary nature of the Layer 2 mechanisms with which DAGR interfaces.

Additional Guidelines

The following are additional guidelines to consider when configuring DAGR:

- Up to 40 DAGR peers, which may be on the same or different interfaces, are supported per system.

- Failover is supported for DAGR routes within 500 ms of receipt of an ARP reply packet.
- On ARP process restart, DAGR groups are reinitialized.

How to Configure ARP

This section contains instructions for the following tasks:

Defining a Static ARP Cache Entry

ARP and other address resolution protocols provide a dynamic mapping between IP addresses and media addresses. Because most hosts support dynamic address resolution, generally you need not to specify static ARP cache entries. If you must define them, you can do so globally. Performing this task installs a permanent entry in the ARP cache. Cisco IOS XR software uses this entry to translate 32-bit IP addresses into 48-bit hardware addresses.

Note From Release 6.5.1 onwards, the supported ARP scale has been increased from 128K to 256K entries per LC CPU. This increase in scale improves performance while multiple ARP operations are being processed on the device.

Optionally, you can specify that the software responds to ARP requests as if it were the owner of the specified IP address by making an alias entry in the ARP cache.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
   - **arp** [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type*
   - **arp** [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type* **alias**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	Do one of the following: • **arp** [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type*	Creates a static ARP cache entry associating the specified 32-bit IP address with the specified 48-bit hardware address.

	Command or Action	Purpose

	• **arp** [**vrf** *vrf-name*] *ip-address hardware-address encapsulation-type* **alias**
	Example:
	`RP/0/RSP0/CPU0:router(config)# arp 192.168.7.19 0800.0900.1834 arpa`
	or
	`RP/0/RSP0/CPU0:router(config)# arp 192.168.7.19 0800.0900.1834 arpa alias`
		Note If an **alias** entry is created, then any interface to which the entry is attached will act as if it is the owner of the specified addresses, that is, it will respond to ARP request packets for this network layer address with the data link layer address in the entry.

Step 3	**commit**	

Enabling Proxy ARP

Cisco IOS XR software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data-link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is disabled by default; this task describes how to enable proxy ARP if it has been disabled.

SUMMARY STEPS

1. **configure**
2. **interface** *type number*
3. proxy-arp
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type number* **Example:** `RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0/CPU0/0`	Enters interface configuration mode.
Step 3	proxy-arp **Example:** `RP/0/RSP0/CPU0:router(config-if)# proxy-arp`	Enables proxy ARP on the interface.

	Command or Action	Purpose
Step 4	**commit**	

Enabling Local Proxy ARP

Local proxy ARP is disabled by default; this task describes how to enable local proxy ARP.

SUMMARY STEPS

1. **configure**
2. **interface** *type number*
3. **local-proxy-arp**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type number* **Example:** `RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/0/0/0`	Enters interface configuration mode.
Step 3	**local-proxy-arp** **Example:** `RP/0/RSP0/CPU0:router(config-if)# local-proxy-arp`	Enables local proxy ARP on the interface.
Step 4	**commit**	

Configuring DAGR

Follow these steps to create a DAGR group on the Cisco ASR 9000 Series Router.

SUMMARY STEPS

1. configure
2. **interface** *type interface-path-id*
3. arp dagr
4. **peer ipv4** *address*
5. **route distance normal** *normal- distance* **priority** *priority-distance*
6. **route metric normal** *normal- metric* **priority** *priority-metric*
7. **timers query** *query-time* **standby** *standby-time*

8. **priority-timeout** *time*
9. Do one of the following:
   - end
   - commit
10. **show arp dagr** [*interface* [*IP-address*]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	Enters interface configuration mode and configures an interface.
Step 3	arp dagr **Example:** `RP/0/RSP0/CPU0:router(config-if)# arp dagr`	Enters DAGR configuration mode.
Step 4	**peer ipv4** *address* **Example:** `RP/0/RSP0/CPU0:router(config-if-dagr)# peer ipv4 10.0.0.100`	Creates a new DAGR group for the virtual IP address.
Step 5	**route distance normal** *normal- distance* **priority** *priority-distance* **Example:** `RP/0/RSP0/CPU0:router(config-if-dagr-peer)# route distance normal 140 priority 3`	(Optional) Configures route distance for the DAGR group.
Step 6	**route metric normal** *normal- metric* **priority** *priority-metric* **Example:** `RP/0/RSP0/CPU0:router(config-if-dagr-peer)# route metric normal 84 priority 80`	(Optional) Configures the route metric for the DAGR group.

	Command or Action	Purpose
Step 7	**timers query** *query-time* **standby** *standby-time* **Example:** `RP/0/RSP0/CPU0:router(config-if-dagr-peer)# timers query 2 standby 19`	(Optional) Configures the time in seconds between successive ARP requests being sent out for the virtual IP address.
Step 8	**priority-timeout** *time* **Example:** `RP/0/RSP0/CPU0:router(config-if-dagr-peer)# priority-timeout 25`	(Optional) Configures a timer for the length of time in seconds to wait before reverting to normal priority from a high-priority DAGR route.

Step 9	Do one of the following:
	• end
	• commit
	Example:
	`RP/0/RSP0/CPU0:router(config-if-dagr)# end`
	or
	`RP/0/RSP0/CPU0:router(config-if-dagr)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 10	**show arp dagr** [*interface* [*IP-address*]] **Example:** `RP/0/RSP0/CPU0:router# show arp dagr`	(Optional) Displays the operational state of all DAGR groups. Using the optional *interface* and *IP-address* arguments restricts the output to a specific interface or virtual IP address.

Configuring ARP purge-delay

With Equal Cost Multi Path (ECMP), traffic is load balanced across multiple paths with equal cost. This should provide resiliency against interface flaps. If an interface goes down, the traffic is then routed via the other interface without traffic loss. However, if the first interface comes up, traffic is routed back over it but

forwarding will only resume once ARP has been (re)resolved and the adjcency (re)installed. Here a short unexpected interface flap causes this traffic loss and is particularly undesirable.

The purge-delay feature allows existing dynamic entries to persist rather than immediately delete entries which could cause traffic loss following an interface flap.

The purge delay feature works by caching existing dynamic ARP entries when an interface goes down and starting a purge delay timer. When the interface is brought back and the purge delay timer not yet fired, the entries are reinstalled as before. The normal entry timeout is reduced in order to re-ARP for the entries after any interface state change related churn has died down; should the purge delay timer fire before the interface comes back up, the entries are deleted from the cache.

SUMMARY STEPS

1. **configure**
2.
3.
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**Example:** `RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0`	Enters interface configuration mode.
Step 3	**Example:** `RP/0/RSP0/CPU0:router(config-if)# arp purge-delay 100`	Sets the purge delay time interval.
Step 4	**commit**	

Configuring ARP timeout

Dynamic ARP entries which are learnt by ARP address resolution (when valid ARP replies are received) are timed out every 4 hours by default in order to remove stale entries.

ARP entries that correspond to the local interface or that are statically configured by the user never time out.

SUMMARY STEPS

1.
2.
3.
4. Do one of the following:

- end
- commit

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**Example:** `RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RSP0`	Enters interface configuration mode.
Step 3	**Example:** `RP/0/RSP0/CPU0:router(config-if)# arp timeout 100`	Sets the ARP cache timeout interval.

Step 4	Do one of the following:
	• end
	• commit
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# end`
	or
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configure Learning of Local ARP Entries

You can configure an interface or a sub-interface to learn only the ARP entries from its local subnet.

Note From Release 6.5.1 onwards, the supported ARP scale has been increased from 128K to 256K entries per LC CPU. This increase in scale improves performance while multiple ARP operations are being processed on the device.

Use the following procedure to configure local ARP learning on an interface.

1. Enter the interface configuration mode.

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

2. Configure the IPv4/IPv6 address for the interface.

```
Router(config-if)# ipv4 address 12.1.3.4 255.255.255.0
```

3. Configure local ARP learning on the interface.

```
Router(config-if)# arp learning local
```

4. Enable the interface and commit your configuration.

```
Router(config-if)# no shut
Router(config-if)# commit
RP/0/0/CPU0:Dec 12 13:41:16.580 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : interface
GigabitEthernet 0/0/0/1, changed state to Down
RP/0/0/CPU0:Dec 12 13:41:16.683 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : interface
GigabitEthernet 0/0/0/1 changed state to Up
```

5. Confirm your configuration.

```
Router(config-if)# show running-configuration
..
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Mon Dec 12 13:41:16 2016
!interface GigabitEthernet 0/0/0/1
 ipv4 address 12.1.3.4 255.255.255.0
 arp learning local
!
```

6. Verify if local ARP learning is working as configured on the interface.

```
Router(config-if)# do show arp idb gigabitEthernet 0/1/0/0 location 0/1/CPU0
Mon Nov 26 14:09:38.898 IST

interface GigabitEthernet 0/1/0/0 (0x00804060):
  IDB Client: default
  IPv4 address 1.1.1.1, Vrf ID 0x60000000
  VRF Name default
  Dynamic learning: Enable
  Dynamic entry timeout: 14400 secs
  Drop adjacency timeout: 3600 secs
  Purge delay: off
  IPv4 caps added (state up)
  MPLS caps not added
  Interface not virtual, not client fwd ref,
  Proxy arp not configured, not enabled
  Local Proxy arp not configured
  Packet IO layer is SPIO
  Srg Role : DEFAULT
  Idb Flag : 49292
  IDB is Complete
  IDB Flag Description:
```

```
[CAPS | COMPLETE | IPV4_CAPS_CREATED | SPIO_ATTACHED |
 SPIO_SUPPORTED]
```

7. (Optional) You can monitor the ARP traffic on the interface.

```
Router(config-if)# do show arp traffic gigabitEthernet 0/1/0/0 location 0/1/CPU0
Mon Nov 26 14:08:34.403 IST

ARP statistics:
  Recv: 0 requests, 0 replies (0 unsolicited)
  Sent: 5 requests, 1 replies (0 proxy, 0 local proxy, 1 gratuitous)
  Subscriber Interface:
         0 requests recv, 0 replies sent, 0 gratuitous replies sent
  Resolve requests rcvd: 1
  Resolve requests dropped: 0
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 2
  Dynamic: 0, Interface: 1, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0,    DropAdj: 1

  IP Packet drop count for GigabitEthernet0_1_0_0: 1
```

Limit ARP Cache Entries per Interface

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
Limit Address Resolution Protocol (ARP) Cache Entries per Interface	Release 7.9.1	In this feature, you can configure the maximum limit for the number of entries of dynamic mapping between IP addresses and media addresses by ARP per interface. Limiting the number of entries provides overflow protections in ARP cache and protects the routers from DOS attacks by preventing memory overuse by cache entries. This feature introduces the **arp cache-limit** command.

The ARP cache overflow occurs when the number of entries in the cache exceeds the maximum limit value of 127999. Such instances make the router vulnerable to threats like DOS attacks. With this feature, you can configure the maximum limit of dynamic ARP entries learned per interface. The router won't accept any cache entries unless cleared after the number entries exceeds the maximum limit in the configuration. You can configure the maximum limit range of 0–127999 per interfaces in the router.

Note The arp cache resources vary depending on the hardware resources available in a router. Ensure the cache-limit configured such that the available resources in the router are able to accomodate the entries.

Feature highlights

This section details the good to know information for using ARP overflow protection:

- The router drops new ARP requests when the number of entries are more than or equal to the applied cache limit value.
- The router won't learn from ARP packets received after exceeding the applied cache limit value.
- The ARP cache limit isn't applicable to static ARP entries.
- The router doesn't enforce the ARP cache limit on ARP client triggered entries.
- The router issues a syslog message when it reaches the cache limit. For every 1000 entries after the cache limit, the router issues a new syslog message. The syslog message includes the interface name and cache entries drop counters. For example, `RP/0/RP0/CPU0:Jul 1 10:10:25.781 IST: grid_svr[211]: %L2-GRID-4-BANK_FULL : GRID POOL:GLIF(2), BANK 0 FULL. Max size 4091, Curr RIDs 4091.`
- You can view the ARP entries statistics using the **show arp idb** command.
- The ARP Cache limit doesn't drops the already learned dynamic ARP entries. That is, if the number of dynamic ARP entries in the cache is higher or equal to the newer cache limit set in the router, then the router will neither take any new entries or drop the preexisting entries in the cache, but it will start issuing the syslog message the cache limit.

Configuration Example

The following example shows how to set the ARP cache limit for an interface:

Configuration

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/0
Router(config-if)#arp cache-limit 3900
Router(config-if)#commit
```

Running Configuration

```
Router# show running-config interface HundredGigE 0/0/0/0
interface HundredGigE0/0/0/0
 arp cache-limit 3900
 !
!
```

Verification

```
Router#show arp idb HundredGigE 0/0/0/0 location RP0
HundredGigE (0x00000090):
  IDB Client: default
  IPv4 address 1.1.1.1, Vrf ID 0x60000000
  VRF Name default
  Dynamic learning: Enable
  Dynamic entry timeout: 14400 secs
  Drop adjacency timeout: Disable
  Purge delay: off
  Cache limit: 3900
  Incomplete glean count: 0
  Complete glean count: 0
  Complete protocol count: 0
  Dropped glean count: 0
```

```
Dropped protocol count: 0
IPv4 caps added (state up)
MPLS caps not added
Interface is virtual, not client fwd ref,
Proxy arp not configured, not enabled
Local Proxy arp not configured
Packet IO layer is SPIO
Srg Role : DEFAULT
Idb Flag : 49294
IDB is Complete
IDB Flag Description:
[VIRTUAL | CAPS | COMPLETE | IPV4_CAPS_CREATED |
 SPIO_ATTACHED | SPIO_SUPPORTED]
Idb Flag Ext : 0x0
Idb Oper Progress : NONE
Client Resync Time : N/A
```

Configuration Examples for ARP Configuration on Cisco IOS XR Software

This section provides the following ARP configuration examples:

Creating a Static ARP Cache Entry: Example

The following is an example of a static ARP entry for a typical Ethernet host:

```
configure
arp 192.168.7.19 0800.0900.1834 arpa
```

The following is an example of a static ARP entry for a typical Ethernet host where the software responds to ARP requests as if it were the owner of both the specified IP address and hardware address, whether proxy ARP is enabled or not:

```
configure
arp 192.168.7.19 0800.0900.1834 arpa alias
```

The following is an example of configuring a static arp entry on an SRP device:

```
configure
arp 192.168.8.20 0800.0900.1723 srp
```

Enabling Proxy ARP: Example

The following is an example of enabling proxy ARP:

```
configure
interface MgmtEth 0/
RSP0


/CPU0/0
proxy-arp
```

Displaying the ARP Table: Example

The following example shows how to display the ARP table:

```
Router# show arp

------------------------------------------------------------------------------
0/1/CPU0
------------------------------------------------------------------------------
Address         Age        Hardware Addr   State      Type  Interface
1.1.1.1         -          027d.42e9.bd36  Interface  ARPA  GigabitEthernet0/1/0/0
1.1.1.2         00:00:06   0000.0000.0000  DropAdj    ARPA  GigabitEthernet0/1/0/0
```

Enabling DAGR and Configuring a DAGR Group: Example

The following is an example of enabling DAGR and configuring a DAGR group peer:

```
configure
 interface gigabitethernet 0/1/0/0.1
  arp dagr
   peer ipv4 192.168.7.19
    priority-timeout 25
    route distance normal 48 priority 5
    route metric normal 48 priority 5
    timers query 2 standby 40
    commit
```

Displaying the Operational State of DAGR Groups: Example

The following example shows how to display the current operational state of the DAGR groups:

```
RP/0/RSP0/CPU0:router# show arp dagr
-------------------------------------------------------------------------------
0/1/CPU0
-------------------------------------------------------------------------------
Interface                Virtual IP      State     Query-pd Dist Metr
GigabitEthernet0/1/0/2     10.168.7.19    Active    None     150  100
GigabitEthernet0/1/0/2     10.24.0.45     Query     1        None None
GigabitEtherget0/1/0/3     10.66.0.45     Init      None     None None
```

Policing Duplicate ARP Packets: Example

This example sets the police interval within which the duplicate ARP packets from the same sender protocol address (IP) or same source MAC address are policed:

```
configure
arp police-interval 34
```

ARP Policer Behaviour

- When the **arp police-interval** command is configured, ARP requests coming from the same IP address or MAC address within the configured interval are dropped.

- If there was an ARP response existing for the ARP request from the same IP address within the configured interval, the new request will be dropped.
- If the ARP response was not existing already for the ARP request from the same IP address, then the MAC policer will be checked.

ARP Throttling

When remote devices scan for destinations that do not exist in the locally connected network, the packets with unresolved ARP requests causes continuous queue of ARP packets pending for resolution. Failed ARP resolution entries impacts forwarding and performance of the router because CPU cycles are consumed when packets are sent for ARP resolution continuously. ARP throttling prevents unresolved packet queuing at the first hop counter for ARP resolution by adding drop adjacencies for such destinations. A router drops packets for which drop adjacency entries are added. Packets for which adjacency entries are added are forwarded to the next hop. Adjacency and drop adjacency entries are added for destinations in the ARP table of every router that forwards traffic.

You can enable ARP throttling for an interface of any router that forwards traffic to the next hop. If ARP resolution fails for any packet on that interface, that packet is added as an entry for drop adjacency in the forwarding plane of the router for a specified period of timeout value. Therefore, until the configured value of timeout gets over, the traffic hitting drop adjacency is dropped at the router where ARP throttling is configured and the packets are not queued up for ARP. Timeout value is configured in seconds. The default timeout value is 1 hour or 3600 seconds. Once timeout is over for the drop adjacency, ARP deletes the drop adjacency entry from the ARP database of the router. ARP also sends a message to Adjacency Information Base (AIB) to delete it. AIB is a database of adjacencies that are learned from the ARP database and AIB provides information to Forwarding Information Base (FIB) that has a database of adjacencies and static routes. Static routes are configuration based and resides in Routing Information Base (RIB) that is linked to the FIB.

Restrictions

- You can configure ARP throttling only on interfaces and not on nodes.
- The entries for drop adjacencies are not retained in the ARP database if there is an interface flap.

Configuration Example

To configure ARP throttling on an interface with specified timeout for drop adjacency, complete the following configurations:

1. Enter interface configuration mode.
2. Configure ARP throttling on the interface for a specified timeout period for drop adjacency.

Configuration

```
/* Enter the global configuration mode and configure an interface */
Router# config
Router(config)# interface GigabitEthernet 0/1/0/0

/* Configure ARP throttling on the interface with specified timeout for drop adjacency. */
Router(config-if)# arp drop-adjacency timeout 1200
Router(config-if)# commit
```

Verification

To verify the drop adjacencies in the ARP database with respect to interfaces, use the **show arp** command. To verify the drop adjacency traffic statistics in the ARP cache, use the **show arp traffic** command.

To verify the different types of adjacencies on a router's interface, use the **show adjacency summary** command:

```
 Router# show adjacency summary location 0/1/CPU0
Mon Nov 26 14:10:25.352 IST

Adjacency table (version 7) has 7 adjacencies:
      2 complete adjacencies
      0 incomplete adjacencies
      5 interface adjacencies
      0 deleted adjacencies in quarantine list
      2 adjacencies of type IPv4
          2 complete adjacencies of type IPv4
          0 incomplete adjacencies of type IPv4
          1 drop adjacency of type IPv4
          0 deleted adjacencies of type IPv4 in quarantine list
          1 multicast adjacency of type IPv4
```

To verify the details of each type of adjacency, use the **show adjacency *interface* internal detail** command. In the output, **Entry-flag: 0x1000** shows that drop adjacencies are identified in the configured interface.

```
RP/0/0/CPU0:ios#show adjacency gigabitEthernet 0/1/0/0 internal detail
Mon Nov 26 14:10:57.440 IST
------------------------------------------------------------------------------
0/1/CPU0
------------------------------------------------------------------------------

GigabitEthernet0/1/0/0, (src mac only) (ipv4)
        Version: 6, references: 2, transient lock: 0
        Encapsulation information (14 bytes) 000000000000027d42e9bd360800
        MTU: 1500
        Adjacency pointer is: 0x571990ac
        Platform adjacency pointer is: 0
        Last updated: Nov 26 14:07:17.695
        Adjacency producer: arp (prod_id: 10)
        Flags: incomplete adj,
                (Base-flag: 0x1, Entry-flag: 0x1)
        Netio idb pointer not cached
        Cached interface type: 15
        Adjacency references:
                ipv4_mfwd_partner (JID 274, PID 44110), 1 reference
                aib (JID 178, PID 44107), 1 reference

Gi0/1/0/0, (interface)
        Version: 1, references: 1, transient lock: 0
        MTU: 1500
        Adjacency pointer is: 0x57198c60
        Platform adjacency pointer is: 0
        Last updated: Nov 26 14:06:57.267
        Adjacency producer: dot1q (prod_id: 11)
        Flags: interface adjacency, incomplete adj,
                (Base-flag: 0x1, Entry-flag: 0x4)
        Netio idb pointer not cached
        Cached interface type: 15
        Adjacency references:
                aib (JID 178, PID 44107), 1 reference

GigabitEthernet0/1/0/0, 1.1.1.2 (ipv4)
        Version: 7, references: 2, transient lock: 0
        Encapsulation information (14 bytes) 000000000000027d42e9bd360800
        MTU: 1500
```

```
        Adjacency pointer is: 0x57199264
        Platform adjacency pointer is: 0
        Last updated: Nov 26 14:07:36.813
        Adjacency producer: arp (prod_id: 10)
         Entry-flag: 0x1000)(Base-flag: 0x1, Entry-flag: 0x1000)
        Netio idb pointer not cached
        Cached interface type: 15
        Adjacency references:
                l2fib_mgr (JID 247, PID 44514), 0 reference
                fib_mgr (JID 261, PID 44119), 1 reference
                aib (JID 178, PID 44107), 1 reference
```

To verify the drop adjacencies in FIB, use the **show cef adjacency {*interface*|*location*}** command:

```
Router# show cef adjacency gigabitEthernet 0/1/0/0 location 0/1/CPU0
Mon Nov 26 14:12:49.924 IST
Display protocol is ipv4
Interface    Address                                          Type    Refcount

Gi0/1/0/0                                                     special 2
             Interface: Gi0/1/0/0 Type:  glean
             Interface Type: 0xf, Base Flags: 0x10001100 (0x573819b8)
             Nhinfo PT: 0x573819b8, Idb PT: 0x5716e354, If Handle: 0x804060
             Dependent adj type: remote (0x57f88060)
             Dependent adj intf: Gi0/1/0/0
             Ancestor If Handle: 0x0
Update time Nov 26 14:07:17.717


Gi0/1/0/0     Prefix: 1.1.1.2/32                              local   3
             Adjacency: PT:0x57199264 1.1.1.2/32
             Interface: Gi0/1/0/0
             NHID: 0x0
             MAC: 00.00.00.00.00.00.02.7d.42.e9.bd.36.08.00
             Interface Type: 0xf, Base Flags: 0x30000001 (0x57f880b8)
             Nhinfo PT: 0x57f880b8, Idb PT: 0x5716e354, If Handle: 0x804060
             Dependent adj type: remote (0x57f88060)
             Dependent adj intf: Gi0/1/0/0
             Ancestor If Handle: 0x0
Update time Nov 26 14:07:36.836
```

To verify the number of drop adjacency packets that are forwarded to the FIB, use the **show cef drops location *location-value*** command:

```
Router# ping 1.1.1.2 count 5
Thu Feb 7 19:31:25.893 IST
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
RP/0/RSP0/CPU0:RR#show cef drops  location 0/1/cPU0
Mon Nov 26 09:11:58.669 UTC
CEF Drop Statistics
Node: 0/1/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :              0
  Null0 drops          packets :              0
  No route drops       packets :              0
  No Adjacency drops   packets :              5
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              3
  Discard drops        packets :              5
  GRE lookup drops     packets :              0
```

```
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :               0

**This counter will get incremented for the traffic received for drop-adjacency only if
interface is configured with "ipv4 unreachabel disable".
              Sample config:
RP/0/RSP0/CPU0:RR#show running-config interface GigabitEthernet 0/1/0/0
Thu Feb 7 19:31:25.893 IST
interface GigabitEthernet0/1/0/0
ipv4 address 1.1.1.1 255.255.255.0
arp drop-adjacency timeout 1200
ipv4 unreachables disable
!
```

To verify the global statistics of the packets that are sent to ICMP instead of ARP, use the **show controllers np counters** ***np-value*** **location** ***location-value*** command. Packets sent to ICMP do not require ARP resolution because they have a drop adjacency ot normal adjacency entry in the FIB.

```
RP/0/RSP0/CPU0:RR#ping 1.1.1.2
Mon Nov 26 09:15:27.370 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
RP/0/RSP0/CPU0:RR#show controllers np counters np0 location 0/1/cPU0
Mon Nov 26 09:15:43.651 UTC

                Node: 0/1/CPU0:
----------------------------------------------------------------

Show global stats counters for NP0, revision v3

Last clearing of counters for this NP: NEVER

Read 53 non-zero NP counters:
Offset  Counter                                                 FrameValue   Rate (pps)
--------------------------------------------------------------------------------------
  16  MDF_TX_LC_CPU                                               3381479           5
  17  MDF_TX_WIRE                                                  963536           0
  21  MDF_TX_FABRIC                                               1824309           0
  33  PARSE_FAB_RECEIVE_CNT                                       1842113           0
  37  PARSE_INTR_RECEIVE_CNT                                    295405833         514
  41  PARSE_INJ_RECEIVE_CNT                                        68023           0
 45  PARSE_ENET_RECEIVE_CNT                                       927472           0
  49  PARSE_TM_LOOP_RECEIVE_CNT                                  11044944          19
  64  DBG_RSV_EP_L_RSV_ING_L3_IFIB                                 927244           0
  65  DBG_RSV_EP_L_RSV_ING_L3_IFIB_MATCH                           927244           0
  66  DBG_RSV_EP_L_RSV_ING_L3_IFIB_PUNT_LOCAL                       31654           0
  68  DBG_RSV_EP_L_RSV_ING_L3_RSLTS_MATCH                           927244           0
  69  DBG_RSV_EP_L_RSV_ING_PUNT                                    4287668           4
142  RSV_DROP_IPV4_DROP_RP_DEST                                        16           0
143  RSV_DROP_IPV4_DROP_RP_DEST_MONITOR                                 2           0
149  RSV_DROP_IPV6_RXADJ_DROP_MONITOR                                   1           0
173  RSV_DROP_IPV4_TXADJ_DROP                                          10           0
272  RSV_DROP_IN_L3_NOT_MYMAC                                           5           0
581  MODIFY_PUNT_REASON_MISS_DROP                                       2           0
776  PUNT_ARP                                                          94           0
790  PUNT_DIAGS                                                      9535           0
832  PUNT_FOR_ICMP                                                    104           0
850  PUNT_ADJ                                                        8279           0
862  PUNT_IPV6_HOP_BY_HOP                                              18           0
902  PUNT_STATISTICS                                               3331795           4
```

```
904  PUNT_DIAGS_RSP_ACT                                  9463           0
906  PUNT_DIAGS_RSP_STBY                                 9462           0
1084  DROP_FRM_RUNT                                         2           0
1683  DISCARD_FRM_ERR_INTF_194                               1           0
1694  DISCARD_CRC_ERR_INTF_198                               1           0
1695  DISCARD_FRM_ERR_INTF_198                               1           0
1869  PRS_HEALTH_MON                                  11044932          19
1879  INTR_FRAME_TYPE_7                                2629849           4
1885  INTR_FRAME_TYPE_13                                701947           0
1902  PARSE_ING_IPV6_LINK_LOCAL                          18938           0
1906  PARSE_RSP_INJ_FAB_CNT                              18008           0
1907  PARSE_RSP_INJ_PORT_CNT                                51           0
1909  PARSE_RSP_INJ_DIAGS_CNT                            18925           0
1911  PARSE_EGR_INJ_PKT_TYP_IPV4                           176           0
1912  PARSE_EGR_INJ_PKT_TYP_IPV6                            10           0
1915  PARSE_EGR_INJ_PKT_TYP_IPV4_PREROUTE                17822           0
1922  PARSE_LC_INJ_FAB_CNT                                7231           0
1923  PARSE_LC_INJ_PORT_CNT                              51253           0
1924  PARSE_LC_INJ_DIAGS_CNT                              9535           0
1926  PARSE_DROP_UNKNOWN_TIMER_FEAT                          3           0
1929  PARSE_FAB_INJ_IPV4_L3_INWARD                      451473           0
1930  PARSE_FAB_INJ_IPV6_L3_INWARD                      451097           0
1945  PARSE_DROP_IN_UIDB_DOWN                                5           0
1979  PARSE_DROP_IPV6_DISABLED                              36           0
1981  PARSE_DROP_IPV6_LENGTH                                 4           0
2127  ING_ICFD_QUEUE_PRI_0                              662786           0
2128  ING_ICFD_QUEUE_PRI_1                              264566           0
2130  ING_ICFD_QUEUE_PRI_3                                 120           0

**The above counter will get incremented for traffic received for a drop-adjacency.
```

Clearing ARP Cache of Drop Adjacencies

You can delete the drop adjacencies on an interface, location, or an IP address by using the command **clear arp-cache drop-adjacency** ***interface ip-address location***. This command deletes the drop adjacencies from the ARP database and AIB. To get more information, see the *clear arp-cache* command in the chapter *ARP Commands* of the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Restrictions

- Configuration of the **clear arp-cache drop-adjacency** command on a particular location is not recommended. If the command is used on a bundle interface that comprises of a few interfaces on few line cards, then drop adjacencies may be deleted in one of the interfaces line cards and not on other line cards. This scenario can result in entry mismatch. You can use the **clear arp-cache drop-adjacency** ***interface location*** **all** command to remove drop adjacency that is learned for the interface on all the line cards.

Installing Drop Adjacencies in Hardware

If ARP throttling is configured on an interface and ARP fails to resolve a dynamic entry on that interface, then ARP marks that entry as drop adjacency entry for the interface in its database and in AIB. The drop adjacency timeout starts for that entry at that interface or hardware as per the configured timeout value. Once the timeout period is over, drop adjacency for that entry is removed from the ARP database and AIB.

Handling Drop Adjacencies Over Virtual Interfaces

If ARP throttling is configured over a virtual interface, drop adjacencies are synced with other interfaces like BVI or Bundle Interfaces over Group Service Process (GSP). This synching occurs in the member line cards in case of Bundles and in all the line cards in case of BVIs. Therefore, when an entry state is changed to drop adjacency or removed from drop adjacency, ARPs running on all the line cards have the same drop adjacency state for a particular entry. The drop adjacency state for an entry is updated in AIB as well.

Handling Drop Adjacencies on Process Restart

ARP stores all adjacencies in the shared memory. Hence, after a process restart or an AIB disconnect followed by an AIB connect, ARP restores all drop adjacencies along with dynamic entries to the AIB.

Note The timers for ARP entries, including timeout for drop adjacencies, is reset after a process restart. Therefore, the duration for drop adjacency entries for timeout is increased.

Handling Drop Adjacencies over ISSU and Geo Redundancy

During ISSU, the drop adjacencies in the ARP database are not synched from the earlier version of the router to the upgraded version of the router. The drop adjacencies are recreated in the refreshed ARP database and AIB of the upgraded router.

Similarly, if ARP throttling and Geo Redundancy are configured for an interface of a router, the drop adjacencies are not synched across the active and backup routers. Once the backup router becomes the active router, the drop adjacencies are revreated in the refreshed ARP database and AIB of the newly active router.

Handling Drop Adjacencies on Interface Flap

In there is an interface flap, the purge delay feature allows the retention of dynamic entries in the ARP database up to a configured timeout period. The dynamic entries are not deleted from the ARP database if the interface comes up within the configured timeout period. However, the entries for drop adjacencies are not retained in the ARP database if there is an interface flap.

Additional References

The following sections provide references related to ARP.

Related Documents

Related Topic	Document Title
ARP commands	*ARP Commands* module in *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Quality of Service Commands* module in *Modular Quality of Service Command Reference for Cisco ASR 9000 Series Routers*
Class-based traffic shaping, traffic policing, low latency queuing, and MDDR	Configuring Modular Quality of Service Congestion Management module in *Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

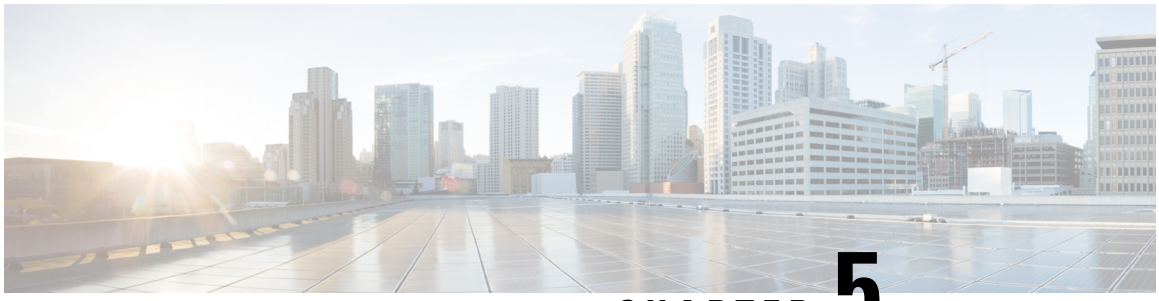
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
RFC 826	Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC 1027	Using ARP to implement transparent subnet gateways

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



CHAPTER 5

Implementing the Dynamic Host Configuration Protocol

This module describes the concepts and tasks you will use to configure Dynamic Host Configuration Protocol (DHCP).

Note For a complete description of the DHCP commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Implementing the Dynamic Host Configuration Protocol

Release	Modification
Release 3.7.2	This feature was introduced .

Prerequisites for Configuring DHCP Relay Agent

The following prerequisites are required to configure a DHCP relay agent:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- A configured and running DHCP client and DHCP server
- Connectivity between the relay agent and DHCP server

Information About DHCP Relay Agent

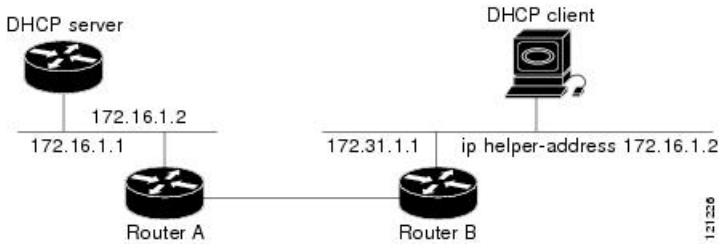
A DHCP relay agent is a host that forwards DHCP packets between clients and servers that do not reside on a shared physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router where IP datagrams are switched between networks transparently.

DHCP clients use User Datagram Protocol (UDP) broadcasts to send DHCPDISCOVER messages when they lack information about the network to which they belong.

If a client is on a network segment that does not include a server, a relay agent is needed on that network segment to ensure that DHCP packets reach the servers on another network segment. UDP broadcast packets are not forwarded, because most routers are not configured to forward broadcast traffic. You can configure a DHCP relay agent to forward DHCP packets to a remote server by configuring a DHCP relay profile and configure one or more helper addresses in it. You can assign the profile to an interface or a VRF.

Figure 12: Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address, on page 66 demonstrates the process. The DHCP client broadcasts a request for an IP address and additional configuration parameters on its local LAN. Acting as a DHCP relay agent, Router B picks up the broadcast, changes the destination address to the DHCP server's address and sends the message out on another interface. The relay agent inserts the IP address of the interface, on which the DHCP client's packets are received, into the gateway address (giaddr) field of the DHCP packet, which enables the DHCP server to determine which subnet should receive the offer and identify the appropriate IP address range. The relay agent unicasts the messages to the server address, in this case 172.16.1.2 (which is specified by the helper address in the relay profile).

Figure 12: Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address



Limitations for DHCPv6 Relay Feature

These are the limitations for implementing DHCPv6 relay feature:

- The multicast addresses are not supported. The **helper-address** command in DHCPv6 relay profile submode will only support global unicast IPv6 address as the helper address.
- Only one relay is supported between client and server with an exception of Lightweight DHCPv6 Relay Agent (LRDA) being present on the access side. That is, the Layer 3 relay packets are not supported.
- Only interface-id and remote-id DHCPv6 option code are added by a relay agent while forwarding the packet to a DHCPv6 server.

Note Configuring DHCPv6 option code is not supported in DHCPv6 relay profile submode.

Secure ARP

In standalone DHCP sessions, the DHCP server adds an ARP entry when it assigns an IP address to a client. However, in IP subscriber sessions, DHCP server does not add an ARP entry. Although ARP establishes correspondences between network addresses, an untrusted device can spoof IP an address not assigned to it posing a security threat for IP subscriber sessions. You can enable the secure ARP feature and allow DHCP to add an ARP cache entry when DHCP assigns an IP address to a client. Secure ARP is disabled by default.

How to Configure and Enable DHCP Relay Agent

This section contains the following tasks:

Configuring and Enabling DHCP Relay Agent with DHCP MAC Address Verification

This section discusses how to configure and enable DHCP Relay Agent with DHCP MAC address verification.

Configuration Example

```
Router# configure

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile client relay
/* Enables DHCP relay profile */

Router(config-dhcpv4)# client-mac-mismatch action drop
/* Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not
 match the L2 header source MAC address in the DHCPv4 relay profile,
 the frame is dropped  */

Router(config-dhcpv4-relay-profile)# relay information option
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information check
```

```
/* (Optional) Configures DHCP to check the validity of the relay agent information
option in forwarded BOOTREPLY messages. */

Router(config-dhcpv4-relay-profile)# relay information policy drop
/* (Optional) Configures the reforwarding policy for a DHCP relay agent;
that is, whether the relay agent will drop or keep (using the 'keep' keyword)
 the relay information. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have
an existing
relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# giaddr policy drop
/* Drops the packet that has an existing nonzero giaddr value. Use the 'replace' keyword
 to replace the existing giaddr value with a value that it generates (the default behavior).
  */

Router(config-dhcpv4-relay-profile)# helper-address vrf vrf1 10.1.1.1
/* Forwards UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# commit

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# vrf vrf1 relay profile client
Router(config-dhcpv4)# commit
/* Configures DHCP Relay on a VRF and commits the entire configuration. */
```

Running Configuration

Confirm your configuration.

```
Router# show run
Thu May 11 09:00:57.839 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Thu May 11 09:00:54 2017 by annseque
!
dhcp ipv4
vrf vrf1 relay profile client
profile client relay
client-mac-match action drop
helper-address vrf vrf1 10.1.1.1
giaddr policy drop
relay information check
relay information option
relay information policy drop
relay information option allow-untrusted
!
!
```

DHCP MAC Address Verification

Use the following show command to check if DHCP MAC address is being verified on the router.

```
Router# show dhcp ipv4 relay statistics raw all
packet_drop_mac_mismatch                      :         0
```

The output validates that the DHCP MAC address of the packets is verified.

Configuring the DHCPv6 (Stateless) Relay Agent

Perform this task to specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface.

Configuration Example

To configure the DHCPv6 (stateless) relay agent, you must complete the following configurations:

1. Enable the DHCP IPv6 configuration mode.
2. Configure the DHCPv6 relay profile.
3. Configure helper addresses.
4. Specify the interface for the relay profile.

Configuration

```
/* Enter the global configuration mode, and then enter the DHCP IPv6 configuration mode */
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile test relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:1::1
Router(config-dhcpv6-relay-profile)# !
Router(config-dhcpv6-relay-profile)# interface TenGigE0/0/0/0 relay profile test
Router(config-dhcpv6)# !
```

Enabling DHCP Relay Agent on an Interface

This task describes how to enable the Cisco IOS XR DHCP relay agent on an interface.

Note On Cisco IOS XR software, the DHCP relay agent is disabled by default.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **interface type name relay profile** *profile-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration submode.
Step 3	**interface type name relay profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# interface gigabitethernet 0/0/0 /0 relay profile client`	Attaches a relay profile to an interface.
Step 4	**commit**	

Enabling DHCPv6 Relay Agent on an Interface

This task describes how to enable the DHCPv6 relay agent on an interface.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv6**
3. **interface** *type interface-instance* **relay profile** *profile-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**dhcp ipv6** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv6`	Configures DHCP for IPv6 and enters the DHCPv6 configuration submode.
Step 3	**interface** *type interface-instance* **relay profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv6)# interface gigabitethernet 0/0/0/0 relay profile client`	Attaches a relay profile to an interface.

	Command or Action	Purpose
Step 4	**commit**	

Enabling DHCPv6 Relay Agent on an Interface: Example

```
configure
dhcp ipv6
interface gigabitethernet 0/0/0/0 relay profile client
!
end
```

Disabling DHCP Relay on an Interface

This task describes how to disable the DHCP relay on an interface by assigning the none profile to the interface.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **interface** *type name* **none**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration submode.
Step 3	**interface** *type name* **none** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# interface gigabitethernet 0/1/4/1 none`	Disables the DHCP relay on the interface.
Step 4	**commit**	

Enabling DHCP Relay on a VRF

This task describes how to enable DHCP relay on a VRF.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **vrf** *vrf-name* **relay profile** *profile-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration submode.
Step 3	**vrf** *vrf-name* **relay profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# vrf default relay profile client`	Enables DHCP relay on a VRF.
Step 4	**commit**	

Configuring the Relay Agent Information Feature

This task describes how to configure the DHCP relay agent information option processing capabilities.

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced (using the replace option).

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **relay**
4. **relay information option**
5. **relay information check**
6. **relay information policy** {**drop** | **keep**}
7. **relay information option allow-untrusted**
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration submode .
Step 3	**profile** *profile-name* **relay** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay`	Enters DHCP IPv4 profile relay submode .
Step 4	**relay information option** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option`	Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server. • This option is injected by the relay agent while forwarding client-originated DHCP packets to the server. Servers recognizing this option can use the information to implement IP address or other parameter assignment policies. When replying, the DHCP server echoes the option back to the relay agent. The relay agent removes the option before forwarding the reply to the client. • The relay agent information is organized as a single DHCP option that contains one or more suboptions. These options contain the information known by the relay agent. The supported suboptions are: • Remote ID • Circuit ID **Note** This function is disabled by default. The port field of the default circuit-ID denotes the configured bundle-ID of the bundle. If circuit IDs require that bundles be unique, and because the port field is 8 bits, the low-order 8 bits of configured bundle IDs must be unique. To achieve this, configure bundle-IDs within the range from 0 to 255.

	Command or Action	Purpose
Step 5	**relay information check** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information check`	(Optional) Configures DHCP to check the validity of the relay agent information option in forwarded BOOTREPLY messages. If an invalid message is received, the relay agent drops the message. If a valid message is received, the relay agent removes the relay agent information option field and forwards the packet. • By default, DHCP does not check the validity of the relay agent information option field in DHCP reply packets, received from the DHCP server. **Note** Use the **relay information check** command to reenable this functionality if the functionality has been disabled.
Step 6	**relay information policy** {**drop** | **keep**} **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp relay information policy drop`	(Optional) Configures the reforwarding policy for a DHCP relay agent; that is, whether the relay agent will drop or keep the relay information. By default, the DHCP relay agent replaces the relay information option.
Step 7	**relay information option allow-untrusted** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option allow-untrusted`	(Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero.
Step 8	**commit**	

Configuring Relay Agent Giaddr Policy

This task describes how to configure the DHCP relay agent's processing capabilities for received BOOTREQUEST packets that already contain a nonzero giaddr attribute.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile relay**
4. **giaddr policy** {**replace** | **drop**}
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enables the DHCP IPv4 configuration submode.
Step 3	**profile relay** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay`	Enables profile relay submode.
Step 4	**giaddr policy** {**replace** | **drop**} **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# giaddr policy drop`	Specifies the giaddr policy. • replace—Replaces the existing giaddr value with a value that it generates. • drop—Drops the packet that has an existing nonzero giaddr value. By default, the DHCP relay agent keeps the existing giaddr value.
Step 5	**commit**	

Configuring a DHCPv4 Relay Profile with Multiple Helper Addresses

You can configure up to 16 helper addresses for a DHCPv4 relay profile, as shown in the following example.

1. Enter the DHCPv4 configuration mode.

   ```
   RP/0/RSP0/CPU0:router(config)# dhcp ipv4
   ```

2. Configure the DHCPv4 relay profile.

   ```
   RP/0/RSP0/CPU0:router(config-dhcpv4)# profile helper relay
   ```

3. Configure helper addresses.

   You can configure up to 16 IPv4 addresses.

   ```
   RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 1.1.1.1
   RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 2.2.2.2
   RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 3.3.3.3
   RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 4.4.4.4
   ```

```
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 5.5.5.5
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 6.6.6.6
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 7.7.7.7
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 8.8.8.8
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 9.9.9.9
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 10.10.10.10
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 11.11.11.11
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 12.12.12.12
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 13.13.13.13
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 14.14.14.14
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 15.15.15.15
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf default 16.16.16.16
```

4. Confirm your configuration.

```
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# show configuration
Thu Feb  2 13:49:15.605 IST
Building configuration...
!! IOS XR Configuration 0.0.0
dhcp ipv4
 profile helper relay
  helper-address vrf default 1.1.1.1
  helper-address vrf default 2.2.2.2
  helper-address vrf default 3.3.3.3
  helper-address vrf default 4.4.4.4
  helper-address vrf default 5.5.5.5
  helper-address vrf default 6.6.6.6
  helper-address vrf default 7.7.7.7
  helper-address vrf default 8.8.8.8
  helper-address vrf default 9.9.9.9
  helper-address vrf default 10.10.10.10
  helper-address vrf default 11.11.11.11
  helper-address vrf default 12.12.12.12
  helper-address vrf default 13.13.13.13
  helper-address vrf default 14.14.14.14
  helper-address vrf default 15.15.15.15
  helper-address vrf default 16.16.16.16
 !
!
end
```

5. Commit your configuration.

```
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# commit
```

6. Exit the configuration mode and verify the configured helper addresses.

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 relay profile name helper
...
Profile: helper
Helper Addresses:
        1.1.1.1, vrf default
        2.2.2.2, vrf default
        3.3.3.3, vrf default
        4.4.4.4, vrf default
        5.5.5.5, vrf default
        6.6.6.6, vrf default
        7.7.7.7, vrf default
        8.8.8.8, vrf default
        9.9.9.9, vrf default
        10.10.10.10, vrf default
        10.10.10.11, vrf default
        10.10.10.13, vrf default
        10.10.10.14, vrf default
        10.10.10.15, vrf default
```

```
        10.10.10.16, vrf default
        10.10.10.17, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option VPN: Disabled
Information Option VPN Mode: RFC
Information Option Policy: Replace
Information Option Check: Disabled
GIADDR Policy: Keep
Broadcast-flag Policy: Ignore
VRF References:
Interface References:
```

You have successfully configured multiple DHCPv4 relay helper addresses.

Configuring a DHCP Proxy Profile

The DHCP proxy performs all the functions of a relay and also provides some additional functions. The DHCP proxy conceals DHCP server details from DHCP clients. The DHCP proxy modifies the DHCP replies such that the client considers the proxy to be the server. In this state, the client interacts with the proxy as if it is the DHCP server.

This task describes how to configure and enable the DHCP proxy profile.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **proxy**
4. **helper-address** [**vrf** *vrf- name*] *address* [**giaddr** *gateway-address*]
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration submode .
Step 3	**profile** *profile-name* **proxy** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client proxy`	Enters DHCP IPv4 profile proxy submode.

	Command or Action	Purpose
Step 4	**helper-address** [**vrf** *vrf- name*] *address* [**giaddr** *gateway-address*] **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# helper-address vrf1 10.10.1.1`	Forwards UDP broadcasts, including DHCP. • The value of the *address* argument can be a specific DHCP server address or a network address (if other DHCP servers are on the destination network segment). Using the network address enables other servers to respond to DHCP requests. • For multiple servers, configure one helper address for each server.
Step 5	**commit**	

Configuring DHCPv6 Relay Binding Database Write to System Persistent Memory

Perform this task to configure the DHCPv6 relay binding database write to the system persistent memory. This helps to recover the DHCPv6 relay binding table after a system reload. The file names used for a full persistent file write are *dhcpv6_srpb_{nodeid}_odd* and *dhcpv6_srpb_{nodeid}_even*. The *nodeid* is the actual node ID of the node where the file is written. The incremental file is named the same way as the full file, with a *_inc* appended to it.

Note With IOS XR Release 6.6.3, DHCPv6 client binding record format written to system persistent memory is changed. Due to this, when you upgrade IOS XR Software from versions lower to 6.6.3 to version 6.6.3 or above, the DHCPv6 process fails to restore the client bindings from the system persistent memory during router reload, and the router losses all the client bindings.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv6**
3. **database** [**relay**] [**full-write-interval** *full-write-interval*] [**incremental-write-interval** *incremental-write-interval*]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router# configure`	
Step 2	**dhcp ipv6** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv6`	Configures DHCP for IPv6 and enters the DHCPv6 configuration mode.
Step 3	**database** [**relay**] [**full-write-interval** *full-write-interval*] [**incremental-write-interval** *incremental-write-interval*] **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv6)# database relay full-write-interval 20 incremental-write-interval 10`	Configures the DHCPv6 relay binding table write to the system persistent memory and specifies the time interval at which the full write and incremental file write are to be performed. The range, in minutes, for *full-write-interval* and *incremental-write-interval* is from 0 to 1440. The default value is 10 for *full-write-interval* and 1 for *incremental-write-interval*. The DHCP mode should be set as **relay**.
Step 4	**commit**	

Configuring DHCPv6 relay binding database write to system persistent memory: Example

```
 configure
 dhcp ipv6
 database relay full-write-interval 15 incremental-write-interval 5
 !
end
```

DHCPv4 Server

DHCP server accepts address assignment requests and renewals and assigns the IP addresses from predefined groups of addresses contained within Distributed Address Pools (DAPS). DHCP server can also be configured to supply additional information to the requesting client such as subnet mask, domain-name, the IP address of the DNS server, the default router, and other configuration parameters. DHCP server can accept broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

The DHCP proxy performs all the functions of a relay and also provides some additional functions. The DHCP proxy conceals DHCP server details from DHCP clients. The DHCP proxy modifies the DHCP replies such that the client considers the proxy to be the server. In this state, the client interacts with the proxy as if it is the DHCP server.

DHCP IPv4 service based mode selection

As part of DHCP IPv4 service based mode selection feature, a new mode called DHCP base is introduced. If an interface is configured in the DHCP base mode, then the DHCP selects either the DHCP proxy or the DHCP server mode to process the client request by matching option 60 (class-identifier) value of the client request with the configured value under the DHCP base profile.

For example:

```
dhcp ipv4
profile DHCP_BASE base
  match option 60 41424344 profile DHCP_PROXY proxy
  match option 60 41424355 profile DHCP_SERVER server
  default profile DEFAULT_PROFILE server
  relay information authenticate inserted
   !
profile DHCP_PROXY proxy
  helper-address vrf default 10.10.10.1 giaddr 0.0.0.0
!
profile DHCP_SERVER server
  lease 1 0 0
  pool IP_POOL
!
profile DEFAULT_PROFILE server
  lease 1 0 0
  pool IP_POOL
!
!
interface gigabitEthernet 0/0/0/0 base profile DHCP_BASE
```

The pool is configured under server-profile-mode and server-profile-class-sub-mode. The class-based pool selection is always given priority over profile pool selection.

The DHCPv4 server profile class sub-mode supports configuring DHCP options except few (0, 12, 50, 52, 53, 54, 58, 59, 61, 82, and 255).

Configuring DHCPv4 Server Profile

Perform this task to configure the DHCPv4 Server.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **server**
4. **bootfile** *boot-file-name*
5. **broadcast-flag policy** *unicast-always*
6. **class** *class-name*
7. **exit**
8. **default-router** *address1 address2 ... address8*
9. **lease** {**infinite** | *days minutes seconds* }
10. **limit lease** {**per-circuit-id** | **per-interface** | **per-remote-id** } *value*
11. **netbios-name server** *address1 address2 ... address8*
12. **netbios-node-type** {**number** | **b-node** | **h-node** | **m-node** | **p-node** }
13. **option** *option-code* {**ascii** *string* | **hex** *string* | **ip** *address*}
14. **pool** *pool-name*
15. **requested-ip-address-check disable**
16. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**dhcp ipv4**
	Example:
	`RP/0/RSP0/CPU0:router(config) # dhcp ipv4`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.

Step 3	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile TEST server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

Step 4	**bootfile** *boot-file-name* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# bootfile b1`	Configures the boot file.
Step 5	**broadcast-flag policy** *unicast-always* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# broadcast-flag policy unicast-always`	Configures the broadcast-flag policy to unicast-always.

Step 6	**class** *class-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class Class_A`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile-class)`
		Creates and enters server profile class configuration submode.

Step 7	**exit** **Example:**	Exits the server profile class submode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile-class)# exit` `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`	
Step 8	**default-router** *address1 address2 ... address8* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# default-router 10.20.1.2`	Configures the name of the default-router or the IP address.
Step 9	**lease** { **infinite** | *days minutes seconds* } **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# lease infinite`	Configures the lease for an IP address assigned from the pool.
Step 10	**limit lease** { **per-circuit-id** | **per-interface** | **per-remote-id** } *value* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# limit lease per-circuit-id 23`	Configures the limit on a lease per-circuit-id, per-interface, or per-remote-id.
Step 11	**netbios-name server** *address1 address2 ... address8* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# netbios-name-server 10.20.3.5`	Configures the NetBIOS name servers.
Step 12	**netbios-node-type** { **number** | **b-node** | **h-node** | **m-node** | **p-node** } **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# netbios-node-type p-node`	Configures the type of NetBIOS node.
Step 13	**option** *option-code* { **ascii** *string* | **hex** *string* | **ip** *address* } **Example:**	Configures the DHCP option code.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# option 23 ip 10.20.34.56`	
Step 14	**pool** *pool-name* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# pool pool1`	Configures the Distributed Address Pool Service (DAPS) pool name.
Step 15	**requested-ip-address-check disable** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# requested-ip-address-check disable`	Validates a requested IP address.
Step 16	**commit**	

Configuring Multiple Classes with a Pool

Perform this task to configure multiple classes with a pool.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **server**
4. **pool** *pool-name*
5. **class** *class-name*
6. **pool** *pool_name*
7. **match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*]
8. **exit**
9. **class** *class-name*
10. **pool** *pool_name*
11. **match vrf** *vrf-name*
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**dhcp ipv4**
	Example:
	`RP/0/RSP0/CPU0:router(config) # dhcp ipv4`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.

Step 3	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile TEST server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

Step 4	**pool** *pool-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# pool POOL_TEST`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Configures the Distributed Address Pool Service(DAPS) pool name.

Step 5	**class** *class-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class Class_A`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Creates and enters the server profile class.

Step 6	**pool** *pool_name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# pool pool_A`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the pool name.

	Command or Action	Purpose

Step 7	**match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*]
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# match option 60 hex abcd`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		The DHCP server selects a pool from a class by matching options in the received DISCOVER packet with the match option. If none of the classes match, then pools configured under the profile mode are selected. The DHCP server requests DAPS to allocate an address from that pool.

Step 8	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# exit`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Exits the server profile class submode.

Step 9	**class** *class-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class Class_B`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Creates and enters the server profile class.

Step 10	**pool** *pool_name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# pool pool_B`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the pool name.

Step 11	**match vrf** *vrf-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# match vrf VRF1`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		The DHCP server selects a pool from a class by matching the options in the received DISCOVER packet with the match command. If none of the classes match, then pools configured under the profile mode are selected. The DHCP server requests DAPS to allocate an address from that pool.

Step 12	**commit**	

Configuring a server profile DAPS with class match option

Perform this task to configure a server profile DAPS with class match option.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **server**
4. **pool** *pool-name*
5. **class** *class-name*
6. **pool***pool_name*
7. **match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*]
8. **exit**
9. **exit**
10. **profile** *profile-name* **server**
11. **dns-server** *address1 address2 ... address8*
12. **pool** *pool_name*
13. **class** *class-name*
14. **pool***pool_name*
15. **match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*]
16. **exit**
17. **exit**
18. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**dhcp ipv4**
	Example:
	`RP/0/RSP0/CPU0:router(config) # dhcp ipv4`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.

Step 3	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile ISP1 server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

	Command or Action	Purpose

Step 4	**pool** *pool-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# pool ISP1_POOL`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Configures the Distributed Address Pool Service(DAPS) pool name.

Step 5	**class** *class-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class ISP1_CLASS`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Creates and enters the server profile class.

Step 6	**pool***pool_name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# pool ISP1_CLASS_POOL`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the pool name.

Step 7	**match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*]
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# match option 60 hex PXEClient_1`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		The DHCP server selects a pool from a class by matching the options in the received DISCOVER packet with the match option. If none of the classes match, then pools configured under the profile mode will be selected. The DHCP server requests the DAPS to allocate an address from that pool.

Step 8	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# exit`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-prfile)#`
		Exits the server profile class sub mode.

Step 9	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# exit`	Exits the server profile sub mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`	

Step 10	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile ISP2 server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

Step 11	**dns-server** *address1 address2 ... address8*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# dns-server 10.20.3.4`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the name of the DNS server or the IP address

Step 12	**pool** *pool_name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# pool ISP2_POOL`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the pool name.

Step 13	**class** *class-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# class ISP2_CLASS`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Creates and enters the server profile class.

Step 14	**pool***pool_name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# pool ISP2_CLASS_POOL`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#`
		Configures the pool name.

Step 15	**match option** *option* [**sub-option** *sub-option*] [**ascii** *asciiString* | **hex** *hexString*] **Example:**	The DHCP server selects a pool from a class by matching the options in the received DISCOVER packet with the match option. If none of the classes match, then pools configured under the profile mode will be selected. The

	Command or Action	Purpose

	<pre>RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# match option 60 hex PXEClient_2
	RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)#</pre>
		DHCP server requests the DAPS to allocate an address from that pool.

Step 16	**exit**
	Example:
	<pre>RP/0/RSP0/CPU0:router(config-dhcpv4-server-class)# exit
	RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#</pre>
		Exits the server profile class sub mode.

Step 17	**exit**
	Example:
	<pre>RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# exit
	RP/0/RSP0/CPU0:router(config-dhcpv4)#</pre>
		Exits the server profile sub mode.

Step 18	**commit**	

Configuring Server Profile without daps pool match option

Perform this task to configure a server profile without daps pool match option.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **server**
4. **dns-server** *address1 address2 ... address8*
5. **exit**
6. **profile** *profile-name* **server**
7. **dns-server** *address1 address2 ... address8*
8. **exit**
9. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose

Step 2	**dhcp ipv4**
	Example:
	`RP/0/RSP0/CPU0:router(config) # dhcp ipv4`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.

Step 3	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile ISP1 server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

Step 4	**dns-server** *address1 address2 ... address8*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# dns-server ISP1.com`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Configures the name of the DNS server or IP address.

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# exit`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Exits the server profile sub mode.

Step 6	**profile** *profile-name* **server**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4 )# profile ISP2 server`
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`
		Enters the server profile configuration mode.

Step 7	**dns-server** *address1 address2 ... address8* **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# dns-server ISP2.com`	Configures the name of the DNS server or IP address.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)#`	

Step 8	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# exit`
	`RP/0/RSP0/CPU0:router(config-dhcpv4)#`
		Exits the server profile sub mode.

Step 9	**commit**	

Configuring an address pool for each ISP on DAPS

Perform this task to configure an address pool for each ISP on Distributed Address Pool Service(DAPS).

SUMMARY STEPS

1. **configure**
2. **pool vrf** [**all** | *vrf-name*] { **ipv4** | **ipv6** } *pool-name*
3. **network** *address*
4. **exit**
5. **pool vrf** [**all** | *vrf-name*] { **ipv4** | **ipv6** } *pool-name*
6. **network** *address*
7. **exit**
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**pool vrf** [**all**	*vrf-name*] { **ipv4**	**ipv6** } *pool-name*
			Example:
			`RP/0/RSP0/CPU0:router(config) # pool vrf ISP_1 ipv4 ISP1_POOL`
			`RP/0/RSP0/CPU0:router(config-pool-ipv4)#`
				Configures an IPv4 pool for the specifed VRF or all vrfs.

Step 3	**network** *address* **Example:**	Specifies network for allocation.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)# network 10.10.10.0` `RP/0/RSP0/CPU0:router(config-pool-ipv4)#`	

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the pool ipv4 configuration submode.

Step 5	**pool vrf** [**all** | *vrf-name*] { **ipv4** | **ipv6** } *pool-name*
	Example:
	`RP/0/RSP0/CPU0:router(config) # pool vrf ISP_2 ipv4 ISP2_POOL`
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)#`
		Configures an IPv4 pool for the specifed VRF or all vrfs.

Step 6	**network** *address*
	Example:
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)# network 20.20.20.0`
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)#`
		Specifies network for allocation.

Step 7	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-pool-ipv4)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the pool ipv4 configuration submode.

Step 8	**commit**	

DHCPv4 Client

The Dynamic Host Configuration Protocol (DHCP) client functionality enables the router interfaces to dynamically acquire the IPv4 address using DHCP.

The DHCP provides configuration parameters to Internet hosts. DHCP consists of two components:

- a protocol to deliver host-specific configuration parameters from a DHCP server to a host.
- a mechanism to allocate network addresses to hosts.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses, and deliver configuration parameters to dynamically configured hosts.

A relay agent is required if the client and server are not on the same Layer 2 network. The relay agent usually runs on the router, and is required because the client device does not know its own IP address initially. The agent sends out a Layer 2 broadcast to find a server that has this information. The router relays these broadcasts to the DHCP server, and forwards the responses back to the correct Layer 2 address so that the correct device gets the correct configuration information.

DHCP has the ability to allocate IP addresses only for a configurable period of time, called the lease period. If the client is required to retain this IP address for a longer period beyond the lease period, the lease period must be renewed before the IP address expires. The client renews the lease based on configuration that was sent from the server. The client unicasts a REQUEST message using the IP address of the server. When a server receives the REQUEST message and responds with an ACK message. The lease period of the client is extended by the lease time configured in the ACK message.

Restrictions and Limitations

- DHCP client can be enabled only on management interfaces.
- Either DHCP or static IP can be configured on an interface.

Enabling DHCP Client on an Interface

The DHCPv4 or DHCPv6 client can be enabled at an interface level. The DHCP component receives a notification when DHCPv4 or DHCPv6 is enabled or disabled on an interface.

```
Router# configure
Router(config)# interface MgmtEth rack/slot/CPU0/port
Router(config)# interface interface_name ipv6 address dhcp
```

DHCPv6 Relay Agent Notification for Prefix Delegation

DHCPv6 relay agent notification for prefix delegation allows the router working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is being relayed by the relay agent to the client. When the relay agent finds the prefix delegation option, the relay agent extracts the information about the prefix being delegated and inserts an IPv6 subscriber route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay are forwarded based on the information contained in the prefix delegation. The IPv6 subscriber route remains in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

The relay agent automatically does the subscriber route management.

The IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and the IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 subscriber route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

This feature leaves an IPv6 route on the routing table of the relay agent. This registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the router doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The IPv6 route in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. When the client sends a DHCP_DECLINE message, the routes are removed.

Configuring DHCPv6 Stateful Relay Agent for Prefix Delegation

Perform this task to configure Dynamic Host Configuration Protocol (DHCP) IPv6 relay agent notification for prefix delegation.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv6**
3. **profile** *profile-name* **proxy**
4. **helper-address** *ipv6-address* **interface** *type interface-path-id*
5. **exit**
6. **interface** *type interface-path-id* **proxy**
7. **profile** *profile-name*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**dhcp ipv6**
	Example:
	`RP/0/RSP0/CPU0:router(config) # dhcp ipv6`
	`RP/0/RSP0/CPU0:router(config-dhcpv6)#`
		Enables DHCP for IPv6 and enters DHCP IPv6 configuration mode.

Step 3	**profile** *profile-name* **proxy**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv6)# profile downstream proxy`
	`RP/0/RSP0/CPU0:router(config-dhcpv6-profile)#`
		Enters the proxy profile configuration mode.

Step 4	**helper-address** *ipv6-address* **interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# helper-address 2001:db8::1 GigabitEthernet 0/1/0/1`
	`RP/0/RSP0/CPU0:router(config-dhcpv6-profile)`
		Configure the DHCP IPv6 relay agent.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# exit`
	`RP/0/RSP0/CPU0:router(config-dhcpv6)#`
		Exits from the profile configuration mode.

Step 6	**interface** *type interface-path-id* **proxy**
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv6)# interface GigabitEthernet 0/1/0/0 proxy`
	`RP/0/RSP0/CPU0:router(config-dhcpv6-if)#`
		Enables IPv6 DHCP on an interface and acts as an IPv6 DHCP stateful relay agent.

Step 7	**profile** *profile-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-dhcpv6-if)# profile downstream`
	`RP/0/RSP0/CPU0:router(config-dhcpv6-if)#`
		Enters the profile configuration mode.

Step 8	**commit**	

Enabling Secure ARP

Secure ARP is disabled by default; this task describes how to enable secure ARP.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. Do one of the following:
   - **profile** *profile-name* **proxy**
   - **profile** *profile-name* **server**
4. **secure-arp**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 configuration mode.
Step 3	Do one of the following: • **profile** *profile-name* **proxy** • **profile** *profile-name* **server** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile profile1 server`	Enters DHCP IPv4 profile proxy or server submode.
Step 4	**secure-arp** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-server-profile)# secure-arp`	Enables secure ARP.
Step 5	**commit**	

Configuration Examples for the DHCP Relay Agent

This section provides the following configuration examples:

DHCP Relay Profile: Example

The following example shows how to configure the Cisco IOS XR relay profile:

```
dhcp ipv4
 profile client relay
  helper-address vrf foo 10.10.1.1
 !
! ...
```

DHCP Relay on an Interface: Example

The following example shows how to enable the DHCP relay agent on an interface:

```
dhcp ipv4
 interface GigabitEthernet 0/1/1/0 relay profile client
!
```

DHCP Relay on a VRF: Example

The following example shows how to enable the DHCP relay agent on a VRF:

```
dhcp ipv4
 vrf default relay profile client
!
```

Relay Agent Information Option Support: Example

The following example shows how to enable the relay agent and the insertion and removal of the DHCP relay information option:

```
dhcp ipv4
 profile client relay
relay information option

 !
!
```

Relay Agent Giaddr Policy: Example

The following example shows how to configure relay agent giaddr policy:

```
dhcp ipv4
 profile client relay
  giaddr policy drop
 !
!
```

Implementing DHCP Snooping

Prerequisites for Configuring DHCP Snooping

The following prerequisites are required example shows how to configure DHCP IPv4 snooping relay agent broadcast flag policy:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- A Cisco ASR 9000 Series Router running Cisco IOS XR software.

- A configured and running DHCP client and DHCP server.

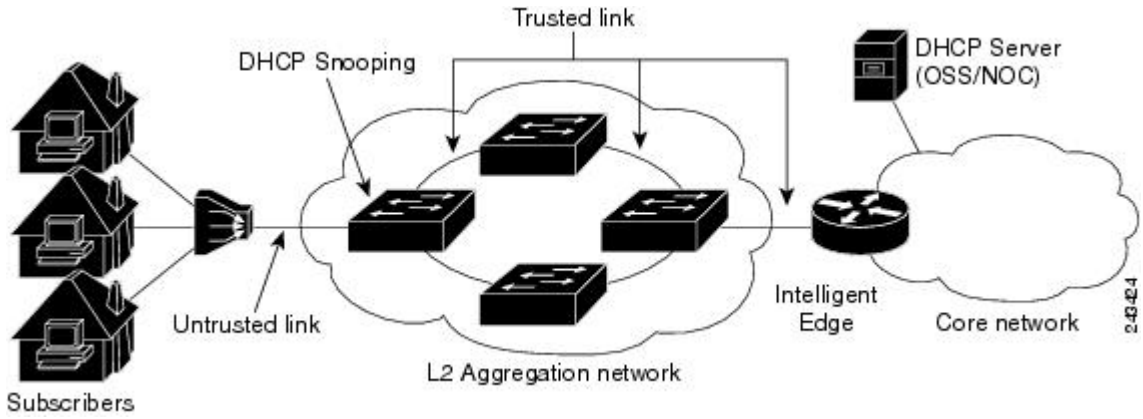
Information about DHCP Snooping

DHCP Snooping features are focused on the edge of the aggregation network. Security features are applied at the first point of entry for subscribers. Relay agent information option information is used to identify the subscriber's line, which is either the DSL line to the subscriber's home or the first port in the aggregation network.

The central concept for DHCP snooping is that of trusted and untrusted links. A trusted link is one providing secure access for traffic on that link. On an untrusted link, subscriber identity and subscriber traffic cannot be determined. DHCP snooping runs on untrusted links to provide subscriber identity. Figure 13: DHCP Snooping in an Aggregation Network, on page 98 shows an aggregation network. The link from the DSLAM to the aggregation network is untrusted and is the point of presence for DHCP snooping. The links connecting the switches in the aggregation network and the link from the aggregation network to the intelligent edge is considered trusted.

Note Enabling both DHCP relay on a BVI and DHCP snooping in a bridge domain that has a BVI can result in duplicate DHCP messages from the DHCP client to the DHCP server.

Figure 13: DHCP Snooping in an Aggregation Network



Trusted and Untrusted Ports

On trusted ports, DHCP BOOTREQUEST packets are forwarded by DHCP snooping. The client's address lease is not tracked and the client is not bound to the port. DHCP BOOTREPLY packets are forwarded.

When the first DHCP BOOTREQUEST packet from a client is received on an untrusted port, DHCP snooping binds the client to the bridge port and tracks the clients's address lease. When that address lease expires, the client is deleted from the database and is unbound from the bridge port. Packets from this client received on this bridge port are processed and forwarded as long as the binding exists. Packets that are received on another bridge port from this client are dropped while the binding exists. DHCP snooping only forwards DHCP BOOTREPLY packets for this client on the bridge port that the client is bound to. DHCP BOOTREPLY packets that are received on untrusted ports are not forwarded.

DHCP Snooping in a Bridge Domain

To enable DHCP snooping in a bridge domain, there must be at least two profiles, a trusted profile and an untrusted profile. The untrusted profile is assigned to the client-facing ports, and the trusted profile is assigned to the server-facing ports. In most cases, there are many client facing ports and few server-facing ports. The simplest example is two ports, a client-facing port and a server-facing port, with an untrusted profile explicitly assigned to the client-facing port and a trusted profile assigned to the server-facing port.

Assigning Profiles to a Bridge Domain

Because there are normally many client-facing ports and a small number of server-facing ports, the operator assigns the untrusted profile to the bridge domain. This configuration effectively assigns an untrusted profile to every port in the bridge domain. This action saves the operator from explicitly assigning the untrusted profile to all of the client-facing ports. Because there also must be server-facing ports that have trusted DHCP snooping profiles, in order for DHCP snooping to function properly, this untrusted DHCP snooping profile assignment is overridden to server-facing ports by specifically configuring trusted DHCP snooping profiles on the server-facing ports. For ports in the bridge domain that do not require DHCP snooping, all should have the **none** profile assigned to them to disable DHCP snooping on those ports.

Relay Information Options

You can configure a DHCP snooping profile to insert the relay information option (option 82) into DHCP client packets only when it is assigned to a client port. The **relay information option allow-untrusted** command addresses what to do with DHCP client packets when there is a null giaddr and a relay-information option already in the client packet when it is received. This is a different condition than a DHCP snooping trusted/untrusted port. The **relay information option allow-untrusted** command determines how the DHCP snooping application handles untrusted relay information options.

How to Configure DHCP Snooping

This section contains the following tasks:

Enabling DHCP Snooping in a Bridge Domain

The following configuration creates two ports, a client-facing port and a server-facing port. In Step 1 through Step 8, an untrusted DHCP snooping profile is assigned to the client bridge port and trusted DHCP snooping profile is assigned to the server bridge port. In Step 9 through Step 18, an untrusted DHCP snooping profile is assigned to the bridge domain and trusted DHCP snooping profiles are assigned to server bridge ports.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *untrusted-profile-name* **snoop**
4. **exit**
5. **dhcp ipv4**
6. **profile** *profile-name* **snoop**
7. **trusted**
8. **exit**
9. **l2vpn**

10. **bridge group** *group-name*
11. **bridge-domain** *bridge-domain-name*
12. **interface** *type interface-path-id*
13. **dhcp ipv4 snoop profile** *untrusted-profile-name*
14. **interface** *type interface-path-id*
15. **dhcp ipv4 snoop profile** *trusted-profile-name*
16. **exit**
17. **exit**
18. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 profile configuration submode.
Step 3	**profile** *untrusted-profile-name* **snoop** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop`	Configures an untrusted DHCP snooping profile for the client port.
Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# exit`	Exits DHCP IPv4 profile configuration mode.
Step 5	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enables DHCP for IPv4 and enters DHCP IPv4 profile configuration mode.
Step 6	**profile** *profile-name* **snoop** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile trustedServerProfile snoop`	Configures a trusted DHCP snooping profile for the server port.
Step 7	**trusted** **Example:** `RP/0/RSP0/CPU0:router(config-dhcv4)# trusted`	Configures a DHCP snoop profile to be trusted.

	Command or Action	Purpose
Step 8	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-dhcv4)# exit`	Exits DHCP IPv4 profile configuration mode.
Step 9	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters l2vpn configuration mode.
Step 10	**bridge group** *group-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group ccc`	Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode.
Step 11	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ddd`	Establishes a bridge domain.
Step 12	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/0`	Identifies an interface.
Step 13	**dhcp ipv4 snoop profile** *untrusted-profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile untrustedClientProfile`	Attaches an untrusted DHCP snoop profile to the bridge port.
Step 14	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# gigabitethernet 0/1/0/1`	Identifies an interface.
Step 15	**dhcp ipv4 snoop profile** *trusted-profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile trustedServerProfile`	Attaches a trusted DHCP snoop profile to the bridge port.
Step 16	**exit** **Example:**	Exits the l2vpn bridge group bridge-domain interface configuration submode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit`	
Step 17	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# exit`	Exits the l2vpn bridge group bridge-domain configuration submode.
Step 18	**commit**	

Disabling DHCP Snooping on a Specific Bridge Port

The following configuration enables DHCP to snoop packets on all bridge ports in the bridge domain ISP1 except for bridge port GigabitEthernet 0/1/0/1 and GigabitEthernet 0/1/0/2. DHCP snooping is disabled on bridge port GigabitEthernet 0/1/0/1. Bridge port GigabitEthernet 0/1/0/2 is the trusted port that connects to the server. In this example, no additional features are enabled, so only DHCP snooping is running.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *group-name*
4. **bridge-domain** *bridge-domain-name*
5. **dhcp ipv4 snoop profile** *profile-name*
6. **interface** *type interface-path-id*
7. **dhcp ipv4 none**
8. **interface** *type interface-path-id*
9. **dhcp ipv4 snoop profile** *profile-name*
10. **exit**
11. **exit**
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters l2vpn configuration submode.
Step 3	**bridge group** *group-name* **Example:**	Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Establishes a bridge domain and enters l2vpn bridge group bridge-domain configuration submode.
Step 5	**dhcp ipv4 snoop profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile untrustedClientProfile`	Attaches the untrusted DHCP snooping profile to the bridge domain.
Step 6	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/1`	Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submode.
Step 7	**dhcp ipv4 none** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# dhcp ipv4 none`	Disables DHCP snooping on the port.
Step 8	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/2`	Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submode.
Step 9	**dhcp ipv4 snoop profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile trustedServerProfile`	Attaches the trusted DHCP snooping profile to a port.
Step 10	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bd-bg)# exit`	Exits l2vpn bridge-domain bridge group interface configuration submode.
Step 11	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# exit`	Exits l2vpn bridge-domain submode.

	Command or Action	Purpose
Step 12	**commit**	

Using the Relay Information Option

This task shows how to use the relay information commands to insert the relay information option (option 82) into DHCP client packets and forward DHCP packets with untrusted relay information options.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile** *profile-name* **snoop**
4. **relay information option**
5. **relay information option allow-untrusted**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**dhcp ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv4`	Enters DHCP IPv4 profile configuration submode.
Step 3	**profile** *profile-name* **snoop** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop`	Configures an untrusted DHCP snooping profile for the client port.
Step 4	**relay information option** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option`	Enables the system to insert the DHCP relay information option field in forwarded BOOTREQUEST messages to a DHCP server.
Step 5	**relay information option allow-untrusted** **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option allow-untrusted`	Configures DHCP IPv4 relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero.
Step 6	**commit**	

Configuration Examples for DHCP Snooping

This section provides the following configuration examples:

Assigning a DHCP Profile to a Bridge Domain: Example

The following example shows how to enable DHCP snooping in a bridge domain:

```
l2vpn
 bridge group GRP1
  bridge-domain ISP1
   dhcp ipv4 profile untrustedClientProfile snoop
```

Disabling DHCP Snooping on a Specific Bridge Port: Example

The following example shows how to disable DHCP snooping on a specific bridge port:

```
interface gigabitethernet 0/1/0/1
 dhcp ipv4 none
```

Configuring a DHCP Profile for Trusted Bridge Ports: Example

The following example shows how to configure a DHCP profile for trusted bridge ports:

```
dhcp ipv4 profile trustedServerProfile snoop
 trusted
```

Configuring an Untrusted Profile on a Bridge Domain: Example

The following example shows how to attach a profile to a bridge domain and disable snooping on a bridge port.

```
l2vpn
 bridge group GRP1
  bridge-domain ISP1
   dhcp ipv4 profile untrustedClientProfile snoop
    interface gigabitethernet 0/1/0/1
     dhcp ipv4 none
```

Configuring a Trusted Bridge Port: Example

The following example shows ow to assign a trusted DHCP snooping profile to a bridge port:

```
l2vpn
 bridge group GRP1
  bridge-domain ISP1
   interface gigabitethernet 0/1/0/2
    dhcp ipv4 profile trustedServerProfile snoop
```

DHCPv6 Proxy Binding Table Reload Persistency

The Cisco IOS-XR Dynamic Host Configuration Protocol (DHCP) application is responsible for maintaining the DHCP binding state for the DHCP leases allocated to clients by the DHCP application. These binding states are learned by the DHCP application (proxy/relay/snooping). DHCP clients expect to maintain a DHCP lease regardless of the events that occur to the DHCP application.

Note From Release 6.2.2 onwards, 200K sessions are supported on a proxy or server running DHCPv6.

This feature enables the DHCP application to maintain bind state through the above events:

- Process restart – Local checkpoint
- RP failover – Hot standby RP through checkpoint
- LC IMDR – Local checkpoint
- LC OIR – Shadow table on RP
- System restart – Bindings saved on local disk

Configuring DHCPv6 Proxy Binding Database Write to System Persistent Memory

Perform this task to configure the DHCPv6 binding database write to the system persistent memory. This helps to recover the DHCPv6 binding table after a system reload. The file names used for a full persistent file write are *dhcpv6_srpb_{nodeid}_odd* and *dhcpv6_srpb_{nodeid}_even*. The *nodeid* is the actual node ID of the node where the file is written. The incremental file is named the same way as the full file, with a *_inc* appended to it.

Note From Release 6.2.2 onwards, 200K sessions are supported on a proxy or server running DHCPv6.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv6**
3. **database** [**proxy**] [**full-write-interval** *full-write-interval*] [**incremental-write-interval** *incremental-write-interval*]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**dhcp ipv6** **Example:** `RP/0/RSP0/CPU0:router(config)# dhcp ipv6`	Configures DHCP for IPv6 and enters the DHCPv6 configuration mode.
Step 3	**database** [**proxy**] [**full-write-interval** *full-write-interval*] [**incremental-write-interval** *incremental-write-interval*] **Example:** `RP/0/RSP0/CPU0:router(config-dhcpv6)# database proxy full-write-interval 20 incremental-write-interval 10`	Configures the DHCPv6 binding table write to the system persistent memory and specifies the time interval at which the full write and incremental file write are to be performed. The range, in minutes, for *full-write-interval* and *incremental-write-interval* is from 0 to 1440. The default value is 10 for *full-write-interval* and 1 for *incremental-write-interval*. The DHCP mode should be set as **proxy**.
Step 4	**commit**	

Configuring DHCP binding database write to system persistent memory: Example

```
 configure
 dhcp ipv6
 database proxy full-write-interval 15 incremental-write-interval 5
 !
end
```

DHCP Session MAC Throttle

The ASR9K router supports the DHCP session MAC throttle feature. This feature limits the number of DHCP client requests reaching the ASR9K, based on the MAC address of the DHCP clients. This feature is supported for the DHCPv4 proxy, the DHCPv4 server, and the DHCPV6 proxy. The feature prevents a DHCP client from sending multiple DISCOVER packets to the ASR9K router, within short periods of time. This, in turn, prevents that client from impacting the session establishment of other DHCP clients.

Note From Release 6.2.2 onwards, 200K sessions are supported on a proxy or server running DHCPv6.

A unique throttle entry is created in the system for each unique MAC address received on any interface where the profile is attached.

To configure the DHCP session MAC throttle feature, use the **sessions mac throttle** command in the respective DHCP profile configuration mode.

Configuring DHCP Session MAC Throttle: Example

```
dhcp ipv4
 profile p1 server
  sessions mac throttle 300 60 40
 !
 interface GigabitEthernet0/0/0/0 server profile p1
!
```

Additional References

The following sections provide references related to implementing the Cisco IOS XR DHCP relay agent and DHCP snooping features.

Related Documents

Related Topic	Document Title
Cisco IOS XR DHCP commands	*DHCP Commands* module in the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services* module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

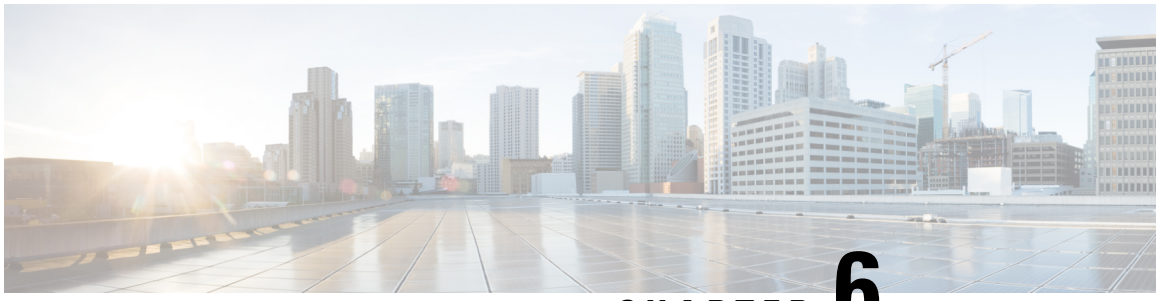
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 2131	*Dynamic Host Configuration Protocol*

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



CHAPTER 6

Implementing Host Services and Applications

Cisco IOS XR software Host Services and Applications features on the router are used primarily for checking network connectivity and the route a packet follows to reach a destination, mapping a hostname to an IP address or an IP address to a hostname, and transferring files between routers and UNIX workstations.

Note For a complete description of host services and applications commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Implementing Host Services and Applications

Release	Modification
Release 3.7.2	This feature was introduced.

Prerequisites for Implementing Host Services and Applications

The following prerequisites are required to implement Cisco IOS XR software Host Services and applications

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Implementing Host Services and Applications

To implement Cisco IOS XR software Host Services and applications features discussed in this document, you should understand the following concepts:

Network Connectivity Tools

Network connectivity tools enable you to check device connectivity by running traceroutes and pinging devices on the network.

Ping

The **ping** command is a common method for troubleshooting the accessibility of devices. It uses two Internet Control Message Protocol (ICMP) query messages, ICMP echo requests, and ICMP echo replies to determine whether a remote host is active. The **ping** command also measures the amount of time it takes to receive the echo reply.

The **ping** command first sends an echo request packet to an address, and then it waits for a reply. The ping is successful only if the echo request gets to the destination, and the destination is able to get an echo reply (hostname is alive) back to the source of the ping within a predefined time interval.

The bulk option has been introduced to check reachability to multiple destinations. The destinations are directly input through the CLI. This option is supported for ipv4 destinations only.

Traceroute

Where the **ping** command can be used to verify connectivity between devices, the **traceroute** command can be used to discover the paths packets take to a remote destination and where routing breaks down.

The **traceroute** command records the source of each ICMP "time-exceeded" message to provide a trace of the path that the packet took to reach the destination. You can use the IP **traceroute** command to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

The **traceroute** command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. The **traceroute** command sends a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, the **traceroute** command sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL increments to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram reaches its destination, the **traceroute** command sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP port unreachable error to the source. This message indicates to the traceroute facility that it has reached the destination.

Domain Services

Cisco IOS XR software domain services acts as a Berkeley Standard Distribution (BSD) domain resolver. The domain services maintains a local cache of hostname-to-address mappings for use by applications, such as Telnet, and commands, such as **ping** and **traceroute** . The local cache speeds the conversion of hostnames to addresses. Two types of entries exist in the local cache: static and dynamic. Entries configured using the **domain ipv4 host** or **domain ipv6 host** command are added as static entries, while entries received from the name server are added as dynamic entries.

The name server is used by the World Wide Web (WWW) for translating names of network nodes into addresses. The name server maintains a distributed database that maps hostnames to IP addresses through the DNS protocol from a DNS server. One or more name servers can be specified using the **domain name-server** command.

When an application needs the IP address of a host or the hostname of an IP address, a remote-procedure call (RPC) is made to the domain services. The domain service looks up the IP address or hostname in the cache, and if the entry is not found, the domain service sends a DNS query to the name server.

You can specify a default domain name that Cisco IOS XR software uses to complete domain name requests. You can also specify either a single domain or a list of domain names. Any IP hostname that does not contain a domain name has the domain name you specify appended to it before being added to the host table. To specify a domain name or names, use either the **domain name** or **domain list** command.

TFTP Server

It is too costly and inefficient to have a machine that acts only as a server on every network segment. However, when you do not have a server on every segment, your network operations can incur substantial time delays across network segments. You can configure a router to serve as a TFTP server to reduce costs and time delays in your network while allowing you to use your router for its regular functions.

Typically, a router that is configured as a TFTP server provides other routers with system image or router configuration files from its flash memory. You can also configure the router to respond to other types of services requests.

File Transfer Services

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), remote copy protocol (rcp) rcp clients, and Secure Copy Protocol (SCP) are implemented as file systems or resource managers. For example, pathnames beginning with tftp:// are handled by the TFTP resource manager.

The file system interface uses URLs to specify the location of a file. URLs commonly specify files or locations on the WWW. However, on Cisco routers, URLs also specify the location of files on the router or remote file servers.

When a router crashes, it can be useful to obtain a copy of the entire memory contents of the router (called a core dump) for your technical support representative to use to identify the cause of the crash. SCP, FTP, TFTP, or rcp can be used to save the core dump to a remote server. See the *System Management Configuration Guide for Cisco ASR 9000 Series Routers* for information on executing a core dump.

RCP

The remote copy protocol (RCP) commands rely on the remote shell (rsh) server (or daemon) on the remote system. To copy files using rcp, you do not need to create a server for file distribution, as you do with TFTP.

You need only to have access to a server that supports the rsh. Because you are copying a file from one place to another, you must have read permissions for the source file and write permission in the destination directory. If the destination file does not exist, rcp creates it for you.

Although Cisco rcp implementation emulates the functions of the UNIX rcp implementation—copying files among systems on the network—Cisco command syntax differs from the UNIX rcp command syntax. Cisco IOS XR software offers a set of copy commands that use rcp as the transport mechanism. These **rcp copy** commands are similar in style to the Cisco IOS XR software TFTP copy commands, but they offer an alternative that provides faster performance and reliable delivery of data. These improvements are possible because the rcp transport mechanism is built on and uses the TCP/IP stack, which is connection-oriented. You can use rcp commands to copy system images and configuration files from the router to a network server and so forth.

FTP

File Transfer Protocol (FTP) is part of the TCP/IP protocol stack, which is used for transferring files between network nodes. FTP is defined in RFC 959.

TFTP

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

SCP

Secure Copy Protocol (SCP) is a file transfer protocol which provides a secure and authenticated method for transferring files. SCP relies on SSHv2 to transfer files from a remote location to a local location or from local location to a remote location.

Cisco IOS XR software supports SCP server and client operations. If a device receives an SCP request, the SSH server process spawns the SCP server process which interacts with the client. For each incoming SCP subsystem request, a new SCP server instance is spawned. If a device sends a file transfer request to a destination device, it acts as the client.

When a device starts an SSH connection to a remote host for file transfer, the remote device can either respond to the request in Source Mode or Sink Mode. In Source Mode, the device is the file source. It reads the file from its local directory and transfers the file to the intended destination. In Sink Mode, the device is the destination for the file to be transferred.

Using SCP, you can copy a file from the local device to a destination device or from a destination device to the local device.

Using SCP, you can only transfer individual files. You cannot transfer a file from a destination device to another destination device.

Cisco inetd

Cisco Internet services process daemon (Cinetd) is a multithreaded server process that is started by the system manager after the system has booted. Cinetd listens for Internet services such as Telnet service, TFTP service, and so on. Whether Cinetd listens for a specific service depends on the router configuration. For example, when the **tftp server** command is entered, Cinetd starts listening for the TFTP service. When a request arrives, Cinetd runs the server program associated with the service.

Telnet

Enabling Telnet allows inbound Telnet connections into a networking device.

How to Implement Host Services and Applications

This section contains the following procedures:

Checking Network Connectivity

As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol. The protocol involves sending a special datagram to the destination host, then waiting for a reply datagram from that host. Results from this echo protocol can help in evaluating the path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

SUMMARY STEPS

1. **ping** [**ipv4** | **ipv6** | **vrf** *vrf-name*] [*host-name* | *ip-address*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**ping** [**ipv4**	**ipv6**	**vrf** *vrf-name*] [*host-name*	*ip-address*] **Example:** `RP/0/RSP0/CPU0:router# ping`	Starts the ping tool that is used for testing connectivity. **Note** If you do not enter a hostname or an IP address on the same line as the **ping** command, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter.

Checking Network Connectivity for Multiple Destinations

The bulk option enables you to check reachability to multiple destinations. The destinations are directly input through the CLI. This option is supported for ipv4 destinations only.

SUMMARY STEPS

1. **ping bulk ipv4** [**input cli** { **batch** | **inline** }]
2. [**vrf** *vrf-name*] [*host-name* | *ip-address*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**ping bulk ipv4** [**input cli** { **batch** | **inline** }] **Example:** `RP/0/RSP0/CPU0:router# ping bulk ipv4 input cli`	Starts the ping tool that is used for testing connectivity.

Step 2	[**vrf** *vrf-name*] [*host-name* | *ip-address*]
	Example:
	`Please enter input via CLI with one destination per line:`
	`vrf myvrf1 1.1.1.1`
	`vrf myvrf2 2.2.2.2`
	`vrf myvrf1 myvrf1.cisco.com`
	`vrf myvrf2 myvrf2.cisco.com`
	
	`Starting pings...`
	`Type escape sequence to abort.`
	`Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:`
	`!`
	`Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms`
	`Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:`
	`!!`
	`Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms`
	`Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:`
	`!`
	`Success rate is 100 percent (1/1), round-trip min/avg/max = 1/4/1 ms`
	`Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:`
	`!!`
	`Success rate is 100 percent (2/2), round-trip min/avg/max = 1/3/1 ms`
		You must hit the Enter button and then specify one destination address per line.

Checking Packet Routes

The **traceroute** command allows you to trace the routes that packets actually take when traveling to their destinations.

SUMMARY STEPS

1. **traceroute** [**ipv4** | **ipv6** | **vrf** *vrf-name*] [*host-name* | *ip-address*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**traceroute** [**ipv4** | **ipv6** | **vrf** *vrf-name*] [*host-name* | *ip-address*] **Example:** `RP/0/RSP0/CPU0:router# traceroute`	Traces packet routes through the network. **Note** If you do not enter a hostname or an IP address on the same line as the **traceroute** command, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter.

Configuring Domain Services

This task allows you to configure domain services.

Before you begin

DNS-based hostname-to-address translation is enabled by default. If hostname-to-address translation has been disabled using the **domain lookup disable** command, re-enable the translation using the **no domain lookup disable** command. See the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers* for more information on the **domain lookup disable** command.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
   - **domain name** *domain-name*
   - or
   - **domain list** *domain-name*
3. **domain name-server** *server-address*
4. **domain** {**ipv4** | **ipv6**} **host** *host-name* {*ipv4address* | *ipv6address*}
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	Do one of the following: • **domain name** *domain-name*	Defines a default domain name used to complete unqualified hostnames.

	Command or Action	Purpose

	• or
	• **domain list** *domain-name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# domain name cisco.com`
	`or`
	`RP/0/RSP0/CPU0:router(config)# domain list domain1.com`	

Step 3	**domain name-server** *server-address* **Example:** `RP/0/RSP0/CPU0:router(config)# domain name-server 192.168.1.111`	Specifies the address of a name server to use for name and address resolution (hosts that supply name information). **Note** You can enter up to six addresses, but only one for each command.
Step 4	**domain** {**ipv4** | **ipv6**} **host** *host-name* {*ipv4address* | *ipv6address*} **Example:** `RP/0/RSP0/CPU0:router(config)# domain ipv4 host1 192.168.7.18`	(Optional) Defines a static hostname-to-address mapping in the host cache using IPv4 or IPv6 . **Note** You can bind up to eight additional associated addresses to a hostname.
Step 5	**commit**	

Configuring a Router as a TFTP Server

This task allows you to configure the router as a TFTP server so other devices acting as TFTP clients are able to read and write files from and to the router under a specific directory, such as slot0:, /tmp, and so on (TFTP home directory).

Note For security reasons, the TFTP server requires that a file must already exist for a write request to succeed.

Before you begin

The server and client router must be able to reach each other before the TFTP function can be implemented. Verify this connection by testing the connection between the server and client router (in either direction) using the **ping** command.

SUMMARY STEPS

1. **configure**
2. **tftp** {**ipv4** | **ipv6**} **server** {**homedir** *tftp-home-directory*} {**max-servers** *number*} [**access-list** *name*]
3. **commit**
4. show cinetd services

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**tftp** {**ipv4** | **ipv6**} **server** {**homedir** *tftp-home-directory*} {**max-servers** *number*} [**access-list** *name*] **Example:** `RP/0/RSP0/CPU0:router(config)# tftp ipv4 server access-list listA homedir disk0`	Specifies: • IPv4 or IPv6 address prefixes (required) • Home directory (required) • Maximum number of concurrent TFTP servers (required) • Name of the associated access list (optional)
Step 3	**commit**	
Step 4	show cinetd services **Example:** `RP/0/RSP0/CPU0:router# show cinetd services`	Displays the network service for each process. The service column shows TFTP if the TFTP server is configured.

Configuring a Router to Use rcp Connections

This task allows you to configure a router to use rcp.

Before you begin

For the rcp copy request to execute successfully, an account must be defined on the network server for the remote username.

If you are reading or writing to the server, the rcp server must be properly configured to accept the rcp read/write request from the user on the router. For UNIX systems, you must add an entry to the hosts file for the remote user on the rcp server.

SUMMARY STEPS

1. **configure**
2. **rcp client username** *username*
3. **rcp client source-interface** *type interface-path-id*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rcp client username** *username* **Example:** `RP/0/RSP0/CPU0:router(config)# rcp client username netadmin1`	Specifies the name of the remote user on the rcp server. This name is used when a remote copy using rcp is requested. If the rcp server has a directory structure, all files and images to be copied are searched for or written relative to the directory in the remote user account.
Step 3	**rcp client source-interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# rcp client source-interface gigabitethernet 1/0/2/1`	Sets the IP address of an interface as the source for all rcp connections.
Step 4	**commit**	

Troubleshooting Tips

When using rcp to copy any file from a source to a destination, use the following path format:

```
copy rcp
:
//username
@
{
hostname
 |
ipaddress
}/
directory-path
/
pie-name target-device
```

When using an IPv6 rcp server, use the following path format:

```
copy rcp
:
//username
@
[ipv6-address]/
directory-path
/
pie-name
```

See the **copy** command in the *System Management Command Reference for Cisco ASR 9000 Series Routers* for detailed information on using rcp protocol with the **copy** command.

Configuring a Router to Use FTP Connections

This task allows you to configure the router to use FTP connections for transferring files between systems on the network. With the the Cisco ASR 9000 Series Routerimplementation of FTP, you can set the following FTP characteristics:

- Passive-mode FTP
- Password
- IP address

SUMMARY STEPS

1. **configure**
2. **ftp client passive**
3. **ftp client anonymous-password** *password*
4. **ftp client source-interface** *type interface-path-id*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ftp client passive** **Example:** `RP/0/RSP0/CPU0:router(config)# ftp client passive`	Allows the software to use only passive FTP connections.
Step 3	**ftp client anonymous-password** *password* **Example:** `RP/0/RSP0/CPU0:router(config)# ftp client anonymous-password xxxx`	Specifies the password for anonymous users.
Step 4	**ftp client source-interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# ftp client source-interface GigabitEthernet 0/1/2/1`	Specifies the source IP address for FTP connections.
Step 5	**commit**	

Troubleshooting Tips

When using FTP to copy any file from a source to a destination, use the following path format:

```
copy ftp
://
username:password
@
{
hostname
 |
ipaddress
}/
directory-path
/
pie-name target-device
```

When using an IPv6 FTP server, use the following path format:

```
copy ftp
:
//username
:
password
@
[ipv6-address]/
directory-path
/
pie-name
```

If unsafe or reserved characters appear in the username, password, hostname, and so on, they have to be encoded (RFC 1738).

The following characters are unsafe:

```
"<", ">", "#", "%" "{", "}", "|", "□", "~", "[", "]", and "'"
```

The following characters are reserved:

```
":", "/" "?", ":", "@", and "&"
```

The *directory-path* is a relative path to the home directory of the user. The slash (/) has to be encoded as %2f to specify the absolute path. For example:

```
ftp://user:password@hostname/%2fTFTPboot/directory/pie-name
```

See the **copy** command in the *System Management Command Reference for Cisco ASR 9000 Series Routers* for detailed information on using FTP protocol with the **copy** command.

Configuring a Router to Use TFTP Connections

This task allows you to configure a router to use TFTP connections. You must specify the source IP address for a TFTP connection.

SUMMARY STEPS

1. **configure**
2. **tftp client source-interface** *type*
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**tftp client source-interface** *type* **Example:** `RP/0/RSP0/CPU0:router(config)# tftp client source-interface GigabitEthernet 1/0/2/1`	Specifies the source IP address for TFTP connections.
Step 3	**commit**	

Troubleshooting Tips

When using TFTP to copy any file from a source to a destination, use the following path format:

```
copy tftp
://{
hostname
 |
ipaddress
}/
directory-path
/
pie-name target-device
```

When using an IPv6 TFTP server, use the following path format:

```
copy tftp
:
//
[ipv6-address]/
directory-path
/
pie-name
```

See the **copy** command in the *System Management Command Reference for Cisco ASR 9000 Series Routers* for detailed information on using TFTP protocol with the **copy** command.

Configuring Telnet Services

This task allows you to configure Telnet services.

SUMMARY STEPS

1. **configure**
2. **telnet** [**ipv4** | **ipv6** | **vrf** *vrf-name*] **server max-servers 1**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**telnet** [**ipv4**	**ipv6**	**vrf** *vrf-name*] **server max-servers 1** **Example:** `RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 1`	Enables one inbound Telnet server on the router. **Note** This command affects only inbound Telnet connections to the router.
Step 3	**commit**	

Transferring Files Using SCP

Secure Copy Protocol (SCP) allows you to transfer files between source and destination devices.

SUMMARY STEPS

1. Do one of the following:
   - **scp** *local-directory/filename username@location/directory/filename*
   - **scp** *username@location/directory/filename local-directory/filename*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Do one of the following: • **scp** *local-directory/filename username@location/directory/filename*	Use the **scp** *local-directory/filename username@location/directory/filename* command to transfer a file from a local directory to a remote directory.

	Command or Action	Purpose

	• **scp** *username@location/directory/filename local-directory/filename*
	Example:
	`RP/0/RSP0/CPU0:router# scp /usr/file1.txt root@209.165.200.1:/root/file3.txt`
	`or`
	`RP/0/RSP0/CPU0:router# scp root@209.165.200.1:/root/file4.txt /usr/file.txt`
		Use the **scp** *username@location/directory/filename local-directory/filename* to transfer a file from a remote directory to a local directory.
		You can transfer one file at a time. If the destination is a server, SSH server process must be running.

Configuring syslog source-interface

Perform this task to configure the logging source interface to identify the syslog traffic, originating in a VRF from a particular router, as coming from a single device.

SUMMARY STEPS

1. **configure**
2. **logging source-interface** *interface* **vrf** *vrf-name*
3. **commit**
4. **show running-configuration logging**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**logging source-interface** *interface* **vrf** *vrf-name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# logging source-interface loopback 0 vrf vrf1`
	`RP/0/RSP0/CPU0:router(config)# logging source-interface loopback 1 vrf default`
		Configures the logging source interface to identify the syslog traffic, originating in a VRF from a particular router, as coming from a single device.

Step 3	**commit**	

Step 4	**show running-configuration logging**
	Example:
	`RP/0/RSP0/CPU0:router(config)# exit`
	`RP/0/RSP0/CPU0:router# show running-configuration logging`
		Verifies that the logging source is correctly configured for the VRF.

	Command or Action	Purpose

	`logging trap debugging`
	`logging 223.255.254.249 vrf vrf1`
	`logging 223.255.254.248 vrf default`
	`logging source-interface Loopback0 vrf vrf1`
	`logging source-interface Loopback1`	

IPv6 Support for IP SLA ICMP Echo Operation

IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation is used to monitor the end-to-end response time between a Cisco router and devices using IP. ICMP Echo is useful for troubleshooting network connectivity issues.

Configuring an IPSLA ICMP echo operation

To monitor IP connections on a device, use the IP SLA ICMP Echo operation. This operation does not require the IP SLAs Responder to be enabled.

SUMMARY STEPS

1. **configure**
2. **ipsla**
3. **operation** *n*
4. **type icmp echo**
5. **timeout** *n*
6. **source address** *address*
7. **destination address** *address*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipsla** **Example:** `RP/0/RSP0/CPU0:router(config)# ipsla`	Enters IP SLA monitor configuration mode.
Step 3	**operation** *n* **Example:** `RP/0/RSP0/CPU0:router(config-ipsla)# operation 500`	Initiates configuration for an IP SLA operation.

	Command or Action	Purpose
Step 4	**type icmp echo** **Example:** `RP/0/RSP0/CPU0:router(config-ipsla-op)# type icmp echo`	Enters IP SLA ICMP Echo configuration mode.
Step 5	**timeout** *n* **Example:** `RP/0/RSP0/CPU0:router(config-ipsla-icmp-echo)# timeout 1000`	Sets the timeout in ms. The default is 5000 milliseconds.
Step 6	**source address** *address* **Example:** `RP/0/RSP0/CPU0:router(config-ipsla-icmp-echo)# source address fe80::226:98ff:fe2e:3287`	Configures the address of the source device.
Step 7	**destination address** *address* **Example:** `RP/0/RSP0/CPU0:router(config-ipsla-icmp-echo)# destination address fe80::226:98ff:fe2e:3287`	Configures the address of the destination device.
Step 8	**commit**	

Configuration Examples for Implementing Host Services and Applications

This section provides the following configuration examples:

Checking Network Connectivity: Example

The following example shows an extended **ping** command sourced from the Router A Ethernet 0 interface and destined for the Router B Ethernet interface. If this ping succeeds, it is an indication that there is no routing problem. Router A knows how to get to the Ethernet of Router B, and Router B knows how to get to the Ethernet of Router A. Also, both hosts have their default gateways set correctly.

If the extended **ping** command from Router A fails, it means that there is a routing problem. There could be a routing problem on any of the three routers: Router A could be missing a route to the subnet of Router B's Ethernet, or to the subnet between Router C and Router B; Router B could be missing a route to the subnet of Router A's subnet, or to the subnet between Router C and Router A; and Router C could be missing a route to the subnet of Router A's or Router B's Ethernet segments. You should correct any routing problems, and then Host 1 should try to ping Host 2. If Host 1 still cannot ping Host 2, then both hosts' default gateways

should be checked. The connectivity between the Ethernet of Router A and the Ethernet of Router B is checked with the extended **ping** command.

With a normal ping from Router A to Router B's Ethernet interface, the source address of the ping packet would be the address of the outgoing interface; that is, the address of the serial 0 interface (172.31.20.1). When Router B replies to the ping packet, it replies to the source address (that is, 172.31.20.1). This way, only the connectivity between the serial 0 interface of Router A (172.31.20.1) and the Ethernet interface of Router B (192.168.40.1) is tested.

To test the connectivity between Router A's Ethernet 0 (172.16.23.2) and Router B's Ethernet 0 (192.168.40.1), we use the extended **ping** command. With extended **ping**, we get the option to specify the source address of the **ping** packet.

In this example, the extended **ping** command verifies the IP connectivity between the two IP addresses 10.0.0.2 and 10.0.0.1.

```
ping

Protocol [ip]:
Target IP address: 10.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface: 10.0.0.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.58.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/49 ms
```

The **traceroute** command is used to discover the paths packets take to a remote destination and where routing breaks down. The **traceroute** command provides the path between the two IP addresses and does not indicate any problems along the path.

```
traceroute

Protocol [ip]:
Target IP address: ena-view3
Source address: 10.0.58.29
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.
Tracing the route to 171.71.164.199

1 sjc-jpollock-vpn.cisco.com (10.25.0.1) 30 msec 4 msec 4 msec
 2  15lab-vlan525-gw1.cisco.com (172.19.72.2) 7 msec  5 msec  5 msec
 3  sjc15-00lab-gw1.cisco.com (172.24.114.33) 5 msec  6 msec  6 msec
 4  sjc5-lab4-gw1.cisco.com (172.24.114.89) 5 msec  5 msec  5 msec
```

```
 5  sjc5-sbb4-gw1.cisco.com (171.71.241.162) 5 msec  6 msec  6 msec
 6  sjc5-dc5-gw1.cisco.com (171.71.241.10) 6 msec  6 msec  5 msec
 7  sjc5-dc1-gw1.cisco.com (171.71.243.2) 7 msec  8 msec  8 msec
 8 ena-view3.cisco.com (171.71.164.199) 6 msec * 8 msec
```

Configuring Domain Services: Example

The following example shows how to configure domain services on a router.

Defining the Domain Host

```
configure

domain ipv4 host host1 192.168.7.18
domain ipv4 host bost2 10.2.0.2 192.168.7.33
```

Defining the Domain Name

```
configure
domain name cisco.com
```

Specifying the Addresses of the Name Servers

```
configure

domain name-server 192.168.1.111
domain name-server 192.168.1.2
```

Configuring a Router to Use rcp, FTP, or TFTP Connections: Example

The following example shows how to configure the router to use rcp, FTP, or TFTP connections.

Using rcp

```
configure

rcp client username netadmin1
rcp client source-interface gigabitethernet 1/0/2/1
```

Using FTP

```
configure

ftp client passive
ftp client anonymous-password xxxx
ftp client source-interface gigabitethernet 0/1/2/1
```

Using TFTP

```
configure
tftp client source-interface gigabitethernet 1/0/2/1
```

Additional References

The following sections provide references related to implementing host services and addresses on the Cisco ASR 9000 Series Router.

Related Documents

Related Topic	Document Title
Host services and applications commands	*Host Services and Applications Commands* module in *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

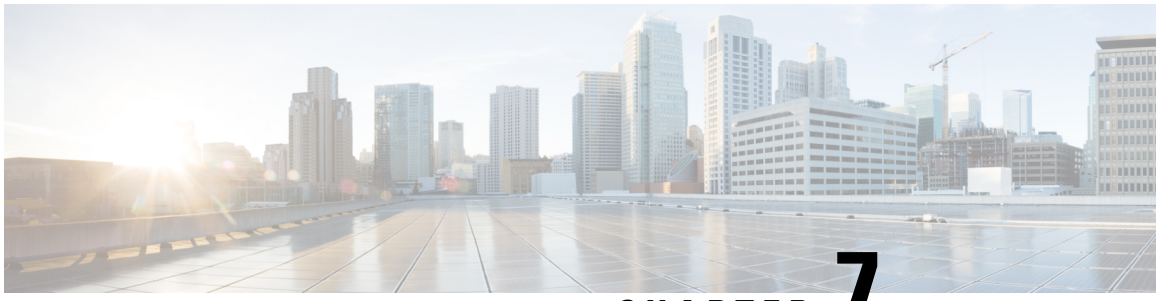
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
RFC-959	File Transfer Protocol
RFC-1738 and RFC-2732	Uniform Resource Locators (URL)
RFC-783	Trivial File Transfer Protocol

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



CHAPTER 7

Implementing Access Lists and Prefix Lists

An access control list (ACL) consists of one or more access control entries (ACE) that collectively define the network traffic profile. This profile can then be referenced by Cisco IOS XR softwarefeatures such as traffic filtering, route filtering, QoS classification, and access control. Each ACL includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

Prefix lists are used in route maps and route filtering operations and can be used as an alternative to access lists in many Border Gateway Protocol (BGP) route filtering commands. A prefix is a portion of an IP address, starting from the far left bit of the far left octet. By specifying exactly how many bits of an address belong to a prefix, you can then use prefixes to aggregate addresses and perform some function on them, such as redistribution (filter routing updates).

This module describes the new and revised tasks required to implement access lists and prefix lists on the Cisco ASR 9000 Series Router

Note For a complete description of the access list and prefix list commands listed in this module, refer to the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Feature History for Implementing Access Lists and Prefix Lists

Release	Modification
Release 3.7.2	This feature was introduced.
Release 4.2.1	IPv6 ACL over BVI interface feature was added.
Release 4.2.1	ACL in Class map feature was added.
Release 5.3.2	Multi-level ACL Chaining feature was added for Cisco ASR 9000 High Density 100GE Ethernet Line Card.

Prerequisites for Implementing Access Lists and Prefix Lists

The following prerequisite applies to implementing access lists and prefix lists:

All command task IDs are listed in individual command references and in the Cisco IOS XR Task ID Reference Guide.If you need assistance with your task group assignment, contact your system administrator.

Restrictions for Implementing Access Lists and Prefix Lists

The following restrictions apply to implementing access lists and prefix lists:

- From Release 5.3.2 onward, on Cisco ASR 9000 High Density 100GE Ethernet Line Cards, up to 4095 unique IPv4 and Ethernet Service (ES) ACLs and up to 4095 unique IPv6 ACLs are supported.
- IPv4 ACLs are not supported for loopback and interflex interfaces.
- IPv4 and IPv6 ACLs are not supported on service application and service infrastructure interfaces.
- If the TCAM utilization is high and large ACLs are modified, then an error may occur. During such instances, do the following to edit an ACL:

Note

1. Remove the ACL from the interface.
2. Reconfigure the ACL.
3. Reapply the ACL to the interface.

Use the **show prm server tcam summary all acl all location** and **show pfilter-ea fea summary location** commands to view the TCAM utilization.

- Filtering of MPLS packets through common ACL and interface ACL is not supported.

  If the packet comes on an ASR 9000 Ethernet Line Card, and is labeled as part of an MPLS flow, then the ingress ASR 9000 Ethernet Line Card cannot apply ACL. Also, for ASR 9000 Ethernet Line Cards, if the label is popped because it is routed to an attached customer edge (CE), then the egress line card (LC) sees a plain IP. But, it still cannot apply an egress (outbound) ACL on the IP packet. Whereas, an ASR 9000 Enhanced Ethernet Line Card can perform an egress IP ACL on this packet before sending it to the directly attached CE.

- Video Monitoring is not supported through ACLs on IPv6 interfaces.
- You can configure an ACL name with a maximum of 64 characters.
- You can configure an ACL name to comprise of only letters and numbers.
- In IPv6 Egress ACLs, TCP flag filtering does not function for IPv6 packets with a fragmentation header. As a result, IPv6 packets with both a fragmentation header and a TCP header (ACK+SYN flags) are not appropriately filtered by the ACL rules.

Restrictions for Implementing ACL-Based Forwarding

The following restrictions apply for implementing ACL-based forwarding (ABF):

- ABF is not supported for **for-us** packets (packets destined for the router).
- The following nexthop configurations are not supported: attaching ACL having a nexthop option in the egress direction, modifying an ACL attached in the egress direction having nexthop, denying an ACE with a nexthop.
- The A9K-SIP-700 LC and ASR 9000 Enhanced Ethernet LC support ABFv4 and ABFv6 in Release 4.2.0. ASR 9000 Ethernet LC does not support ABFv6 in Release 4.2.0, it only supports ABFv4.
- ABFv4 is supported on BVI interfaces for ASR 9000 Enhanced Ethernet line card. It is not supported for ASR 9000 Ethernet line card.

Note Nexthop egress over A9K-SIP-700 line card, ASR 9000 Ethernet line card, or virtual interfaces like GRE or BVI is supported when ABFv4 is configured for a BVI interface.

- ABFv6 is supported on IRB/BVI interfaces for ASR 9000 Enhanced Ethernet line card. It is not supported for ASR 9000 Ethernet line card.

Note There is one exception to this. In case of IP to TAG, the label is imposed by the ingress LC (based on ABF nexthop), and the packet crosses the fabric as a tag packet. These packets are handled by A9K-SIP-700 without any issue.

- Packets punted in the ingress direction from the NPU to the LC CPU are not subjected to ABF treatment due to lack of ABF support in the slow path.
- IP packet(s) needing fragmentation are not subjected to ABF. The packet is forwarded in the traditional way. Fragmented packets received are handled by ABF.

Hardware Limitations

- Support for ABF is only for IPv4 and Ethernet line cards. IPv6 and other interfaces are not supported.
- ABF is an ingress line card feature and the egress line card must be ABF aware.

Information About Implementing Access Lists and Prefix Lists

To implement access lists and prefix lists, you must understand the following concepts:

Access Lists and Prefix Lists Feature Highlights

This section lists the feature highlights for access lists and prefix lists.

- Cisco IOS XR software provides the ability to clear counters for an access list or prefix list using a specific sequence number.
- Cisco IOS XR software provides the ability to copy the contents of an existing access list or prefix list to another access list or prefix list.
- Cisco IOS XR software allows users to apply sequence numbers to permit or deny statements and to resequence, add, or remove such statements from a named access list or prefix list.

Note Resequencing is only for IPv4 prefix lists.

- Cisco IOS XR software does not differentiate between standard and extended access lists. Standard access list support is provided for backward compatibility.
- To double the TCAM scale value of the extended ACL for IPv4/IPv6 in Cisco ASR 9000 High Density 100GE Ethernet line cards, users must disable ISSU (and reload).
- Layer 2 (Ethernet) ACL is supported on Layer 2 interfaces.

- Layer 3 (IPv4 and IPv6) ACL over Layer 2 interfaces for the IPOE model is supported in both ingress and egress directions.

Purpose of IP Access Lists

Access lists perform packet filtering to control which packets move through the network and where. Such controls help to limit network traffic and restrict the access of users and devices to the network. Access lists have many uses, and therefore many commands accept a reference to an access list in their command syntax. Access lists can be used to do the following:

- Filter incoming packets on an interface.
- Filter outgoing packets on an interface.
- Restrict the contents of routing updates.
- Limit debug output based on an address or protocol.
- Control vty access.
- Identify or classify traffic for advanced features, such as congestion avoidance, congestion management, and priority and custom queueing.

How an IP Access List Works

An access list is a sequential list consisting of permit and deny statements that apply to IP addresses and possibly upper-layer IP protocols. The access list has a name by which it is referenced. Many software commands accept an access list as part of their syntax.

An access list can be configured and named, but it is not in effect until the access list is referenced by a command that accepts an access list. Multiple commands can reference the same access list. An access list can control traffic arriving at the router or leaving the router, but not traffic originating at the router. Note that, traffic such as SSH, ICMP and telnet traffic are blocked by ACL, in spite of being originated from the router. This is because, those packets are not injected as high priority packets, and hence get subjected to ACL processing. At the same time, BGP traffic bypasses the ACL applied on the interface, as it is a control packet which is injected as a critical inject packet from RSP or LC. Such packets are handled in the system with high priority and do not get dropped.

IP Access List Process and Rules

Use the following process and rules when configuring an IP access list:

- The software tests the source or destination address or the protocol of each packet being filtered against the conditions in the access list, one condition (permit or deny statement) at a time.
- If a packet does not match an access list statement, the packet is then tested against the next statement in the list.
- If a packet and an access list statement match, the remaining statements in the list are skipped and the packet is permitted or denied as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered.

- If the access list denies the address or protocol, the software discards the packet and returns an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP is configurable in the Cisco IOS XR software.
- If no conditions match, the software drops the packet because each access list ends with an unwritten or implicit deny statement. That is, if the packet has not been permitted or denied by the time it was tested against each statement, it is denied.
- The access list should contain at least one permit statement or else all packets are denied.
- Because the software stops testing conditions after the first match, the order of the conditions is critical. The same permit or deny statements specified in a different order could result in a packet being passed under one circumstance and denied in another circumstance.
- Only one access list per interface, per protocol, per direction is allowed.
- Inbound access lists process packets arriving at the router. Incoming packets are processed before being routed to an outbound interface. An inbound access list is efficient because it saves the overhead of routing lookups if the packet is to be discarded because it is denied by the filtering tests. If the packet is permitted by the tests, it is then processed for routing. For inbound lists, permit means continue to process the packet after receiving it on an inbound interface; **deny** means discard the packet.
- Outbound access lists process packets before they leave the router. Incoming packets are routed to the outbound interface and then processed through the outbound access list. For outbound lists, permit means send it to the output buffer; deny means discard the packet.
- An access list can not be removed if that access list is being applied by an access group in use. To remove an access list, remove the access group that is referencing the access list and then remove the access list.
- An access list must exist before you can use the **ipv4 access group** command.

Helpful Hints for Creating IP Access Lists

Consider the following when creating an IP access list:

- Create the access list before applying it to an interface.
- Organize your access list so that more specific references in a network or subnet appear before more general ones.
- To make the purpose of individual statements more easily understood at a glance, you can write a helpful remark before or after any statement.

Source and Destination Addresses

Source address and destination addresses are two of the most typical fields in an IP packet on which to base an access list. Specify source addresses to control packets from certain networking devices or hosts. Specify destination addresses to control packets being sent to certain networking devices or hosts.

Wildcard Mask and Implicit Wildcard Mask

Address filtering uses wildcard masking to indicate whether the software checks or ignores corresponding IP address bits when comparing the address bits in an access-list entry to a packet being submitted to the access list. By carefully setting wildcard masks, an administrator can select a single or several IP addresses for permit or deny tests.

Wildcard masking for IP address bits uses the number 1 and the number 0 to specify how the software treats the corresponding IP address bits. A wildcard mask is sometimes referred to as an *inverted mask*, because a 1 and 0 mean the opposite of what they mean in a subnet (network) mask.

- A wildcard mask bit 0 means *check* the corresponding bit value.
- A wildcard mask bit 1 means *ignore* that corresponding bit value.

You do not have to supply a wildcard mask with a source or destination address in an access list statement. If you use the **host** keyword, the software assumes a wildcard mask of 0.0.0.0.

From Release 5.2.2, you can supply a wildcard mask with a source or destination address in an access list statement. The wildcard masking feature now supports IPv6 ACL with wildcard masking. This feature is supported in ASR 9000 Enhanced Ethernet Line Card.

Unlike subnet masks, which require contiguous bits indicating network and subnet to be ones, wildcard masks allow noncontiguous bits in the mask. For IPv6 access lists, only contiguous bits are supported.

You can also use CIDR format (/x) in place of wildcard bits. For example, the IPv4 address 1.2.3.4 0.255.255.255 corresponds to 1.2.3.4/8 and for IPv6 address 2001:db8:abcd:0012:0000:0000:0000:0000 corresponds to 2001:db8:abcd:0012::0/64.

Transport Layer Information

You can filter packets on the basis of transport layer information, such as whether the packet is a TCP, UDP, ICMP, or IGMP packet.

IP Access List Entry Sequence Numbering

The ability to apply sequence numbers to IP access-list entries simplifies access list changes. Prior to this feature, there was no way to specify the position of an entry within an access list. If a user wanted to insert an entry (statement) in the middle of an existing list, all the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

The IP Access List Entry Sequence Numbering feature allows users to add sequence numbers to access-list entries and resequence them. When you add a new entry, you choose the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry.

Sequence Numbering Behavior

The following details the sequence numbering behavior:

- If entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum configurable sequence number is 2147483643 for IPv4 and IPv6 entries. For other entries, the maximum configurable sequence number is 2147483646. If the generated sequence number exceeds this maximum number, the following message displays:

```
Exceeded maximum sequence number.
```

- If you provide an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.
- ACL entries can be added without affecting traffic flow and hardware performance.

- If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.
- Distributed support is provided so that the sequence numbers of entries in the route processor (RP) and line card (LC) are synchronized at all times.
- This feature works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable.

Understanding IP Access List Logging Messages

Cisco IOS XR software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the access list causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** command in global configuration mode.

Note ACL logging isn't supported for ingress MPLS packets.

The first packet that triggers the access list causes an immediate logging message, and subsequent packets are collected over 5-minute intervals before they are displayed or logged.

However, you can use the { **ipv4 | ipv6** } **access-list log-update threshold** command to set the number of packets that, when they match an access list (and are permitted or denied), cause the system to generate a log message. You might do this to receive log messages more frequently than at 5-minute intervals.

Caution If you set the *update-number* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 isn't recommended because the volume of log messages could overwhelm the system.

Even if you use the { **ipv4 | ipv6} access-list log-update threshold** command, the 5-minute timer remains in effect, so each cache is emptied at the end of 5 minutes, regardless of the number of messages in each cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it's when a threshold isn't specified.

Note The logging facility might drop some logging message packets if there are too many to be handled or if more than one logging message is handled in 1 second. This behavior prevents the router from using excessive CPU cycles because of too many logging packets. Therefore, the logging facility shouldn't be used as a billing tool or as an accurate source of the number of matches to an access list.

Enable Logging on ACE

This section shows you how to enable the ACE of an ACL to log informational messages when it matches incoming packets, using the optional keyword **log**. The router supports this feature only for IPv4 or IPv6 ingress ACLs. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

```
Router#configure
Router(config)#ipv4 access-list test
Router(config-ipv4-acl)#10 permit udp 10.85.1.0 255.255.255.0 log
Router(config-ipv4-acl)#exit
Router(config)# interface FortyGigE0/0/0/22
Router(config-if)# ipv4 access-group test ingress
Router(config-if)# commit
```

Note Set log-level to **informational** or higher with the **logging console** command, so that the router displays the ACL log-messages on the console.

```
Router#configure
Router(config)#logging console informational
Router(config)# commit
```

For more information on log-levels, see section *Syslog Message Severity Levels* in the *Implementing System Logging* chapter of the *System Monitoring Configuration Guide*.

The following snippet shows a sample log message:

```
Router: ipv4_acl_mgr[350]: %ACL-IPV4_ACL-6-IPACCESSLOGP : access-list test (10) permit udp

10.85.1.2(0) -> 10.0.0.1(0), 1 packet
```

Extended Access Lists with Fragment Control

In earlier releases, the non-fragmented packets and the initial fragments of a packet were processed by IP extended access lists (if you apply this access list), but non-initial fragments were permitted, by default. However, now, the IP Extended Access Lists with Fragment Control feature allows more granularity of control over non-initial fragments of a packet. Using this feature, you can specify whether the system examines non-initial IP fragments of packets when applying an IP extended access list.

As non-initial fragments contain only Layer 3 information, these access-list entries containing only Layer 3 information, can now be applied to non-initial fragments also. The fragment has all the information the system requires to filter, so the access-list entry is applied to the fragments of a packet.

This feature adds the optional **fragments** keyword to the following IP access list commands: **deny (IPv4), permit (IPv4)** , **deny (IPv6)** , **permit (IPv6).** By specifying the **fragments** keyword in an access-list entry, that particular access-list entry applies only to non-initial fragments of packets; the fragment is either permitted or denied accordingly.

The behavior of access-list entries regarding the presence or absence of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then...

...no **fragments** keyword and all of the access-list entry information matches	For an access-list entry containing only Layer 3 information:
	• The entry is applied to non-fragmented packets, initial fragments, and non-initial fragments.
	
	For an access-list entry containing Layer 3 and Layer 4 information:
	• The entry is applied to non-fragmented packets and initial fragments.
	  • If the entry matches and is a permit statement, the packet or fragment is permitted.
	  • If the entry matches and is a deny statement, the packet or fragment is denied.
	• The entry is also applied to non-initial fragments in the following manner. Because non-initial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
	  • If the entry is a **permit** statement, the non-initial fragment is permitted.
	  • If the entry is a deny statement, the next access-list entry is processed.
	
	Note Note that the deny statements are handled differently for non-initial fragments versus non-fragmented or initial fragments.

...the **fragments** keyword and all of the access-list entry information matches	The access-list entry is applied only to non-initial fragments. **Note** The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

You should not add the **fragments** keyword to every access-list entry, because the first fragment of the IP packet is considered a non-fragment and is treated independently of the subsequent fragments. Because an initial fragment will not match an access list permit or deny entry that contains the **fragments** keyword, the packet is compared to the next access list entry until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every deny entry. The first deny entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second deny entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single deny access-list entry with the **fragments** keyword for that host is all that has to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each fragment counts individually as a packet in access-list accounting and access-list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Note Within the scope of ACL processing, Layer 3 information refers to fields located within the IPv4 header; for example, source, destination, protocol. Layer 4 information refers to other data contained beyond the IPv4 header; for example, source and destination ports for TCP or UDP, flags for TCP, type and code for ICMP.

Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through Layer 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Comments About Entries in Access Lists

You can include comments (remarks) about entries in any named IP access list using the **remark** access list configuration command. The remarks make the access list easier for the network administrator to understand and scan. Each remark line is limited to 255 characters.

The remark can go before or after a **permit** or **deny** statement. You should be consistent about where you put the remark so it is clear which remark describes which **permit** or **deny** statement. For example, it would be confusing to have some remarks *before* the associated **permit** or **deny** statements and some remarks *after* the associated statements. Remarks can be sequenced.

Remember to apply the access list to an interface or terminal line after the access list is created. See the"Applying Access Lists, on page 151" section for more information.

Access Control List Counters

In Cisco IOS XR software, ACL counters are maintained both in hardware and software. Hardware counters are used for packet filtering applications such as when an access group is applied on an interface. Software counters are used by all the applications mainly involving software packet processing.

Packet filtering makes use of 64-bit hardware counters per ACE. If the same access group is applied on interfaces that are on the same line card in a given direction, the hardware counters for the ACL are shared between two interfaces.

To display the hardware counters for a given access group, use the **show access-lists ipv4** [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**location** *node-id*}] command in EXEC mode.

To clear the hardware counters, use the **clear access-list ipv4** *access-list-name* [**hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**location** *node-id*}] command in EXEC mode.

Hardware counting is not enabled by default for IPv4 ACLs because of a small performance penalty. To enable hardware counting, use the **ipv4 access-group** *access-list-name* {**ingress** | **egress**} [**hardware-count**]

command in interface configuration mode. This command can be used as desired, and counting is enabled only on the specified interface.

Note Hardware counters are enabled by default on 100Gigabit ethernet interfaces, Cisco ASR 9000 Ethernet line cards, and Cisco ASR 9000 Enhanced Ethernet line cards.

Software counters are updated for the packets processed in software, for example, exception packets punted to the LC CPU for processing, or ACL used by routing protocols, and so on. The counters that are maintained are an aggregate of all the software applications using that ACL. To display software-only ACL counters, use the **show access-lists ipv4** *access-list-name* [**sequence** *number*] command in EXEC mode.

All the above information is true for IPv6, except that hardware counting is always enabled; there is no **hardware-count** option in the IPv6 access-group command-line interface (CLI).

BGP Filtering Using Prefix Lists

Prefix lists can be used as an alternative to access lists in many BGP route filtering commands. The advantages of using prefix lists are as follows:

- Significant performance improvement in loading and route lookup of large lists.
- Incremental updates are supported.
- More user friendly CLI. The CLI for using access lists to filter BGP updates is difficult to understand and use because it uses the packet filtering format.
- Greater flexibility.

Before using a prefix list in a command, you must set up a prefix list, and you may want to assign sequence numbers to the entries in the prefix list.

How the System Filters Traffic by Prefix List

Filtering by prefix list involves matching the prefixes of routes with those listed in the prefix list. When there is a match, the route is used. More specifically, whether a prefix is permitted or denied is based upon the following rules:

- An empty prefix list permits all prefixes.
- An implicit deny is assumed if a given prefix does not match any entries of a prefix list.
- When multiple entries of a prefix list match a given prefix, the longest, most specific match is chosen.

Sequence numbers are generated automatically unless you disable this automatic generation. If you disable the automatic generation of sequence numbers, you must specify the sequence number for each entry using the *sequence-number* argument of the **permit** and **deny** commands in either IPv4 or IPv6 prefix list configuration command. Use the **no** form of the **permit** or **deny** command with the *sequence-number* argument to remove a prefix-list entry.

The **show** commands include the sequence numbers in their output.

Information About Implementing ACL-based Forwarding

To implement access lists and prefix lists, you must understand the following concepts:

ACL-based Forwarding Overview

Converged networks carry voice, video and data. Users may need to route certain traffic through specific paths instead of using the paths computed by routing protocols. This is achieved by specifying the next-hop address in ACL configurations, so that the configured next-hop address from ACL is used for fowarding packet towards its destination instead of routing packet-based destination address lookup. This feature of using next-hop in ACL configurations for forwarding is called ACL Based Forwarding (ABF).

ACL-based forwarding enables you to choose service from multiple providers for broadcast TV over IP, IP telephony, data, and so on, which provides a cafeteria-like access to the Internet. Service providers can divert user traffic to various content providers.

The ABF feature can be configured along with object groups while defining an ACEs (Access Control Entry).

ABF-OT

To provide flexibility to the user in selecting the suitable next hop, the ABF functionality is enhanced to interact with object-tracking (OT), which impacts:

- Tracking prefix in CEF
- Tracking the line-state protocol
- IPSLA (IP Service Level Agreement)

IPv6 ACL Based Forwarding Object Tracking

The IPv6 ACL based forwarding (ABF) object tracking feature enables ABF to decide which next hop address to use, based on the state of the object being tracked for the next hop. IPv6 SLA echos are used to determine reachability to the next hop address. If the primary route is unreachable, the secondary route is used to forward traffic. IPv6 ABF object tracking is supported on ASR 9000 Enhanced Ethernet line cards only.

For information about the **object** command which is used to configure an object for tracking, see the *System Management Command Reference for Cisco ASR 9000 Series Routers*.

IPSLA support for Object tracking

The OT-module interacts with the IPSLA-module to get reachability information. With IPSLA, the routers perform periodic measurements

Configuring IPv4/IPv6 ACLs to Filter By Packet Length

You can configure an access control list to filter packets by the packet length at an ingress or egress interface. Depending on whether a packet matches the packet-length condition in a permit or deny statement, the packet is either processed or dropped respectively at the interface.

The ACL packet length match condition can be configured in simple or scaled ACLs in IPv4 or IPv6 networks.

To learn about the various packet-length options, see the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference*.

Note ACLs with packet length filtering are supported in both IPv4 and IPv6 networks only on Cisco ASR 9000 High Density 100GE Ethernet line cards. The following limitations must be noted:

- When an ACL is applied to a BVI interface on a chassis that contains other line cards in addition to the Cisco ASR 9000 High Density 100GE Ethernet line card, the ACL configuration cannot be committed.
- When an ACL is applied to a link bundle that includes a port from a Cisco ASR 9000 High Density 100GE Ethernet line card and a different line card, then the ACL configuration cannot be committed.

Access Control List Counters

In Cisco IOS XR software, ACL counters are maintained both in hardware and software. Hardware counters are used for packet filtering applications such as when an access group is applied on an interface. Software counters are used by all the applications mainly involving software packet processing.

Packet filtering makes use of 64-bit hardware counters per ACE. If the same access group is applied on interfaces that are on the same line card in a given direction, the hardware counters for the ACL are shared between two interfaces.

To display the hardware counters for a given access group, use the **show access-lists ipv4** [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**location** *node-id*}] command in EXEC mode.

To clear the hardware counters, use the **clear access-list ipv4** *access-list-name* [**hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**location** *node-id*}] command in EXEC mode.

Hardware counting is not enabled by default for IPv4 ACLs because of a small performance penalty. To enable hardware counting, use the **ipv4 access-group** *access-list-name* {**ingress** | **egress**} [**hardware-count**] command in interface configuration mode. This command can be used as desired, and counting is enabled only on the specified interface.

Note Hardware counters are enabled by default on 100Gigabit ethernet interfaces, Cisco ASR 9000 Ethernet line cards, and Cisco ASR 9000 Enhanced Ethernet line cards.

Software counters are updated for the packets processed in software, for example, exception packets punted to the LC CPU for processing, or ACL used by routing protocols, and so on. The counters that are maintained are an aggregate of all the software applications using that ACL. To display software-only ACL counters, use the **show access-lists ipv4** *access-list-name* [**sequence** *number*] command in EXEC mode.

All the above information is true for IPv6, except that hardware counting is always enabled; there is no **hardware-count** option in the IPv6 access-group command-line interface (CLI).

ACL Statistics Counter

The ACL statistics counter feature allows you to track the count of packets that a router either permits or denies. A router permits or denies packets based on the ACL rules that you configure on a router interface. By default, the ACL statistics counter allows you to track only the the count of packets denied. By configuring the command, **hw-module profile stats acl-permit**, you can also track the count of packets that are permitted. Routers use this knowledge of the count of packets for ACL-based traffic mirroring. Support for ACL permit counters also allows you to track the ACE through which a router permits a packet.

Restrictions

- ACL-based forwarding (ABF) is not supported on a router after you configure the **hw-module profile stats acl-permit** command on that router.
- After you configure the **hw-module profile stats acl-permit** command on the router, based on the requirement, you must reload the router or the line cards. Configuring of the command followed by reloading the router or line cards enables the tracking of the permitted packet count on the router or line cards.

Configuration Example

To enable the tracking of the permitted packet count based on the ACL rules, use the following steps:

1. Enter global configuration mode and configure an ACL.

```
Router# configure
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit ipv4 any any
Router(config-ipv4-acl)# 20 deny udp any any
Router(config-ipv4-acl)# commit
Router(config)# exit
```

2. Enter interface configuration mode and attach the configured ACL on an interface.

```
Router(config)# interface HundredGigE 0/0/0/0
Router(config-if)# ipv4 access-group TEST ingress
Router(config-if)# commit
Router(config-if)# exit
```

3. Enable the tracking of the permitted packet count.

```
Router(config)# hw-module profile stats acl-permit
Router(config)# commit
```

4. Based on the requirement, reload the router or line cards.

```
Router# reload location 0/0/CPU0
```

5. Running Configuration.

```
Router# show running-configuration
ipv4 access-list TEST
10 permit ipv4 any any
20 deny udp any any
!
interface HundredGigE 0/0/0/0
ipv4 access-group TEST ingress
!
hw-module profile stats acl-permit
end
```

6. Verification.

   Use the **show access-lists ipv4** *acl-name* **hardware ingress location** *node-id* command to verify that you have enabled or disabled the tracking of the permitted packet count.

```
Router# show access-lists ipv4 TEST hardware ingress location 0/0/CPU0
ipv4 access-list test-v4-ttl
 10 permit ipv4 any any ttl eq 100
 20 deny ipv4 any any ttl eq 200 (44043 matches)
Router# configure
Router(config)# hw-module profile stats acl-permit
In order to activate/deactivate this stats profile, you must manually reload the
chassis/all line cards
Router(config)# commit
Router# reload location 0/0/CPU0
```

```
Router# show access-lists ipv4 TEST hardware ingress location 0/0/CPU0
ipv4 access-list test-v4-ttl
 10 permit ipv4 any any ttl eq 100 (346318 matches)
 20 deny ipv4 any any ttl eq 200 (44043 matches)
```

ACL Counters Using SNMP

Apart from viewing the access control list counters using commands, you can also get the ACL counter information using SNMP. When the router receives an SNMP request for ACE counters, the router responds by sending the packet count that matches each access control entry along with the byte count to the SNMP server.

You can use the **counter** *counter-name* command to aggregate several ACEs into a single counter.

The following features are supported when you retrieve ACL counters using SNMP:

- Hardware counters for interface ACLs applied with the **interface-statistics** command.
- Hardware ACL statistics on GigabitEthernet, TenGigabitEthernet, HundredGigabitEthernet, Bundle Ethernet interfaces, and subinterfaces.
- ACE label counter statistics.

The following features are not supported when you retrieve ACL counters using SNMP:

- Software counters.
- Counter names cannot be configured on ABF ACLs.
- Common ACLs. If an interface has both common ACL and interface ACL, statistics pertaining to ACEs from the common ACL are not returned.
- Hardware statistics for subscriber interfaces.
- Hardware statistics for ACEs with the same counter name.

Only Cisco ASR 9000 Enhanced Ethernet Line Cards support this feature. We recommend that you do not enable more than 50 unique counters in an ACL.

How to Implement Access Lists and Prefix Lists

IPv6 ACL support is available on the Cisco ASR 9000 SIP 700 linecard and the ASR 9000 Ethernet linecards. The relevant scale is:

- ACL enabled interfaces - 1000 (500 in each direction); for ASR 9000 Ethernet linecards- 4000
- Unique ACLs - 512 (with 5 ACEs each); for ASR 9000 Ethernet linecards- 2000
- Maximum ACEs per ACL - 8000 (for ASR 9000 Ethernet lincards, ACEs could be 16000, 8000, 4000- based on the LC model)
- IPv6 ACL log will also be supported.

This section contains the following procedures:

Configuring Extended Access Lists

This task configures an extended IPv4 or IPv6 access list.

SUMMARY STEPS

1. **configure**
2. {**ipv4** | **ipv6**} **access-list** *name*
3. [*sequence-number*] **remark** *remark*
4. Do one of the following:
   - [*sequence-number*]{**permit** | **deny**} *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]
   - [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [*routing*] [**authen**] [**destopts**] [**fragments**] [**log** | **log-input**]
5. Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
6. **commit**
7. **show access-lists** {**ipv4** | **ipv6**} [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose

Step 2	{**ipv4** | **ipv6**} **access-list** *name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl_1`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 access-list acl_2`
		Enters either IPv4 or IPv6 access list configuration mode and configures the named access list.

Step 3	[*sequence-number*] **remark** *remark* **Example:** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out`	(Optional) Allows you to comment about a **permit** or **deny** statement in a named access list. • The remark can be up to 255 characters; anything longer is truncated. • Remarks can be configured before or after **permit** or **deny** statements, but their location should be consistent.

Step 4	Do one of the following:
	• [*sequence-number*]{**permit** | **deny**} *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]
	• [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [*routing*] [**authen**] [**destopts**] [**fragments**] [**log** | **log-input**]
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 172.16.0.0 0.0.255.255`
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny 192.168.34.0 0.0.0.255`
	or
	`RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit icmp any any`
	`RP/0/RSP0/CPU0:router(config-ipv6-acl)# 30 deny tcp any any gt 5000`
		Specifies one or more conditions allowed or denied in IPv4 access list acl_1.
		• The optional **log** keyword causes an information logging message about the packet that matches the entry to be sent to the console.
		• The optional **log-input** keyword provides the same function as the **log** keyword, except that the logging message also includes the input interface.
		or
		Specifies one or more conditions allowed or denied in IPv6 access list acl_2.
		• Refer to the **deny** (IPv6) and **permit** (IPv6) commands for more information on filtering IPv6 traffic based on based on IPv6 option headers and optional, upper-layer protocol type information.
		Note Every IPv6 address list has two implicit permits used for neighbor advertisement and solicitation: Implicit Neighbor Discovery–Neighbor Advertisement (NDNA) permit, and Implicit Neighbor Discovery–Neighbor Solicitation (NDNS) permit.

	Command or Action	Purpose
		Note Every IPv6 access list has an implicit **deny ipv6 any any** statement as its last match condition. An IPv6 access list must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise an access list.
Step 6	**commit**	
Step 7	**show access-lists** {**ipv4** | **ipv6**} [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_1`	(Optional) Displays the contents of current IPv4 or IPv6 access lists. • Use the *access-list-name* argument to display the contents of a specific access list. • Use the **hardware** , **ingress** or **egress** , and **location** or **sequence** keywords to display the access-list hardware contents and counters for all interfaces that use the specified access list in a given direction (ingress or egress). The access group for an interface must be configured using the **ipv4 access-group** command for access-list hardware counters to be enabled. • Use the **summary** keyword to display a summary of all current IPv4 or IPv6 access-lists. • Use the **interface** keyword to display interface statistics.

What to do next

After creating an access list, you must apply it to a line or interface. See the Applying Access Lists, on page 151 section for information about how to apply an access list.

ACL commit fails while adding and removing unique Access List Entries (ACE). This happens due to the absence of an assigned manager process. The user has to exit the config-ipv4-acl mode to configuration mode and re-enter the config-ipv4-acl mode before adding the first ACE.

Applying Access Lists

After you create an access list, you must reference the access list to make it work. Access lists can be applied on *either* outbound or inbound interfaces. This section describes guidelines on how to accomplish this task for both terminal lines and network interfaces.

Set identical restrictions on all the virtual terminal lines, because a user can attempt to connect to any of them.

For inbound access lists, after receiving a packet, Cisco IOS XR software checks the source address of the packet against the access list. If the access list permits the address, the software continues to process the

packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message. The ICMP message is configurable.

For outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you apply an access list that has not yet been defined to an interface, the software acts as if the access list has not been applied to the interface and accepts all packets. Note this behavior if you use undefined access lists as a means of security in your network.

Controlling Access to an Interface

This task applies an access list to an interface to restrict access to that interface.

Access lists can be applied on *either* outbound or inbound interfaces.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. Do one of the following:
   - **ipv4 access-group** *access-list-name* {**ingress** | **egress**} [**hardware-count**] [**interface-statistics**]
   - **ipv6 access-group** *access-list-name* {**ingress** | **egress**} [**interface-statistics**]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/2/0/2`
		Configures an interface and enters interface configuration mode.
		• The *type* argument specifies an interface type. For more information on interface types, use the question mark (?) online help function.
		• The *instance* argument specifies either a physical interface instance or a virtual instance.
		  • The naming notation for a physical interface instance is *rack/slot/module/port*. The slash (/) between values is required as part of the notation.
		  • The number range for a virtual interface instance varies depending on the interface type.

Step 3	Do one of the following:	Controls access to an interface.

	Command or Action	Purpose

	• **ipv4 access-group** *access-list-name* {**ingress** | **egress**} [**hardware-count**] [**interface-statistics**]
	• **ipv6 access-group** *access-list-name* {**ingress** | **egress**} [**interface-statistics**]
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-in-filter in`
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-out-filter out`
		• Use the *access-list-name* argument to specify a particular IPv4 or IPv6 access list.
		• Use the **in** keyword to filter on inbound packets or the **out** keyword to filter on outbound packets.
		• Use the **hardware-count** keyword to enable hardware counters for the IPv4 access group.
		  • Hardware counters are automatically enabled for IPv6 access groups.
		• Use the **interface-statistics** keyword to specify per-interface statistics in the hardware.
		This example applies filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/2.

Step 4	**commit**	

Controlling Access to a Line

This task applies an access list to a line to control access to that line.

SUMMARY STEPS

1. **configure**
2. **line** {**aux** | **console** | **default** | **template** *template-name*}
3. **access-class** *list-name*{**ingress** | **egress**}
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**line** {**aux**	**console**	**default**	**template** *template-name*} **Example:** `RP/0/RSP0/CPU0:router(config)# line default`	Specifies either the auxiliary, console, default, or a user-defined line template and enters line template configuration mode. • Line templates are a collection of attributes used to configure and manage physical terminal line connections (the console and auxiliary ports) and vty connections. The following templates are available in Cisco IOS XR software: • Aux line template—The line template that applies to the auxiliary line.

	Command or Action	Purpose
		• Console line template— The line template that applies to the console line. • Default line template—The default line template that applies to a physical and virtual terminal lines. • User-defined line templates—User-defined line templates that can be applied to a range of virtual terminal lines.
Step 3	**access-class** *list-name*{**ingress** | **egress**} **Example:** `RP/0/RSP0/CPU0:router(config-line)# access-class acl_2 out`	Restricts incoming and outgoing connections using an IPv4 or IPv6 access list. • In the example, outgoing connections for the default line template are filtered using the IPv6 access list acl_2.
Step 4	**commit**	

Configuring Prefix Lists

This task configures an IPv4 or IPv6 prefix list.

SUMMARY STEPS

1. **configure**
2. {**ipv4** | **ipv6**} **prefix-list** *name*
3. [*sequence-number*] **remark** *remark*
4. [*sequence-number*] {**permit** | **deny**} *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]
5. Repeat Step 4 as necessary. Use the **no** *sequence-number* command to delete an entry.
6. **commit**
7. Do one of the following:
   - **show prefix-list ipv4** [*name*] [*sequence-number*]
   - **show prefix-list ipv6** [*name*] [*sequence-number*] [*summary*]
8. **clear** {**ipv4** | **ipv6**} **prefix-list** *name* [*sequence-number*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	{**ipv4** | **ipv6**} **prefix-list** *name* **Example:**	Enters either IPv4 or IPv6 prefix list configuration mode and configures the named prefix list.

	Command or Action	Purpose

	`RP/0/RSP0/CPU0:router(config)# ipv4 prefix-list pfx_1`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list pfx_2`
		• To create a prefix list, you must enter at least one **permit** or **deny** clause.
		• Use the **no** {**ipv4** | **ipv6**} **prefix-list** *name* command to remove all entries in a prefix list.

Step 3	[*sequence-number*] **remark** *remark*
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4_pfx)# 10 remark Deny all routes with a prefix of 10/8`
	`RP/0/RSP0/CPU0:router(config-ipv4_pfx)# 20 deny 10.0.0.0/8 le 32`
		(Optional) Allows you to comment about the following **permit** or **deny** statement in a named prefix list.
		• The remark can be up to 255 characters; anything longer is truncated.
		• Remarks can be configured before or after **permit** or **deny** statements, but their location should be consistent.

Step 4	[*sequence-number*] {**permit** | **deny**} *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*] **Example:** `RP/0/RSP0/CPU0:router(config-ipv6_pfx)# 20 deny 128.0.0.0/8 eq 24`	Specifies one or more conditions allowed or denied in the named prefix list. • This example denies all prefixes matching /24 in 128.0.0.0/8 in prefix list pfx_2.
Step 5	Repeat Step 4 as necessary. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise a prefix list.
Step 6	**commit**	

Step 7	Do one of the following:
	• **show prefix-list ipv4** [*name*] [*sequence-number*]
	• **show prefix-list ipv6** [*name*] [*sequence-number*] [*summary*]
	Example:
	`RP/0/RSP0/CPU0:router# show prefix-list ipv4 pfx_1`
	or
	`RP/0/RSP0/CPU0:router# show prefix-list ipv6 pfx_2 summary`
		(Optional) Displays the contents of current IPv4 or IPv6 prefix lists.
		• Use the *name* argument to display the contents of a specific prefix list.
		• Use the *sequence-number* argument to specify the sequence number of the prefix-list entry.
		• Use the **summary** keyword to display summary output of prefix-list contents.

Step 8	**clear** {**ipv4** | **ipv6**} **prefix-list** *name* [*sequence-number*] **Example:** `RP/0/RSP0/CPU0:router# clear prefix-list ipv4 pfx_1 30`	(Optional) Clears the hit count on an IPv4 or IPv6 prefix list. **Note** The *hit count* is a value indicating the number of matches to a specific prefix-list entry.

Configuring Standard Access Lists

This task configures a standard IPv4 access list.

Standard access lists use source addresses for matching operations.

SUMMARY STEPS

1. **configure**
2. **ipv4 access-list** *name*
3. [*sequence-number*] **remark** *remark*
4. [*sequence-number*] {**permit** | **deny**} *source* [*source-wildcard*] [**log** | **log-input**]
5. Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
6. **commit**
7. **show access-lists** [**ipv4** | **ipv6**] [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 access-list** *name* **Example:** `RP/0/RSP0/CPU0:router# ipv4 access-list acl_1`	Enters IPv4 access list configuration mode and configures access list acl_1.
Step 3	[*sequence-number*] **remark** *remark* **Example:** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out`	(Optional) Allows you to comment about the following **permit** or **deny** statement in a named access list. • The remark can be up to 255 characters; anything longer is truncated. • Remarks can be configured before or after **permit** or **deny** statements, but their location should be consistent.
Step 4	[*sequence-number*] {**permit**	**deny**} *source* [*source-wildcard*] [**log**	**log-input**] **Example:** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255` or	Specifies one or more conditions allowed or denied, which determines whether the packet is passed or dropped. • Use the *source* argument to specify the number of network or host from which the packet is being sent. • Use the optional *source-wildcard* argument to specify the wildcard bits to be applied to the source.

	Command or Action	Purpose
	`RRP/0/RSP0/CPU0:routerrouter(config-ipv4-acl)# 30 deny 192.168.34.0 0.0.0.255`	• The optional **log** keyword causes an information logging message about the packet that matches the entry to be sent to the console. • The optional **log-input** keyword provides the same function as the **log** keyword, except that the logging message also includes the input interface.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise an access list.
Step 6	**commit**	
Step 7	**show access-lists** [**ipv4** | **ipv6**] [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_1`	(Optional) Displays the contents of the named IPv4 access list. • The contents of an IPv4 standard access list are displayed in extended access-list format.

What to do next

After creating a standard access list, you must apply it to a line or interface. See the Applying Access Lists, on page 151" section for information about how to apply an access list.

Copying Access Lists

This task copies an IPv4 or IPv6 access list.

SUMMARY STEPS

1. **copy access-list** {**ipv4** | **ipv6**}*source-acl destination-acl*
2. **show access-lists** {**ipv4** | **ipv6**}[*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**copy access-list** {**ipv4** | **ipv6**}*source-acl destination-acl* **Example:**	Creates a copy of an existing IPv4 or IPv6 access list. • Use the *source-acl* argument to specify the name of the access list to be copied.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router# copy ipv6 access-list list-1 list-2`	• Use the *destination-acl* argument to specify where to copy the contents of the source access list. • The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list, the access list is not copied.
Step 2	**show access-lists** {**ipv4** | **ipv6**}[*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 list-2`	(Optional) Displays the contents of a named IPv4 or IPv6 access list. For example, you can verify the output to see that the destination access list list-2 contains all the information from the source access list list-1.

Sequencing Access-List Entries and Revising the Access List

This task shows how to assign sequence numbers to entries in a named access list and how to add or delete an entry to or from an access list. It is assumed that a user wants to revise an access list. Resequencing an access list is optional.

Note When an ACL is configured under an interface and its resequenced and rolled back, the interface experiences traffic loss for a short period of time.

SUMMARY STEPS

1. **resequence access-list** {**ipv4** | **ipv6**} *name* [*base* [*increment*]]
2. **configure**
3. {**ipv4** | **ipv6**} **access-list** *name*
4. Do one of the following:
   - [*sequence-number*] {**permit** | **deny**} *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]
   - [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**log** | **log-input**]
5. Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
6. **commit**

7. **show access-lists** [**ipv4** | **ipv6**] [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**resequence access-list** {**ipv4** | **ipv6**} *name* [*base* [*increment*]] **Example:** `RP/0/RSP0/CPU0:router# resequence access-list ipv4 acl_3 20 15`	(Optional) Resequences the specified IPv4 or IPv6 access list using the starting sequence number and the increment of sequence numbers. • This example resequences an IPv4 access list named acl_3. The starting sequence number is 20 and the increment is 15. If you do not select an increment, the default increment 10 is used.
Step 2	**configure**	

Step 3	{**ipv4** | **ipv6**} **access-list** *name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl_1`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 access-list acl_2`
		Enters either IPv4 or IPv6 access list configuration mode and configures the named access list.

Step 4	Do one of the following:
	• [*sequence-number*] {**permit** | **deny**} *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]
	• [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**log** | **log-input**]
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 172.16.0.0 0.0.255.255`
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny 192.168.34.0 0.0.0.255`
	or
		Specifies one or more conditions allowed or denied in IPv4 access list acl_1.
		• The optional **log** keyword causes an information logging message about the packet that matches the entry to be sent to the console.
		• The optional **log-input** keyword provides the same function as the **log** keyword, except that the logging message also includes the input interface.
		• This access list happens to use a **permit** statement first, but a **deny** statement could appear first, depending on the order of statements you need.
		or
		Specifies one or more conditions allowed or denied in IPv6 access list acl_2.
		• Refer to the **permit** (IPv6) and **deny** (IPv6) commands for more information on filtering IPv6

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit icmp any any` `RP/0/RSP0/CPU0:router(config-ipv6-acl)# 30 deny tcp any any gt 5000`	traffic based on IPv6 option headers and upper-layer protocols such as ICMP, TCP, and UDP. **Note** Every IPv6 access list has an implicit **deny ipv6 any any** statement as its last match condition. An IPv6 access list must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise the access list.
Step 6	**commit**	
Step 7	**show access-lists** [**ipv4** | **ipv6**] [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_1`	(Optional) Displays the contents of a named IPv4 or IPv6 access list. • Review the output to see that the access list includes the updated information.

What to do next

If your access list is not already applied to an interface or line or otherwise referenced, apply the access list. See the "Applying Access Lists, on page 151" section for information about how to apply an access list.

Copying Prefix Lists

This task copies an IPv4 or IPv6 prefix list.

SUMMARY STEPS

1. **copy prefix-list** {**ipv4** | **ipv6**} *source-name destination-name*
2. Do one of the following:
   - **show prefix-list ipv4** [*name*] [*sequence-number*] [**summary**]
   - **show prefix-list ipv6** [*name*] [*sequence-number*] [**summary**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**copy prefix-list** {**ipv4** | **ipv6**} *source-name destination-name* **Example:** `RP/0/RSP0/CPU0:router# copy prefix-list ipv6 list_1 list_2`	Creates a copy of an existing IPv4 or IPv6 prefix list. • Use the *source-name* argument to specify the name of the prefix list to be copied and the *destination-name* argument to specify where to copy the contents of the source prefix list. • The *destination-name* argument must be a unique name; if the *destination-name* argument name exists for a prefix list, the prefix list is not copied.
Step 2	Do one of the following: • **show prefix-list ipv4** [*name*] [*sequence-number*] [**summary**] • **show prefix-list ipv6** [*name*] [*sequence-number*] [**summary**] **Example:** `RP/0/RSP0/CPU0:router# show prefix-list ipv6 list_2`	(Optional) Displays the contents of current IPv4 or IPv6 prefix lists. • Review the output to see that prefix list list_2 includes the entries from list_1.

Sequencing Prefix List Entries and Revising the Prefix List

This task shows how to assign sequence numbers to entries in a named prefix list and how to add or delete an entry to or from a prefix list. It is assumed a user wants to revise a prefix list. Resequencing a prefix list is optional.

Before you begin

Note Resequencing IPv6 prefix lists is not supported.

SUMMARY STEPS

1. **resequence prefix-list ipv4** *name* [*base* [*increment*]]
2. **configure**
3. {**ipv4** | **ipv6**} **prefix-list** *name*
4. [*sequence-number*] {**permit** | **deny**} *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]
5. Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
6. **commit**

7. Do one of the following:
   - **show prefix-list ipv4** [*name*] [*sequence-number*]
   - **show prefix-list ipv6** [*name*] [*sequence-number*] [**summary**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**resequence prefix-list ipv4** *name* [*base* [*increment*]] **Example:** `RP/0/RSP0/CPU0:router# resequence prefix-list ipv4 pfx_1 10 15`	(Optional) Resequences the named IPv4 prefix list using the starting sequence number and the increment of sequence numbers. • This example resequences a prefix list named pfx_1. The starting sequence number is 10 and the increment is 15.
Step 2	**configure**	
Step 3	{**ipv4** | **ipv6**} **prefix-list** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list pfx_2`	Enters either IPv4 or IPv6 prefix list configuration mode and configures the named prefix list.
Step 4	[*sequence-number*] {**permit** | **deny**} *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*] **Example:** `RP/0/RSP0/CPU0:router(config-ipv6_pfx)# 15 deny 128.0.0.0/8 eq 24`	Specifies one or more conditions allowed or denied in the named prefix list.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise the prefix list.
Step 6	**commit**	
Step 7	Do one of the following: • **show prefix-list ipv4** [*name*] [*sequence-number*] • **show prefix-list ipv6** [*name*] [*sequence-number*] [**summary**] **Example:** `RP/0/RSP0/CPU0:router# show prefix-list ipv6 pfx_2`	(Optional) Displays the contents of current IPv4 or IPv6 prefix lists. • Review the output to see that prefix list pfx_2 includes all new information.

How to Implement ACL-based Forwarding

This section contains the following procedures:

Configuring ACL-based Forwarding with Security ACL

Perform this task to configure ACL-based forwarding with security ACL.

SUMMARY STEPS

1. **configure**
2. **ipv4 access-list** *name*
3. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**[default] nexthop1** [**ipv4** *ipv4-address1*] **nexthop2**[**ipv4** *ipv4-address2*] **nexthop3**[**ipv4** *ipv4-address3*]] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**] [[**track** *track-name*] [**ttl** *ttl* [*value1 ... value2*]]
4. **commit**
5. **show access-list ipv4** [[*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 access-list** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv4 access-list security-abf-acl`	Enters IPv4 access list configuration mode and configures the specified access list.

Step 3	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**[default] nexthop1** [**ipv4** *ipv4-address1*] **nexthop2**[**ipv4** *ipv4-address2*] **nexthop3**[**ipv4** *ipv4-address3*]] [**dscp** *dscp*] [**fragments**] [**log**	**log-input**] [[**track** *track-name*] [**ttl** *ttl* [*value1 ... value2*]]
		Example:
		`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 10.0.0.0 0.255.255.255 any nexthop 50.1.1.2`
		`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 15 permit ipv4 30.2.1.0 0.0.0.255 any`
		`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit ipv4 30.2.0.0 0.0.255.255 any nexthop 40.1.1.2`
			Sets the conditions for an IPv4 access list. The configuration example shows how to configure ACL-based forwarding with security ACL.
			• The **nexthop1, nexthop2, nexthop3** keywords forward the specified next hop for this entry. You can configure a mximum of 3 nexthops per ACEs.
			• Enable object-tracking for each next-hop in the ACE to decide which next hop address to use, based on the state of the object being tracked for the next hop.
			• If the **default** keyword is configured, ACL-based forwarding action is taken only if the results of the PLU lookup for the destination of the packets

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 25 permit ipv4 any any`	determine a default route; that is, no specified route is determined to the destination of the packet.
Step 4	**commit**	
Step 5	**show access-list ipv4** [[*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter location** *node-id*}]] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 security-abf-acl`	Displays the information for ACL software.

Implementing IPSLA-OT

In this section, the following procedures are discussed:

- Enabling track mode, on page 164
- Configuring track type, on page 165
- Configuring tracking type (line protocol), on page 165
- Configuring track type (list), on page 166
- Configuring tracking type (route), on page 167
- Configuring tracking type (rtr), on page 167

Note When a large number of IPSLA instances need to be configured, it's more convenient to create a configuration file with all the configurations and then load the configuration file. The configuration statements in the configuration file should be properly indented including the exit statements, otherwise the configuration won't work when loading the configuration file.

Enabling track mode

SUMMARY STEPS

1. configure
2. **track** *track-name*
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RSP0/CPU0:router(config)# track t1`	Enters track configuration mode.
Step 3	**commit**	

Configuring track type

There are different mechanisms to track the availability of the next-hop device. The tracking type can be of four types, using:

- line protocol
- list
- route
- IPSLA

Configuring tracking type (line protocol)

Line protocol is one of the object types the object tracker component can track. This object type provides an option for tracking state change notification from an interface. Based on the interface state change notification, it decides whether the track state should be UP or DOWN.

SUMMARY STEPS

1. configure
2. **track** *track-name*
3. **type line-protocol state interface** *type interface-path-id*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RSP0/CPU0:router(config)# track t1`	Enters track configuration mode.
Step 3	**type line-protocol state interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-track)# type line-protocol state interface tengige 0/4/4/0`	Sets the interface which needs to be tracked for state change notifications.
Step 4	**commit**	

Configuring track type (list)

List is a boolen object type. Boolean refers to the capability of performing a boolean AND or boolean OR operation on combinations of different object types supported by object tracker.

SUMMARY STEPS

1. configure
2. **track** *track-name*
3. **type list boolean and**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RSP0/CPU0:router(config)# track t1`	Enters track configuration mode.

	Command or Action	Purpose
Step 3	**type list boolean and** **Example:** `RP/0/RSP0/CPU0:router(config-track)# type list boolean and`	Sets the list of track objects on which boolean AND or boolean OR operations could be performed.
Step 4	**commit**	

Configuring tracking type (route)

Route is a route object type. The object tracker tracks the fib notification to determine the route reachability and the track state.

SUMMARY STEPS

1. configure
2. **track** *track-name*
3. **type route reachability**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RSP0/CPU0:router(config)# track t1`	Enters track configuration mode.
Step 3	**type route reachability** **Example:** `RP/0/RSP0/CPU0:router(config-track)# type route reachability`	Sets the route on which reachability state needs to be learnt dynamically.
Step 4	**commit**	

Configuring tracking type (rtr)

IPSLA is an ipsla object type. The object tracker tracks the return code of ipsla operation to determine the track state changes.

SUMMARY STEPS

1. configure
2. **track** *track-name*
3. **type rtr** *ipsla operation id* **reachability**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RSP0/CPU0:router(config)# track t1`	Enters track configuration mode.
Step 3	**type rtr** *ipsla operation id* **reachability** **Example:** `RP/0/RSP0/CPU0:routertype rtr 100 reachability`	Sets the ipsla operation id which needs to be tracked for reachability.
Step 4	**commit**	

Configuring Pure ACL-Based Forwarding for IPv6 ACL

SUMMARY STEPS

1. **configure**
2. {**ipv6** } **access-list** *name*
3. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]] [**ttl** *ttl value* [*value1 ... value2*]][**default] nexthop1** [**track** *track-name-1*] [**vrf** *vrf-name1*][**ipv6** *ipv6-address1*] [**nexthop2** [**track** *track-name-2*] [**vrf** *vrf-name2*] [**ipv6** *ipv6-address2*] [**nexthop3** [**track** *track-name-3*] [**vrf** *vrf-name3*] [**ipv6***ipv6-address3*]]]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	{**ipv6** } **access-list** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 access-list security-abf-acl`	Enters IPv6 access list configuration mode and configures the specified access list.
Step 3	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]] [**ttl** *ttl value* [*value1 ... value2*]][**default] nexthop1** [**track** *track-name-1*] [**vrf** *vrf-name1*][**ipv6** *ipv6-address1*] [**nexthop2** [**track** *track-name-2*] [**vrf** *vrf-name2*] [**ipv6** *ipv6-address2*] [**nexthop3** [**track** *track-name-3*] [**vrf** *vrf-name3*] [**ipv6***ipv6-address3*]]] **Example:** `RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 any any default nexthop1 vrf vrf_A ipv6 11::1 nexthop2 vrf vrf_B ipv6 nexthop3 vrf vrf_C ipv6 33::3`	Sets the conditions for an IPv6 access list. The configuration example shows how to configure pure ACL-based forwarding for ACL. • Forwards the specified next hop for this entry. • The track option specifies object tracking name for the corresponding next hop.
Step 4	**commit**	

ACL-Chaining

ACL-Chaining also known as Multi-ACL enables customers to apply two IPv4 or IPv6 (common and interface) ACLs on an interface for packet filtering at the router. One ACL is common across multiple interfaces on the line card. This provides Ternary Content Addressable Memory(TCAM)/HW scalability. This feature is supported on A9K-SIP-700 Line Card and ASR 9000 Enhanced Ethernet Line Card only.

ACL-Chaining Overview

Currently, the packet filter process (pfilter_ea) supports only one ACL to be applied per direction and per protocol on an interface. This leads to manageability issues if there are common ACL entries needed on most interfaces. Duplicate ACEs are configured for all those interfaces, and any modification to the common ACEs needs to be performed for all ACLs.

A typical ACL on the edge box for an ISP has two sets of ACEs:

- common ISP specific ACEs (ISP protected address block)
- customer/interface specific ACEs (Customer source address block)

The purpose of these address blocks is to deny access to ISP's protected infrastructure networks and anti-spoofing protection by allowing only customer source address blocks. This results in configuring unique ACL per interface and most of the ACEs being common across all the ACLs on a box. ACL provisioning and modification is very cumbersome. Any changes to the ACE impacts every customer interface. (This also wastes the HW/TCAM resources as the common ACEs are being replicated in all ACLs).

The ACL chaining feature also known as Multi-ACL allows you to configure more than one ACL that can be applied to a single interface. The goal is to separate various types of ACLs for management, and also allow you to apply both of them on the same interface, in a defined order.

Restrictions for Common ACL

The following restrictions apply while implementing Common ACL:

- Common ACL is supported in only ingress direction and for L3 interfaces only.
- The **interface-statistics** option is not available for common ACLs.
- The **hardware-count** option is available for only IPv4 ACLs.
- Only one common IPv4 and IPv6 ACL is supported on each line card.
- The common ACL option is not available for Ethernet Service (ES) ACLs.
- The IPv4 and IPv6 common ACL is limited to 200 Ternary Content Addressable Memory(TCAM) entries for the ASR 9000 Enhanced Ethernet line card and A9K-SIP-700 line card. Although, A9K-SIP-700 line card may support more.
- Common ACL is not supported on ASR 9000 Ethernet Line Card and ASR 9000 Enhanced Ethernet-TR Line Card.
- You can specify only common ACL or only interface ACL or both common and interface ACL in this command.
- The **compress** option is not supported for common ACLs.
- Object-groups are not supported with common ACLs.
- The **interface-statistics** and **hardware-count** options are not supported for ACLs on the A9K-SIP-700 line card.

Configuring an Interface to accept Common ACL

Perform this task to configure the interface to accept a common ACL along with the interface specific ACL:

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. { **ipv4 | ipv6** } **access-group** { **common** *access-list-name* { [*access-list-name* **ingress** [**interface-statistics**]] | **ingress** } | *access-list-name* { **ingress | egress** } [**interface-statistics**] } [**hardware-count**]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/2/0/1`	This command configures an interface (in this case a TenGigabitEThernet interface) and enters the interface configuration mode.
Step 3	{ **ipv4 | ipv6** } **access-group** { **common** *access-list-name* { [*access-list-name* **ingress** [**interface-statistics**]] | **ingress** } | *access-list-name* { **ingress | egress** } [**interface-statistics**] } [**hardware-count**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group common acl-p acl1 ingress`	Configures the interface to accept a common ACL along with the interface specific ACL. **Note** The **interface-statistics** and **hardware-count** options are not supported for ACLs on the A9K-SIP-700 line card.
Step 4	**commit**	

Configuring an Interface to Accept Multiple ACLs on Cisco ASR 9000 High Density 100GE Ethernet Line Cards

You can configure an interface on Cisco ASR 9000 High Density 100GE Ethernet line cards (such as A9K-8x100G-LB-SE and A9K-8x100G-LB-TR) to accept up to five IPv4 and/or IPv6 ACLs. This feature extends the ACL chaining from two ACLs to a maximum of five ACLs on Cisco ASR 9000 High Density 100GE Ethernet line cards only.

The following restrictions apply while configuring multiple ACLs on Cisco ASR 9000 High Density 100GE Ethernet line cards:

-
- Multi-level ACL is supported only in the ingress direction and for L3 interfaces only.
- The multi-level ACL feature is not available for Ethernet Service (ES) ACLs.
- ACLs with obj-groups are not supported.
- Compression is not supported.
- Access List Based Forwarding (ABF) enabled rules for ACLs are not supported.
- An ACL already applied in per-ace mode cannot be applied elsewhere in interface-stats mode.
- Accessing the ACL counters using SNMP query is not supported.

Perform this task to configure an interface on Cisco ASR 9000 High Density 100GE Ethernet line cards to accept up to five IPv4 and/or IPv6 ACLs:

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. [**ipv4 | ipv6**] **access-group common** *acl-c1* **common** *acl-c2 acl-i2 acl-i4 acl-i5* **ingress**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/0`	This command configures an interface (in this case a GigabitEthernet interface) and enters the interface configuration mode.
Step 3	[**ipv4 | ipv6**] **access-group common** *acl-c1* **common** *acl-c2 acl-i2 acl-i4 acl-i5* **ingress** **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group common acl-a common acl-b acl-x acl-y acl-z ingress`	Configures the interface to accept five ACLs in the inbound direction. There can be any combination of common and/or interface ACLs up to a total of five ACLs. In this command: • "*acl_c1* and "*acl_c2*" are common ACLs, each preceded by the "**common**" keyword • "*acl_i2*", "*acl_i4*," and "*acl_i5*" are interface ACLs
Step 4	**commit**	

ACL Scale Enhancements

The Access Control List (ACL) Scale enhancements feature enables you to define ACL rules as a set of several rules (super-set of ACEs (Access Control Entry)). This is achieved with object-groups of prefixes and ports, which are referred by ACE in the same way as single source address or destination address prefix and ports are referred.

Note The ACL Scale enhancements feature is not supported on first generation ASR 9000 Ethernet Line Card.

ACL Scale Enhancements: Backward Compatibility

With the support of object-groups, configuring ACE in the existing way in which one ACE entry uses object groups, while another ACE entry does not use object groups is supported.

Note From Release 4.3.1, object group is only supported on ASR 9000 Enhanced Ethernet Line Card.

```
ipv4 access-list acl1
     10 permit tcp  net-group  group1  host 10.10.10.1  eq 2200
     20 permit tcp 10.10.10.3/32  host 1.1.1.2   eq  2000
!
```

It is possible that a user configures a host or prefix in an ACE entry, where the same host or prefix is added to an existing source group, eliminating the need to configure a separate ACE entry. However, such an optimization is not automated. A user could intentionally configure a particular prefix in a separate ACE for the purpose of separate counter or accounting for that prefix.

The object-groups can be configured along with ABF while defining an ACEs (Access Control Entry).

Configuring a Network Object-Group

Perform this task to configure a network object group and to enter the network object group configuration mode.

SUMMARY STEPS

1. **configure**
2. **object-group network** { **ipv4 | ipv6** } *object-group-name*
3. **description** *description*
4. **host** *address*
5. *address { mask | prefix }*
6. **range** *address address*
7. **object-group** *name*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**object-group network** { **ipv4 | ipv6** } *object-group-name* **Example:**	Configures a network object group and enters the network object group configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# object-group network ipv4 ipv4_type5_obj1`	
Step 3	**description** *description* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-ipv4)# description network-object-group`	Describes the object group.
Step 4	**host** *address* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-ipv4)# host 10.20.2.3`	Configures the host IPv4 address for the object group.
Step 5	*address { mask | prefix }* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-ipv4)# 10.20.20.3 255.255.255.0`	Configures the host address mask or prefix.
Step 6	**range** *address address* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-ipv4)# range 10.20.20.10 10.20.20.40`	Configures the range of host IPv4 address for the object group.
Step 7	**object-group** *name* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-ipv4)# object-group`	Specifies the name of the nested object group.
Step 8	**commit**	

Configuring a Port Object-Group

Perform this task to configure a port object group and to enter the port object group configuration mode.

SUMMARY STEPS

1. **configure**
2. **object-group port** *object-group-name*
3. **description** *description*
4. **{ eq | lt | gt }***{ protocol | number }*
5. **range** *range range*
6. **object-group** *name*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**object-group port** *object-group-name* **Example:** `RP/0/RSP0/CPU0:router(config)# object-group port ipv4_type5_obj1`	Configures a port object group and enters the port object group configuration mode.
Step 3	**description** *description* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-port)# description port-object-group`	Configures the description for the object group.

Step 4	**{ eq | lt | gt }***{ protocol | number }*
	Example:
	`RP/0/RSP0/CPU0:router(config-object-group-port)# eq ftp`
	`or`
	`RP/0/RSP0/CPU0:router(config-object-group-port)# eq 21`
		Matches packets on ports equal to, less than, or greater than the specified port number or protocol.

Step 5	**range** *range range* **Example:** `RP/0/RSP0/CPU0:router(config-object-group-port)# range 1000 2000`	Configures the range of host ports for the object group.
Step 6	**object-group** *name* **Example:**	Specifies the name of the nested object group.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-object-group-port)# object-group port-group2`	
Step 7	**commit**	

Configuring ACL with Object-Groups

You must be aware of the following information that apply to object-group ACLs:

- You can configure ACLs that contain both conventional and object-group ACEs.
- You can modify the objects in an object group dynamically without redefining the object group or the ACE that references the object group.
- You can configure an object-group ACL multiple times with a source group, or a destination group, or both source and destination groups.
- The command `show access-lists` *`access-list-name`* `hardware ingress detail location` *`location`* displays compressed output for source and destination IP addresses when the `detail` keyword is used while attaching ACLs to interfaces.

Configuring object-group ACLs involves the following restrictions:

- Compression level 0 is the default compression mode for object-group ACLs.
- Object-group ACLs can only be configured on an interface. They cannot be used or referenced by applications like SSH, SNMP, NTP.
- Compression is not supported on L2 interfaces.
- To delete an object-group, you must first delete it from all ACLs.
- Compression requires only internal TCAM lookups for both compression mode 0 and compression mode 3.
- When object-groups ACLs are edited, it leads to a full replacement of the old ACL with the edited ACL. Therefore, the TCAM should have enough space to support the old ACL and the edited ACL until the edited ACL configuration is committed and the old ACL is deleted.
- Compression is supported on Cisco ASR 9000 4th Generation QSFP28 based dense 100GE line cards. You can configure only one compression mode per protocol on a line card.
- Compression is supported only on IPv4 and IPv6 protocols.
- You cannot configure object-group ACLs along with QoS policies.
- Object-group ACLs are not supported in any policy based configuration.

Perform this task to configure ACL with object groups.

SUMMARY STEPS

1. **configure**

2. **{ ipv4 | ipv6 } access-list** *name*
3. [*sequence-number*] **permit** *protocol* **net-group** *source-net-object-group-name* **port-group** *source-port-object-group-name* **net-group** *destination-net-object-group-name* **port-group** *destination-port-object-group-name* [**precedence** *precedence*] [**[default] nexthop1** [**vrf** *vrf-name*][**ipv4** *ipv4-address1*] **nexthop2**[**vrf** *vrf-name*][**ipv4** *ipv4-address2*] **nexthop3**[**vrf** *vrf-name*][**ipv4** *ipv4-address3*]] [**dscp range** *dscp dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [[**track** *track-name*] [**ttl** *ttl* [*value1 ... value2*]]
4. **exit**
5. **interface** *type interface-path-id*
6. **ipv4 access-group** *access-list-name* {**ingress** | **egress** } **compress level** *level* [**hardware-count**] [**interface-statistics**]
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**{ ipv4 | ipv6 } access-list** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl1`	Configures the specified access list, and enters IPv4 or IPv6 access list configuration mode.

Step 3	[*sequence-number*] **permit** *protocol* **net-group** *source-net-object-group-name* **port-group** *source-port-object-group-name* **net-group** *destination-net-object-group-name* **port-group** *destination-port-object-group-name* [**precedence** *precedence*] [**[default] nexthop1** [**vrf** *vrf-name*][**ipv4** *ipv4-address1*] **nexthop2**[**vrf** *vrf-name*][**ipv4** *ipv4-address2*] **nexthop3**[**vrf** *vrf-name*][**ipv4** *ipv4-address3*]] [**dscp range** *dscp dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [[**track** *track-name*] [**ttl** *ttl* [*value1 ... value2*]]
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit tcp net-group network-group-west net-group network-group-east port-group`
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit ipv4 net-group network-group-west1 net-group network-group-east1`
		Configures ACL with object groups.
		Note You must configure network object groups and port object groups before configuring ACL. For more information about configuring network object groups, see Configuring a Network Object-Group, on page 173. For more information about configuring port object groups, see Configuring a Port Object-Group, on page 174.
		When a network or port object-group is part of an ACL attached to an interface, you can add or remove members from the corresponding network or port object-group.
		When a network or port object-group is part of an ACL attached to an interface, adding or removing object-groups which are part of inherited or nested object-groups is not supported.
		A member is either an IPv4/IPv6 address/prefix or port.

Step 4	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit`	
Step 5	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2`	Configures an interface and enters interface configuration mode. • The *type* argument specifies an interface type. For more information on interface types, use the question mark (?) online help function. • The *interface-path-id* argument specifies either a physical interface instance or a virtual instance.The *interface-path-id* argument specifies either a physical interface instance or a virtual instance.

Step 6	**ipv4 access-group** *access-list-name* {**ingress** | **egress** } **compress level** *level* [**hardware-count**] [**interface-statistics**]
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group acl1 ingress compress level 1`
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group acl1 engress compress level 3`
		Controls access to an interface. Use the **compress level** keyword to specify ACL compression in the hardware.
		• level 0 indicates no compression
		• level 1 indicates source compression
		• level 3 indicates all compression

Step 7	**commit**	

Atomic ACL Updates By Using the Disable Option

Atomic ACL updates involve the insertion, modification, or removal of Access List Entries (ACEs) on an interface that is in operation. Such atomic updates consume up to 50% of TCAM resources. There can be an instance where multiple modifications are required and the available resources are not sufficient. The solution to this problem is to disable atomic ACL updates such that the old ACEs are deleted before the new ACEs are added.

Note When you configure the **atomic-disable** statement in an ACL, any ACE modification detaches the ACL, until the modification is complete. In addition to this, the ACL rules are not applied during the modification process. Hence, it is recommended to configure to either permit or deny all traffic until the modification is complete.

Configuration for Disabling Atomic ACL Updates

To disable atomic updates on the hardware, by permitting all packets, use the following configuration.

```
RP/0/RSP0/CPU0:router# hardware access-list atomic-disable
```

Modifying ACLs when Atomic ACL Updates are Disabled

On disabling atomic ACL updates on the hardware, use the steps in this section to modify ACLs.

Add an ACE

Use the following steps to add an ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
!
```

2. Add the ACE to the ACL.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 permit ipv4 30.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if your ACE was added successfully.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
 30 permit ipv4 30.1.1.0/24 any
!
```

You have successfully added an ACE.

Delete an ACE

Use the steps in this section to delete an ACE.

1. Locate the ACL containing the ACE that you want deleted.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
 30 permit ipv4 30.1.1.0/24 any
!
```

2. Delete the ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# no 30
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the ACE has been removed from the ACL.

```
RP/0/RSP0/CPU0:router(config-ipv4-acl)# do show access-lists
...
```

```
ipv4 access-list list1
 10 permit ipv4 10.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

You have successfully deleted an ACE.

Replace an ACE

Use the steps in this section to replace an ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config-ipv4-acl)#do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 10.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

2. Configure the new ACE to replace the existing ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 11.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the ACE replacement is successful.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

You have successfully replaced an ACE.

Delete an ACE and Add a New ACE

Use the following steps to delete an ACE and add a new ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

2. Delete the required ACE, and add the new ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# no 20
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 12.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the modification is successful.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 12.1.1.0 0.0.0.255 any
```

You have successfully deleted an ACE, and added a new ACE.

Similarly, you can combine the addition, removal, and replacement of ACEs.

Configuring ACL Counters for SNMP Query

You can configure ACL counters and access the counters using SNMP query. This section explains how to configure ACL counters for SNMP query.

SUMMARY STEPS

1. **configure**
2. {**ipv4** | **ipv6**} **access-list** *name*
3. Do one of the following:
   - [*sequence-number*] {**permit** | **deny**} *source* {[*source source-wildcard*] | [*destination destination-wildcard*]} **counter** *counter-name*
   - [*sequence-number*] {**permit** | **deny**} *protocol* {[*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | [*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*]} **counter** *counter-name*
4. Repeat Step 3 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
5. **commit**
6. **show access-lists** {**ipv4** | **ipv6**} [*access-list-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	{**ipv4** | **ipv6**} **access-list** *name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl_1`
	or
	`RP/0/RSP0/CPU0:router(config)# ipv6 access-list acl_2`
		Enters either IPv4 or IPv6 access list configuration mode and configures the named access list.

Step 3	Do one of the following: • [*sequence-number*] {**permit** | **deny**} *source* {[*source source-wildcard*] | [*destination destination-wildcard*]} **counter** *counter-name* • [*sequence-number*] {**permit** | **deny**} *protocol* {[*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | [*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*]} **counter** *counter-name*	Specifies one or more conditions allowed or denied in IPv4 access list acl_1 or IPv6 access list acl_2. The **counter** *counter-name* keyword enables ACL counters which you can access using SNMP query.

	Command or Action	Purpose

	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 172.16.0.0 0.0.255.255 counter counter1`
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny 192.168.34.0 0.0.0.255 counter counter2`
	or
	`RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit icmp any any counter counter3`
	`RP/0/RSP0/CPU0:router(config-ipv6-acl)# 30 deny tcp any any gt 5000 counter counter4`	

Step 4	Repeat Step 3 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise an access list.
Step 5	**commit**	
Step 6	**show access-lists** {**ipv4** | **ipv6**} [*access-list-name*] **Example:** `RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_1`	(Optional) Displays the contents of current IPv4 or IPv6 access lists.

Optimizing ACL Level 3 compression

Table 9: Feature History Table

Feature Name	Release Information	Description
Optimizing ACL Level 3 compression	Release 7.5.3	This feature allows you to change the TCAM (ternary content-addressable memory) size that is allowed for ACL level 3 compression from 70 to 76 bytes and conversely. The option to increase TCAM space by 6 bytes for the compression fields enables you to avoid ACL L3 compression failures when the compression field configurations exceed 70 bytes. This feature introduces the **hardware access-list l3-compression-optimisation** command.

Starting with Cisco IOS-XR Release 7.5.3, you can configure the concatenated TCAM key size that is allocated for ACL level 3 compression. TCAM is a specialized high speed dedicated hardware memory that could be used to perform specific functions at faster pace. The ACL Layer 3 compression concatenated TCAM stores the ACLs in hardware memory in a compressed format such that large ACLs could be accomodated within the available memory. By default, the concatenated TCAM size allocated for ACL level 3 compression and non-compression fields is 80 bytes. In the concatenated TMAC, the compression fields are allowed 70 bytes and non-compression fields have 10 bytes. In some scenarios, when the size of compression configurations exceeds the allotted TCAM, ACL compression fails. To avoid such failures, you can add another 6 bytes for data for compression fields in the 10 bytes of space set aside for non-compression fields in the concatenated TCAM.

Guidelines:

- Before enabling ACL Layer 3 optimization using the **hardware access-list l3-compression-optimisation** command, you must mandatorily disable the atomicity for ACL modification using the **hardware access-list atomic disable** command.
- ACL Layer 3 optimization does not support ACL matching for Time to Live (TTL), packet length, type of service (TOS), and IPv6 extension header fields.
- On enabling ACL Layer 3 optimization at global configuration level, the ACE supports configuring Source IP address, Destination IP address, and Port fields only.

Configuration:

You can enable ACL Level 3 compression optimization using the following configuration:

1. Disable the atomic access-control list (ACL) updates.

```
Router# configure
Router#(config)# hardware access-list atomic disable
Router(config)# commit
```

2. Enable ACL level 3 compression.

```
Router# configure
Router#(config)# hardware access-list l3-compression-optimisation
Router(config)# commit
```

3. Reload the line card or reapply the ACL to the interface.

To disable the ACL Level 3 compression optimization, do the following:

```
Router# configure
Router#(config)# no hardware access-list l3-compression-optimisation
Router(config)# commit
```

Configuration Examples for Implementing Access Lists and Prefix Lists

This section provides the following configuration examples:

Resequencing Entries in an Access List: Example

The following example shows access-list resequencing. The starting value in the resequenced access list is 10, and increment value is 20. The subsequent entries are ordered based on the increment values that users provide, and the range is from 1 to 2147483646.

When an entry with no sequence number is entered, by default it has a sequence number of 10 more than the last entry in the access list.

```
ipv4 access-list acl_1
10 permit ip host 10.3.3.3 host 172.16.5.34
20 permit icmp any any
30 permit tcp any host 10.3.3.3
40 permit ip host 10.4.4.4 any
60 permit ip host 172.16.2.2 host 10.3.3.12
70 permit ip host 10.3.3.3 any log
80 permit tcp host 10.3.3.3 host 10.1.2.2
100 permit ip any any

configure
 ipv4 access-list acl_1
 end
resequence ipv4 access-list acl_1 10 20

show access-lists ipv4 acl_1

10 permit ip host 10.3.3.3 host 172.16.5.34
30 permit icmp any any
50 permit tcp any host 10.3.3.3
70 permit ip host 10.4.4.4 any
90 permit ip host 172.16.2.2 host 10.3.3.12
110 permit ip host 10.3.3.3 any log
130 permit tcp host 10.3.3.3 host 10.1.2.2
150 permit ip any any


ipv4 access-list acl_1
10 permit ip host 10.3.3.3 host 172.16.5.34
20 permit icmp any any
30 permit tcp any host 10.3.3.3
40 permit ip host 10.4.4.4 any
60 permit ip host 172.16.2.2 host 10.3.3.12
70 permit ip host 10.3.3.3 any log
80 permit tcp host 10.3.3.3 host 10.1.2.2
100 permit ip any any

configure
ipv6 access-list acl_1
end
resequence ipv6 access-list acl_1 10 20

ipv4 access-list acl_1
10 permit ip host 10.3.3.3 host 172.16.5.34
30 permit icmp any any
50 permit tcp any host 10.3.3.3
70 permit ip host 10.4.4.4 any
90 Dynamic test permit ip any any
110 permit ip host 172.16.2.2 host 10.3.3.12
130 permit ip host 10.3.3.3 any log
150 permit tcp host 10.3.3.3 host 10.1.2.2
170 permit ip host 10.3.3.3 any
190 permit ip any any
```

Adding Entries with Sequence Numbers: Example

In the following example, an new entry is added to IPv4 access list acl_5.

```
ipv4 access-list acl_5
 2 permit ipv4 host 10.4.4.2 any
 5 permit ipv4 host 10.0.0.44 any
 10 permit ipv4 host 10.0.0.1 any
 20 permit ipv4 host 10.0.0.2 any
configure
ipv4 access-list acl_5
 15 permit 10.5.5.5 0.0.0.255
end
ipv4 access-list acl_5
 2 permit ipv4 host 10.4.4.2 any
 5 permit ipv4 host 10.0.0.44 any
 10 permit ipv4 host 10.0.0.1 any
 15 permit ipv4 10.5.5.5 0.0.0.255 any
 20 permit ipv4 host 10.0.0.2 any
```

Adding Entries Without Sequence Numbers: Example

The following example shows how an entry with no specified sequence number is added to the end of an access list. When an entry is added without a sequence number, it is automatically given a sequence number that puts it at the end of the access list. Because the default increment is 10, the entry will have a sequence number 10 higher than the last entry in the existing access list.

```
configure
ipv4 access-list acl_10
permit 10 .1.1.1 0.0.0.255
permit 10 .2.2.2 0.0.0.255
permit 10 .3.3.3 0.0.0.255
end

ipv4 access-list acl_10
 10 permit ip 10 .1.1.0 0.0.0.255 any
 20 permit ip 10 .2.2.0 0.0.0.255 any
 30 permit ip 10 .3.3.0 0.0.0.255 any

configure
ipv4 access-list acl_10
permit 10 .4.4.4 0.0.0.255
end

ipv4 access-list acl_10
 10 permit ip 10 .1.1.0 0.0.0.255 any
 20 permit ip 10 .2.2.0 0.0.0.255 any
 30 permit ip 10 .3.3.0 0.0.0.255 any
 40 permit ip 10 .4.4.0 0.0.0.255 any
```

Atomic ACL Updates By Using the Disable Option

Atomic ACL updates involve the insertion, modification, or removal of Access List Entries (ACEs) on an interface that is in operation. Such atomic updates consume up to 50% of TCAM resources. There can be an instance where multiple modifications are required and the available resources are not sufficient. The solution to this problem is to disable atomic ACL updates such that the old ACEs are deleted before the new ACEs are added.

Note When you configure the **atomic-disable** statement in an ACL, any ACE modification detaches the ACL, until the modification is complete. In addition to this, the ACL rules are not applied during the modification process. Hence, it is recommended to configure to either permit or deny all traffic until the modification is complete.

Configuration for Disabling Atomic ACL Updates

To disable atomic updates on the hardware, by permitting all packets, use the following configuration.

```
RP/0/RSP0/CPU0:router# hardware access-list atomic-disable
```

Modifying ACLs when Atomic ACL Updates are Disabled

On disabling atomic ACL updates on the hardware, use the steps in this section to modify ACLs.

Add an ACE

Use the following steps to add an ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
!
```

2. Add the ACE to the ACL.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 permit ipv4 30.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if your ACE was added successfully.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
 30 permit ipv4 30.1.1.0/24 any
!
```

You have successfully added an ACE.

Delete an ACE

Use the steps in this section to delete an ACE.

1. Locate the ACL containing the ACE that you want deleted.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
```

```
!
ipv4 access-list list1
 10 permit ipv4 10.1.1.0/24 any
 20 permit ipv4 20.1.1.0/24 any
 30 permit ipv4 30.1.1.0/24 any
!
```

2. Delete the ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# no 30
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the ACE has been removed from the ACL.

```
RP/0/RSP0/CPU0:router(config-ipv4-acl)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 10.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

You have successfully deleted an ACE.

Replace an ACE

Use the steps in this section to replace an ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config-ipv4-acl)#do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 10.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

2. Configure the new ACE to replace the existing ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 11.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the ACE replacement is successful.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

You have successfully replaced an ACE.

Delete an ACE and Add a New ACE

Use the following steps to delete an ACE and add a new ACE.

1. Locate the ACL you want to modify.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 20.1.1.0 0.0.0.255 any
```

2. Delete the required ACE, and add the new ACE.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list list1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# no 20
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 12.1.1.0/24 any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit
```

3. Verify if the modification is successful.

```
RP/0/RSP0/CPU0:router(config)# do show access-lists
...
ipv4 access-list list1
 10 permit ipv4 11.1.1.0 0.0.0.255 any
 20 permit ipv4 12.1.1.0 0.0.0.255 any
```

You have successfully deleted an ACE, and added a new ACE.

Similarly, you can combine the addition, removal, and replacement of ACEs.

IPv6 ACL in Class Map

In Release 4.2.1, Quality of Service (Qos) features on ASR 9000 Ethernet line card and ASR 9000 Enhanced Ethernet line card are enhanced to support these:

- ASR 9000 Enhanced Ethernet LC:
  - Support on L2 and L3 interface and sub-interface
  - Support on bundle L2 and L3 interface and sub-interface
  - Support for both ingress and egress directions
  - ICMP code and type for IPv4/IPv6
- ASR 9000 Ethernet LC:
  - Support on only L3 interface and sub-interface
  - Support on L3 bundle interface and sub-interface
  - Support for both ingress and egress directions
  - ICMP code and type for IPv4/IPv6
- IPv6-supported match fields:
  - IPv6 Source Address
  - IPv6 Destination Address
  - IPv6 Protocol
  - Time to live (TTL) or hop limit
  - Source Port
  - Destination Port
  - TCP Flags
  - IPv6 Flags (Routing Header(RH), Authentication Header(AH) and Destination Option Header(DH))

- Class map with IPv6 ACL that also supports:
  - IPv4 ACL
  - Discard class
  - QoS Group
  - Outer CoS
  - Inner CoS
  - Outer VLAN (ASR 9000 Enhanced Ethernet LC only)
  - Inner VLAN (ASR 9000 Enhanced Ethernet LC only)
  - match-not option
  - type of service (TOS) support
- Policy-map with IPv6 ACL supports:
  - hierarchical class-map

Configuring IPv6 ACL QoS - An Example

This example shows how to configure IPv6 ACL QoS with IPv4 ACL and other fields :

```
ipv6 access-list aclv6
10 permit ipv6 1111:6666::2/64 1111:7777::2/64 authen
30 permit tcp host 1111:4444::2 eq 100 host 1111:5555::2 ttl eq 10
!

ipv4 access-list aclv4
10 permit ipv4 host 10.6.10.2 host 10.7.10.2
!

class-map match-any c.aclv6
match access-group ipv6 aclv6
match access-group ipv4 aclv4
match cos 1
end-class-map
!

policy-map p.aclv6
class c.aclv6
  set precedence 3
!
class class-default
!
end-policy-map
!



show qos-ea km policy p.aclv6 vmr interface tenGigE 0/1/0/6.10 hw

================================================================================
```

```
B : type & id      E : ether type     VO : vlan outer     VI : vlan inner
Q : tos/exp/group  X : Reserved       DC : discard class  Fl : flags
F2: L2 flags       F4: L4 flags       SP/DP: L4 ports
T : IP TTL         D : DFS class#      L : leaf class#
Pl: Protocol       G : QoS Grp         M : V6 hdr ext.     C : VMR count
------------------------------------------------------------------------------
policy name p.aclv6 and km format type 4
Total Egress TCAM entries: 5
|B    F2 VO   VI   Q  G  DC T  F4 Pl SP   DP   M  IPv4/6 SA                          IPv4/6
 DA
==============================================================================
V|3019 00 0000 0000 00 00 00 00 00 00 0000 0000 80 11116666:00000000:00000000:00000000
11117777:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF 7F 00000000:00000000:FFFFFFFF:FFFFFFFF
00000000:00000000:FFFFFFFF:FFFFFFFF
R| C=0 03080200 000000A6 F06000FF 0000FF00 0002FF00 00FF0000 FF000000 00000000
V|3019 00 0000 0000 00 00 00 0A 01 00 0064 0000 00 11114444:00000000:00000000:00000002
11115555:00000000:00000000:00000002
M|0000 FF FFFF FFFF FF FF FF 00 FE FF 0000 FFFF FF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=1 03080200 000000A6 F06000FF 0000FF00 0002FF00 00FF0000 FF000000 00000000
V|3018 00 0000 0000 00 00 00 00 00 00 0000 0000 00 0A060A02 -------- -------- --------
0A070A02 -------- -------- --------
M|0000 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF FF 00000000 -------- -------- --------
00000000 -------- -------- --------
R| C=2 03080200 000000A6 F06000FF 0000FF00 0002FF00 00FF0000 FF000000 00000000
V|3018 00 2000 0000 00 00 00 00 00 00 0000 0000 00 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
M|0003 FF 1FFF FFFF FF FF FF FF FF FF FFFF FFFF FF FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
R| C=3 03080200 000000A6 F06000FF 0000FF00 0002FF00 00FF0000 FF000000 00000000
V|3018 00 0000 0000 00 00 00 00 00 00 0000 0000 00 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
M|0003 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF FF FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
R| C=4 03000200 00010002 FF0000FF 0000FF00 0002FF00 00FF0000 FF000000 00000000
```

This example shows how to configure hierarchical policy map:

```
ipv6 access-list aclv6.p
10 permit ipv6 1111:1111::/8 2222:2222::/8

ipv6 access-list aclv6.c
10 permit ipv6 host 1111:1111::2 host 2222:2222::3

class-map match-any c.aclv6.c
match not access-group ipv6 aclv6.c
end-class-map
!

class-map match-any c.aclv6.p
match access-group ipv6 aclv6.p
end-class-map
!

policy-map child
class c.aclv6.c
  set precedence 7
!

policy-map parent
class c.aclv6.p
```

```
  service-policy child
  set precedence 1



(config)#do show qos-ea km policy parent vmr interface tenGigE 0/1/0/6 hw

================================================================================
B : type & id      E : ether type     VO : vlan outer     VI : vlan inner
Q : tos/exp/group  X : Reserved       DC : discard class  Fl : flags
F2: L2 flags       F4: L4 flags       SP/DP: L4 ports
T : IP TTL         D : DFS class#      L : leaf class#
Pl: Protocol       G : QoS Grp         M : V6 hdr ext.     C : VMR count

================================================================================
policy name parent and format type 4
Total Ingress TCAM entries: 3
|B    F2 VO   VI   Q  G  DC T  F4 Pl SP   DP   M  IPv4/6 SA                          IPv4/6
 DA
================================================================================
V|200D 00 0000 0000 00 00 00 00 00 00 0000 0000 00 11111111:00000000:00000000:00000002
22222222:00000000:00000000:00000003
M|0000 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF FF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=0 11800200 00020000 29000000 80004100 00000000 00000000 00000000 00000000
V|200D 00 0000 0000 00 00 00 00 00 00 0000 0000 00 11000000:00000000:00000000:00000000
22000000:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF FF 00FFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
00FFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
R| C=1 11800200 00010000 29000000 80004700 00000000 00000000 00000000 00000000
V|200C 00 0000 0000 00 00 00 00 00 00 0000 0000 00 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
M|0003 FF FFFF FFFF FF FF FF FF FF FF FFFF FFFF FF FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
FFFFFFFF:FFFFFFFF:FFFFFFFF:FFFFFFFF
R| C=2 11000200 00030000 00000000 00000000 00000000 00000000 00000000 00000000
```

IPv4 and IPv6 ACL Over BVI

IPv4 and IPv6 ACLs are supported over BVI from Cisco ASR 9000 Second Generation Line Cards.

On the A9K-SIP-700 line cards and Cisco ASR 9000 First Generation Line Cards, ACLs on BVIs are not supported.

Note For Cisco ASR 9000 First Generation Line Cards, ACLs can be applied on the EFP level (IPv4 L3 ACL can be applied on an L2 interface).

Configuring IPv4 ACL over BVI interface - An Example

This example shows how to configure IPv4 ACL over a BVI interface:

```
ipv4 access-list bvi-acl
10 permit ipv4 any any ttl eq 70
```

```
20 deny ipv4 any any ttl eq 60
```

Configuring ABFv4/v6 over IRB/BVI interface

Perform this task to configure ABF (access-list based forwarding) v4/v6 over Integrated Routing and Bridging(IRB) or Bridge-Group Virtual Interface (BVI) interface:

SUMMARY STEPS

1. **configure**
2. **ipv4 access-list** *access-list-name*
3. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **nexthop1** [**vrf** *vrf-name*][**ipv4** *ipv4-address1*] **nexthop2** [**vrf** *vrf-name*] [**ipv4** *ipv4-address2*] **nexthop3** [**vrf** *vrf-name*] [**ipv4** *ipv4-address3*]
4. **exit**
5. **ipv6 access-list** *access-list-name*
6. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **nexthop1** [**vrf** *vrf-name*][**ipv6** *ipv6-address1*] **nexthop2** [**vrf** *vrf-name*] [**ipv6** *ipv6-address2*] **nexthop3** [**vrf** *vrf-name*] [**ipv6** *ipv6-address3*]
7. **exit**
8. **interface** *type interface-path-id*
9. { **ipv4** | **ipv6**} **address** *address {network-mask* | *ipv6-prefix}*
10. { **ipv4** | **ipv6**} **access-group** *access-list-name* **{ingress** | **egress}**
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 access-list** *access-list-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv4 acess-list abf-v4`	Enters the IPv4 access list configuration mode, and configures the named access list.
Step 3	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **nexthop1** [**vrf** *vrf-name*][**ipv4** *ipv4-address1*] **nexthop2** [**vrf** *vrf-name*] [**ipv4** *ipv4-address2*] **nexthop3** [**vrf** *vrf-name*] [**ipv4** *ipv4-address3*] **Example:**	Configures the permit conditions for an IPv4 access list.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 any any nexthop1 ipv4 192.168.1.20 nexthop2 ipv4 192.168.9.2 nexthop3 ipv4 192.168.10.2`	

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Returns to global configuration mode.

Step 5	**ipv6 access-list** *access-list-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 acess-list abf-v6`	Enters the IPv6 access list configuration mode, and configures the named access list.
Step 6	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **nexthop1** [**vrf** *vrf-name*][**ipv6** *ipv6-address1*] **nexthop2** [**vrf** *vrf-name*] [**ipv6** *ipv6-address2*] **nexthop3** [**vrf** *vrf-name*] [**ipv6** *ipv6-address3*] **Example:** `RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 any any nexthop1 ipv6 5001:5001::2 nexthop2 ipv6 9001:9001::2 nexthop3 ipv6 1901:1901::2`	Configures the permit conditions for an IPv6 access list.

Step 7	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Returns to global configuration mode.

Step 8	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface BVI 18`	Configures an interface and enters interface configuration mode. • The *type* argument specifies an interface type. For more information on interface types, use the question mark (?) online help function.

	Command or Action	Purpose

		• The *instance* argument specifies either a physical interface instance or a virtual instance.
		  • The naming notation for a physical interface instance is *rack/slot/module/port*. The slash (/) between values is required as part of the notation.
		  • The number range for a virtual interface instance varies depending on the interface type.

Step 9	{ **ipv4 | ipv6**} **address** *address {network-mask | ipv6-prefix}*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)#ipv4 address 192.168.18.1 255.255.255.0`
	`or`
	`RP/0/RSP0/CPU0:router(config-if)#ipv6 address 1801:1801::1/64`
		Configures the primary IPv4 address or IPv6 address for an interface.
		The network mask can be specified in either of two ways:
		• The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address.
		• The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.
		This ipv6-prefix must be in the form documented in RFC 2373 where the address is specified between colons in hexadecimal using 16-bit values.

Step 10	{ **ipv4 | ipv6**} **access-group** *access-list-name* **{ingress | egress}**
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group abfv4 ingress`
	`or`
	`RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group abfv6 ingress`
		Controls access to an interface. The **ipv6 access-group** command is similar to the **ipv4 access-group** command, except that it is IPv6-specific. Use the *access-list-name* to specify a particular IPv6 access list. Use the **ingress** keyword to filter on inbound packets or the **egress** keyword to filter on outbound packets.

Step 11	**commit**	

Configuring ABFv4 over IRB/BVI interface: Example

This example shows how to configure ABFv4 over Integrated Routing and Bridging (IRB)/Bridge-Group Virtual Interface (BVI) interface:

```
interface BVI18
 ipv4 address 192.168.18.1 255.255.255.0
 ipv4 access-group abfv4 ingress
```

```
!


l2vpn
 bridge group bg18
  bridge-domain bd18
   interface GigabitEthernet0/0/1/18
   !
   routed interface BVI18
  !
 !
!

ipv4 access-list abfv4
 10 permit ipv4 any any nexthop1 ipv4 192.168.1.20 nexthop2 ipv4 192.168.9.2 nexthop3 ipv4
 192.168.10.2
!
```

Configuring ABFv6 over IRB/BVI interface: Example

This example shows how to configure ABFv6 over Integrated Routing and Bridging (IRB) or Bridge-Group Virtual Interface (BVI) interface:

```
interface BVI18
 ipv4 address 192.168.18.1 255.255.255.0
 ipv6 address 1801:1801::1/64
 ipv4 access-group abfv4 ingress
 ipv6 access-group abfv6 ingress
!

l2vpn
 bridge group bg18
  bridge-domain bd18
   interface GigabitEthernet0/0/1/18
   !
   routed interface BVI18
  !
 !
!
ipv4 access-list abfv4
 10 permit ipv4 any any nexthop1 ipv4 192.168.1.20 nexthop2 ipv4 192.168.9.2 nexthop3 ipv4
 192.168.10.2
!
ipv4 access-list ipv4-abf
 10 permit ipv4 any any nexthop1 vrf 1 ipv4 45.45.45.2
!

ipv6 access-list ipv6-abf
 10 permit ipv6 any any nexthop1 vrf 1 ipv6 2040::2
!
ipv6 access-list ipv6-vrf
 10 permit ipv6 2001::1/64 any nexthop1 ipv6 2075::2
!
ipv6 access-list abfv6-bvi
 10 permit ipv6 any any nexthop1 ipv6 5001:5001::2 nexthop2 ipv6 9001:9001::2 nexthop3 ipv6
 1901:1901::2
!
ipv6 access-list ipv6-thor
 10 permit ipv6 any any nexthop1 vrf 4 ipv6 2001::2
```

```
!
```

Configuring an Interface to accept Common ACL - Examples

This section provides configuration examples of common ACL.

This example shows how to replace an ACL configured on the interface without explicitly deleting the ACL:

```
Interface Pos0/2/0/0
ipv4 access-group common  C_acl ACL1 ingress
commit
replace Interface acl ACL1 by ACL2
Interface Pos0/2/0/0
ipv4 access-group common  C_acl ACL2 ingress
commit
```

This example shows how common ACL cannot be replaced on interfaces without deleting it explicitly from the interface:

```
Interface Pos0/2/0/0
ipv4 access-group common  C_acl1 ACL1 ingress
commit
change the common acl to C_acl2
Interface Pos0/2/0/0
no ipv4 access-group common  C_acl1  ACL1 ingress
commit
Interface Pos0/2/0/0
ipv4 access-group common  C_acl2  ACL1 ingress
commit
```

Note When reconfiguring common ACL, you must ensure that no other interface on the line card is attached to the common ACL. In other words, atomic replacement of common ACL is not possible.

Note If both common ACL and interface ACL are attached to an interface and only one of the above is reconfigured on the interface, then the other will be removed automatically.

```
Interface Pos0/2/0/0
ipv4 access-group common  C_acl1 ACL1 ingress
commit

Interface Pos0/2/0/0
ipv4 access-group  ACL1 ingress
commit
This removes the common acl.
```

```
Interface Pos0/2/0/0
ipv4 access-group common  C_acl1 ACL1 ingress
commit

Interface Pos0/2/0/0
ipv4 access-group common C_acl1  ingress
commit
```

This example shows how the interface ACL is removed:

```
Interface Pos0/2/0/0
ipv4 access-group common  C_acl1 ACL1 ingress
commit

Interface Pos0/2/0/0
no ipv4 access-group common  acl  acl ingress
Commit
```

Configuring ACL Counters for SNMP Query: Example

The following example shows how to configure IPv4 ACL counters for SNMP query.

```
configure
ipv4 access-list CounterExample
permit any ?
  counter    Count matches on this entry
  log        Log matches against this entry
  log-input  Log matches against this entry, including input interface
permit any counter ?
  WORD  Name of counter
permit any counter TestCounter
show configuration

Building configuration...
!! IOS XR Configuration 0.0.0
ipv4 access-list CounterExample
 10 permit ipv4 any any counter TestCounter
permit tcp any any counter TestCounter2

show configuration
Building configuration...
!! IOS XR Configuration 0.0.0
ipv4 access-list CounterExample
 10 permit ipv4 any any counter TestCounter
 20 permit tcp any any counter TestCounter2

commit

show access-lists ipv4 CounterExample

ipv4 access-list CounterExample
 10 permit ipv4 any any counter TestCounter
 20 permit tcp any any counter TestCounter2
```

The following example shows how to configure IPv6 ACL counters for SNMP query.

```
conf igure
```

```
ipv6 access-list V6CounterExample
permit tcp any any counter ?
  WORD  Name of counter
permit tcp any any counter TestCounter6

show configconfiguration
Building configuration...
!! IOS XR Configuration 0.0.0
ipv6 access-list V6CounterExample
 10 permit tcp any any counter TestCounter6

commit

show access-lists ipv6 V6CounterExample

ipv6 access-list V6CounterExample
 10 permit tcp any any counter TestCounter6
```

Additional References

The following sections provide references related to implementing access lists and prefix lists.

Related Documents

Related Topic	Document Title
Access list commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Access List Commands* module in *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
Prefix list commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Prefix List Commands* module in *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
Terminal services commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Terminal Services Commands* module in *System Management Command Reference for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

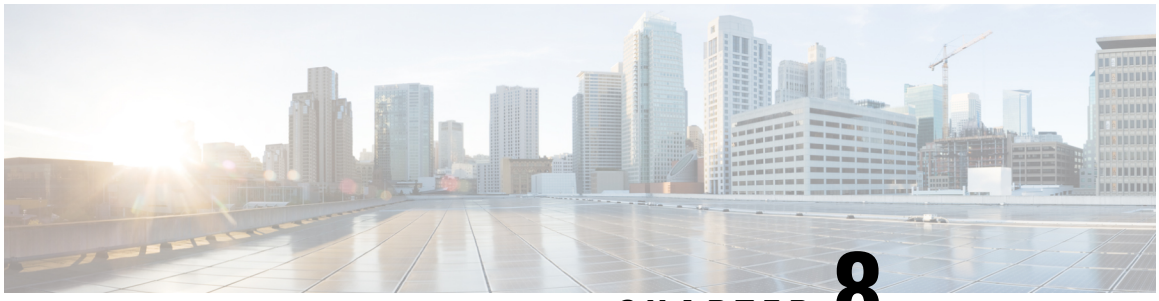
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 8

Implementing Enhanced Policy Based Routing

This section explains the procedures for configuring Enhanced Policy Based Routing (ePBR) with ACLs, MPLS-TE, and BGP Flow spec.

Configuring ACLs with Enhanced Policy Based Routing

Enhanced Policy based routing (ePBR) is used to direct packets that arrive at an interface to a specified next-hop. ePBR is very useful in managing a large number of configured access lists more efficiently.

In ePBR, the router drops the traffic packets if the next hop configured in the PBR policy is not reachable. To avoid packet loss in such scenarios, you must configure multiple next hops for each access control entry.

Restrictions

- PBR is not supported on Pseudowire Headend (PHWE) subinterfaces.
- On Cisco ASR 9000 Series 3rd Generation Line Cards, compressed Access Control Lists (ACLs) are not supported when combined with Policy Based Routing (PBR). However, ACLs without compression can be used with PBR.

Configuration

Use the following sample configuration to configure ACLs with ePBR.

```
/* Configure an access list */
Router(config)# ipv4 access-list INBOUND-ACL
Router(config-ipv4-acl)# 10 permit ipv4 any host 1.1.1.10
Router(config-ipv4-acl)# 20 permit ipv4 any host 1.2.3.4
Router(config-ipv4-acl)# commit
Mon Nov  6 17:22:42.529 IST
Router(config-ipv4-acl)# exit

/* Configure a class map for the access list */
```

```
Router(config)# class-map type traffic match-any INBOUND-CLASS
Router(config-cmap)# match access-group ipv4 INBOUND-ACL
Router(config-cmap)# end-class-map
Router(config)# commit
Mon Nov  6 17:29:12.026 IST

/* Configure an ePBR policy map with the class map */
Router(config)# policy-map type pbr INBOUND-POLICY
Router(config-pmap)# class type traffic INBOUND-CLASS
Router(config-pmap-c)# redirect nexthop 192.168.10.1
Router(config-pmap-c)# exit
Router(config-pmap)# class type traffic class-default
Router(config-pmap-c)# transmit
Router(config-pmap-c)# commit
Mon Nov  6 17:25:33.858 IST
Router(config-pmap)# end-policy-map

/* Configure a GigE interface and apply the ePBR policy map to the interface */
Router(config)# interface GigabitEthernet 0/0/0/0
Router(config-if)# ipv4 address 10.10.10.1 255.255.255.0
Router(config-if)# service-policy type pbr input INBOUND-POLICY
Router(config-if)# commit
Mon Nov  6 17:31:23.645 IST
Router(config-if)# exit
```

Running Configuration

Validate the configuration by using the **show run** command.

```
Router(config)# show running-config
Mon Nov  6 17:31:59.015 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Mon Nov  6 17:31:23 2017 by UNKNOWN
!
ipv4 access-list INBOUND-ACL
 10 permit ipv4 any host 1.1.1.10
 20 permit ipv4 any host 1.2.3.4
!
!
class-map type traffic match-any INBOUND-CLASS
 match access-group ipv4 INBOUND-ACL
 end-class-map
!
!
policy-map type pbr INBOUND-POLICY
 class type traffic INBOUND-CLASS
  redirect ipv4 nexthop 192.168.10.1
 !
 class type traffic class-default
  transmit
 !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 service-policy type pbr input INBOUND-POLICY
 ipv4 address 10.10.10.1 255.255.255.0
!
```

Using ePBR for MPLS Packets on Subscriber Interfaces

The enhanced policy based routing (ePBR) match/redirect MPLS packets on subscriber interfaces feature enables the capability to match MPLS labeled packets and redirect those to an external server by re-writing the source and destination IP addresses of the packets. This feature is applicable when the DNS server (an external server) is hidden in the MPLS cloud.

The traffic that is entering the MPLS cloud will be matched for a specific destination address and based on it, the new destination will be set. When the packet returns from the DNS server, the source address is changed back to the original source address.

Use Case: Using ePBR for MPLS Packets on Subscriber Interfaces

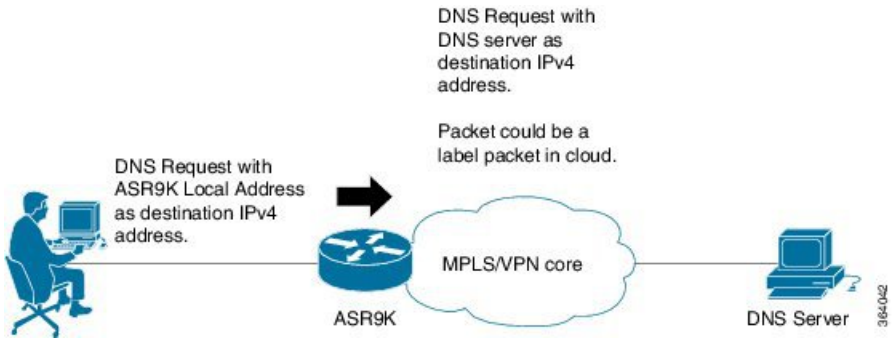
The ePBR match/redirect MPLS packets on subscriber Interfaces feature is applicable when a packet arrives at an interface with a destination address of a known server. This feature changes the known destination address to a required address that is hidden in the DNS cloud. For example, when the packet reaches a known interface with a specific IP address, say 10.0.0.1, it can to be redirected to a new IP address, say 172.16.0.1 , that is hidden in the cloud.

For subscriber to core DNS packets, the sequence for match and redirect is:

- Match the incoming packet for the known DNS server. This address could be a local address on the Cisco ASR 9000 Series Router, which the subscriber uses as DNS server address.
- Set the destination address to a new IP address to which the packet has to be redirected.

This figure explains the match and redirect sequence for subscriber to core DNS packets.

Figure 14: Subscriber to core DNS packets

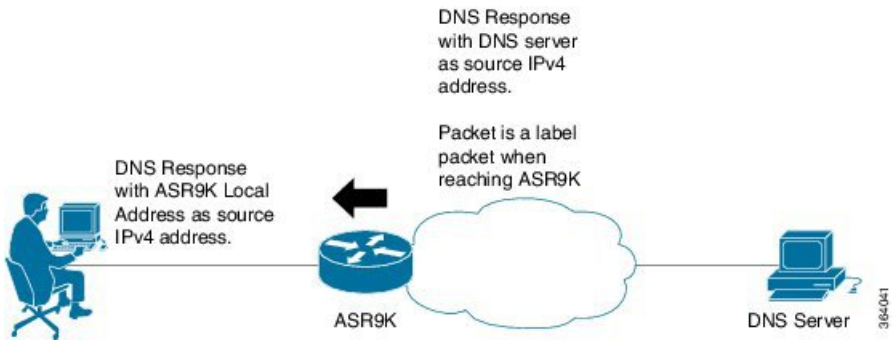


For core to subscriber DNS packets, the sequence for match and redirect is :

- Match the incoming labeled DNS packet's source IP address from the core.
- Set the source address to a local address, which the subscriber uses as DNS server address. The packet would be forwarded based on label + destination IP address, which is the subscriber address.

This figure explains the match and redirect sequence for core to subscriber DNS packets.

Figure 15: Core to subscriber DNS packets



Configuring ePBR-Based MPLS Redirection

These examples show how to configure ePBR-based MPLS match/redirect configuration.

Match configuration for IPv4 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_src_test
  set source-address ipv4 17.17.18.18
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_mpls_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_src_test
match mpls disposition access-group ipv4 ACL_MPLS_SRC
 end-class-map
!

show running-config ipv4 access-list ACL_MPLS_SRC
Wed Sep  3 02:53:40.918 UTC
ipv4 access-list ACL_MPLS_SRC
10 permit ipv4 30.1.1.1/24 112.112.0.1/24
!
```

Match configuration for IPv6 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_ipv6_src_test
  set source-address ipv4 10.10.10.10
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config class-map type traffic class_mpls_ipv6_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_ipv6_src_test
match mpls disposition access-group ipv6 ACL_MPLS_IPV6__SRC
 end-class-map
!
```

```
show running-config ipv6 access-list ACL_MPLS_IPV6_SRC
Wed Sep  3 02:53:40.918 UTC
Ipv6 access-list ACL_MPLS_IPV6_SRC
10 permit ipv6 any any
!
```

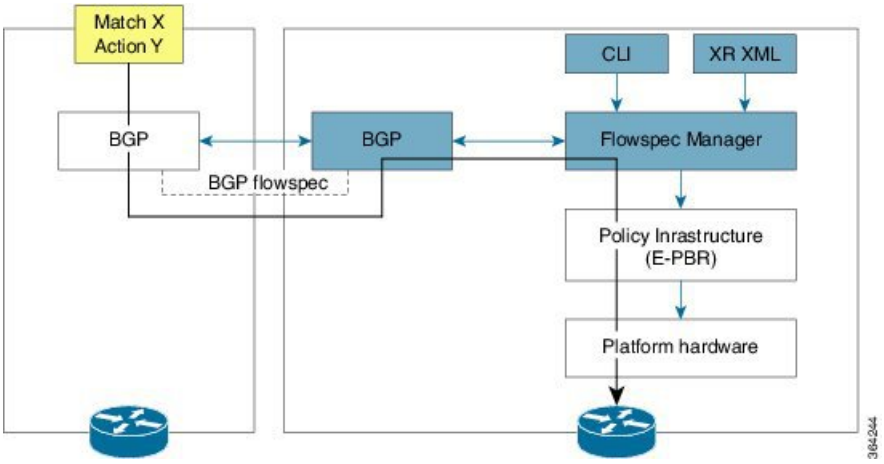
Set destination configuration:

```
show running-config policy-map type pbr pbr_prec_exp
Wed Sep  3 03:11:16.000 UTC
policy-map type pbr pbr_prec_exp
class type traffic class_prec_exp
  set destination-address ipv4 192.168.0.1
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_prec_e$
Wed Sep  3 03:11:30.339 UTC
class-map type traffic match-all class_prec_exp
match mpls experimental topmost 2
 match mpls disposition access-group ipv4 acl2
 end-class-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config ipv4 access-list acl2
Wed Sep  3 03:11:47.963 UTC
ipv4 access-list acl2
5 permit ipv4 host 10.10.10.10 any
10 permit ipv4 any any
!
```

BGP Flowspec Client-Server (Controller) Model and Configuration with ePBR

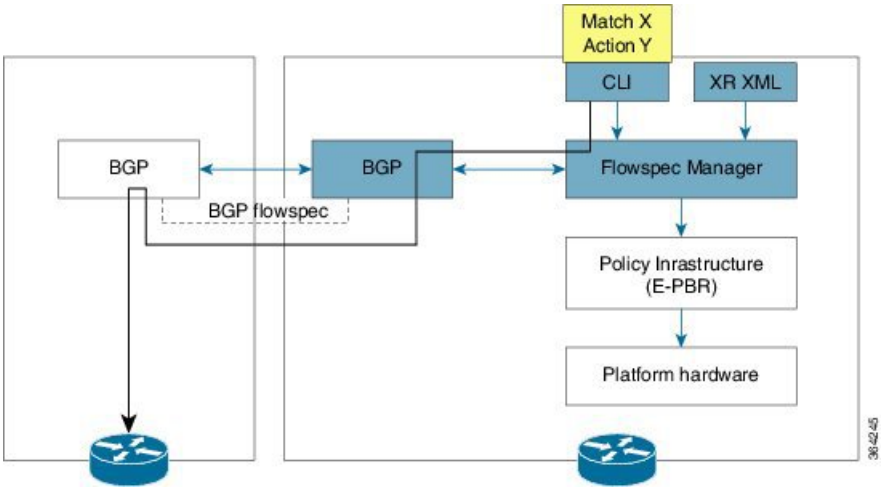
The BGP Flowspec model comprises of a Client and a Server (Controller). The Controller is responsible for sending or injecting the flowspec NRLI entry. The client (acting as a BGP speaker) receives that NRLI and programs the hardware forwarding to act on the instruction from the Controller. An illustration of this model is provided below.

BGP Flowspec Client



Here, the Controller on the left-hand side injects the flowspec NRLI, and the client on the right-hand side receives the information, sends it to the flowspec manager, configures the ePBR (Enhanced Policy-based Routing) infrastructure, which in turn programs the hardware from the underlaying platform in use.

BGP Flowspec Controller



The Controller is configured using CLI to provide that entry for NRLI injection.

BGP Flowspec Configuration

- **BGP-side**: You must enable the new address family for advertisement. This procedure is applicable for both the Client and the Controller. Enable BGP Flowspec, on page 207 explains the procedure.

  Client-side: No specific configuration, except availability of a flowspec-enabled peer.

- **Controller-side**: This includes the policy-map definition and the association to the ePBR configuration consists of two procedures: the class definition, and using that class in ePBR to define the action. The following topics explain the procedure:

  - Configure a Policy Map, on page 210
  - Configure a Class Map, on page 208
  - Link BGP Flowspec to ePBR Policies , on page 212

Configuring BGP Flowspec with ePBR

The following sections explain the procedures for configuring BGP flowspec with ePBR.

Use the following procedures to enable and configure the BGP flowspec feature:

- Enable BGP Flowspec, on page 207
- Configure a Class Map, on page 208
- Link BGP Flowspec to ePBR Policies , on page 212

Note To save configuration changes, you must commit changes when the system prompts you.

Enable BGP Flowspec

You must enable the address family for propagating the BGP flowspec policy on both the Client and Server using the following steps:

SUMMARY STEPS

1. **configure**
2. **router bgp** *as-number*
3. **address-family** { **ipv4** | **ipv6** | **vpnv4** | **vpnv6** } **flowspec**
4. **exit**
5. **neighbor** *ip-address*
6. **remote-as** *as-number*
7. **address-family** { **ipv4** | **ipv6** } **flowspec**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router bgp** *as-number* **Example:** `RP/0/RSP0/CPU0:router(config)# router bgp 100`	Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.
Step 3	**address-family** { **ipv4**	**ipv6**	**vpnv4**	**vpnv6** } **flowspec** **Example:** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 flowspec`	Specifies either the IPv4, IPv6, vpn4 or vpn6 address family and enters address family configuration submode, and initializes the global address family for flowspec policy mapping.

	Command or Action	Purpose
Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-bgp-af)# exit`	Returns the router to BGP configuration mode.
Step 5	**neighbor** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-bgp)#neighbor 1.1.1.1`	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.
Step 6	**remote-as** *as-number* **Example:** `RP/0/RSP0/CPU0:router(config-bgp-nbr)#remote-as 100`	Assigns a remote autonomous system number to the neighbor.
Step 7	**address-family** { **ipv4** | **ipv6** } **flowspec** **Example:** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 flowspec`	Specifies an address family and enters address family configuration submode, and initializes the global address family for flowspec policy mapping.

Configuring an address family for flowspec policy mapping: Example

```
router bgp 100
 address-family ipv4 flowspec
 ! Initializes the global address family
 address-family ipv6 flowspec
 !
 neighbor 1.1.1.1
  remote-as 100
  address-family ipv4 flowspec
  ! Ties it to a neighbor configuration
  address-family ipv6 flowspec
  !
```

Configure a Class Map

In order to associate the ePBR configuration to BGP flowspec you must perform these sub-steps: define the class and use that class in ePBR to define the action. The steps to define the class include:

SUMMARY STEPS

1. **configure**
2. **class-map [type traffic] [match-all]** *class-map-name*
3. **match** *match-statement*
4. **end-class-map**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**class-map [type traffic] [match-all]** *class-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# class-map type traffic match all classc1`	Creates a class map to be used for matching packets to the class whose name you specify and enters the class map configuration mode. If you specify **match-any** , one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default. If you specify **match-all** , the traffic must match all the match criteria.
Step 3	**match** *match-statement* **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# match protocol ipv4 1 60`	Configures the match criteria for a class map on the basis of the statement specified. Any combination of tuples 1-13 match statements can be specified here. The tuple definition possibilities include: • Type 1: **match destination-address** {**ipv4** | **ipv6**} *address/mask length* • Type 2: **match source-address** {**ipv4** | **ipv6**} *address/mask length* • Type 3: **match protocol** {*protocol-value* | *min-value* *−max-value*} **Note** In case of IPv6, it will map to last next-header. • Type 4: Create two class-maps: one with source-port and another with destination-port: • **match source-port** {*source-port-value* | *min-value* *−max-value*} **Note** Only up to 5 port numbers are supported in a single match string. • **match destination-port** {*destination-port-value* | *min-value* *−max-value*} **Note** These are applicable only for TCP and UDP protocols.

	Command or Action	Purpose
		• Type 5: **match destination-port** {*destination-port-value* | [*min-value* – *max-value*]} • Type 6: **match source-port** {*source-port-value* | [*min-value* – *max-value*]} • Type 7: **match** {**ipv4** | **ipv6**} **icmp-code** {*value* | *min-value* –*max-value*} • Type 8: **match** {**ipv4** | **ipv6**} **icmp-type** {*value* | *min-value* –*max-value*} • Type 9: **match tcp-flag** *value* **bit-mask** *mask_value* • Type 10: **matchpacket length** {*packet-length-value* | *min-value* –*max-value*}} • Type 11: **match dscp** {*dscp-value* | *min-value* –*max-value*} • Type 12: **match fragment-type** {**dont-fragment** **is-fragment** **first-fragment** **last-fragment**} • Type 13: **match ipv6 flow-label ipv4 flow-label** {*value* | *min-value* –*max-value*} *BGP Flowspec Commands* in the *Routing Command Reference for Cisco ASR 9000 Series Routers* guide provides additional details on the various commands used for BGP flowspec configuration.
Step 4	**end-class-map** **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# end-class-map`	Ends the class map configuration and returns the router to global configuration mode.

What to do next

Associate the class defined in this procedure to a PBR policy as described in Configure a Policy Map, on page 210.

Configure a Policy Map

This procedure helps you define a policy map and associate it with traffic class you configured previously in Configure a Class Map, on page 208 .

SUMMARY STEPS

1. **configure**
2. **policy-map type pbr** *policy-map*
3. **class** *class-name*
4. **class type traffic** *class-name*
5. *action*
6. **exit**

7. **end-policy-map**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type pbr** *policy-map* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type pbr policyp1`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters the policy map configuration mode.
Step 3	**class** *class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	Specifies the name of the class whose policy you want to create or change.
Step 4	**class type traffic** *class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic classc1`	Associates a previously configured traffic class with the policy map, and enters control policy-map traffic class configuration mode.
Step 5	*action* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# set dscp 5`	Define extended community actions as per your requirement. The options include: • Traffic rate: **police rate** *rate* • Redirect VRF: **redirect** { **ipv4ipv6** }**extcommunity rt** *route_target_string* • Traffic Marking: **set** { **dscp** *rate* | **destination-address** {**ipv4** | **ipv6**} *8-bit value*} • Redirect IP NH: **redirect** { **ipv4ipv6** } **nexthop** *ipv4 addressipv6 address* { *ipv4 addressipv6 address*}
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	Returns the router to policy map configuration mode.

	Command or Action	Purpose
Step 7	**end-policy-map** **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# end-policy-map`	Ends the policy map configuration and returns the router to global configuration mode.

What to do next

Perform VRF and flowspec policy mapping for distribution of flowspec rules using the procedure explained in Link BGP Flowspec to ePBR Policies , on page 212

Link BGP Flowspec to ePBR Policies

For BGP flowspec, an ePBR policy is applied on a per VRF basis, and this policy is applied on all the interfaces that are part of the VRF. If you have already configured a ePBR policy on an interface, it will not be overwritten by the BGP flowspec policy. If you remove the policy from an interface, ePBR infrastructure will automatically apply BGP flowspec policy on it, if one was active at the VRF level.

Note At a time only one ePBR policy can be active on an interface.

SUMMARY STEPS

1. **configure**
2. **flowspec**
3. **local-install interface-all**
4. **address-family ipv4**
5. **local-install interface-all**
6. **service-policy type pbr** *policy-name*
7. **exit**
8. **address-family ipv6**
9. **local-install interface-all**
10. **service-policy type pbr** *policy-name*
11. **vrf** *vrf-name*
12. **address-family ipv4**
13. **local-install interface-all**
14. **service-policy type pbr** *policy-name*
15. **exit**
16. **address-family ipv6**
17. **local-install interface-all**
18. **service-policy type pbr** *policy-name*
19. **commit**
20. **exit**
21. **show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**flowspec** **Example:** `RP/0/RSP0/CPU0:router(config)# flowspec`	Enters the flowspec configuration mode.
Step 3	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# address-family ipv4`	Specifies either an IPv4 address family and enters address family configuration submode.
Step 5	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 6	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv4 interface to be used as the service policy for that interface.
Step 7	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# exit`	Returns the router to flowspec configuration mode.
Step 8	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)#`	Specifies an IPv6 address family and enters address family configuration submode.

	Command or Action	Purpose
	`address-family ipv6`	
Step 9	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 10	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv6 interface to be used as the service policy for that interface.
Step 11	**vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# vrf vrf1`	Configures a VRF instance and enters VRF flowspec configuration submode.
Step 12	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf)# address-family ipv4`	Specifies an IPv4 address family and enters address family configuration submode.
Step 13	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 14	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv4 interface to be used as the service policy for that interface.
Step 15	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# exit`	Returns the router to VRF flowspec configuration submode.

	Command or Action	Purpose
Step 16	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf)# address-family ipv6`	Specifies either an IPv6 address family and enters address family configuration submode.
Step 17	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 18	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv6 interface to be used as the service policy for that interface.
Step 19	**commit**	
Step 20	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# exit`	Returns the router to flowspec configuration mode.
Step 21	**show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf** **Example:** `RP/0/RSP0/CPU0:routershow flowspec vrf vrf1 ipv4 summary`	(Optional) Displays flowspec policy applied on an interface.

Verify BGP Flowspec

Use these different **show** commands to verify your flowspec configuration. For instance, you can use the associated flowspec and BGP show commands to check whether flowspec rules are present in your table, how many rules are present, the action that has been taken on the traffic based on the flow specifications you have defined and so on.

SUMMARY STEPS

1. **show processes flowspec_mgr location all**
2. **show flowspec summary**

3. **show flowspec vrf** *vrf_name* | **all** { **afli-all** | **ipv4** | **ipv6** }
4. **show bgp ipv4 flowspec**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**show processes flowspec_mgr location all**
	Example:
	`# show processes flowspec_mgr location all`
	`node:  node0_3_CPU0`
	`Job Id: 10`
	`PID: 43643169`
	`Executable path:`
	`/disk0/iosxr-fwding-5.2.CSC33695-015.i/bin/flowspec_mgr`
	`Instance #: 1`
	`Version ID: 00.00.0000`
	`Respawn: ON`
	`Respawn count: 331`
	`Max. spawns per minute: 12`
	`Last started: Wed Apr  9 10:42:13 2014`
	`Started on config: cfg/gl/flowspec/`
	`Process group: central-services core: MAINMEM`
	`startup_path: /pkg/startup/flowspec_mgr.startup`
	`Ready: 1.113s`
	`Process cpu time: 0.225 user, 0.023 kernel, 0.248 total`
	`JID  TID CPU Stack pri state  TimeInState HR:MM:SS:MSEC  NAME`
	`1082  1  0  112K  10 Receive  2:50:23:0508 0:00:00:0241 flowspec_mgr`
	`1082  2  1  112K  10 Sigwaitinfo 2:52:42:0583 0:00:00:0000 flowspec_mgr`
		Specifies whether the flowspec process is running on your system or not. The flowspec manager is responsible for creating, distributing and installing the flowspec rules on the hardware.

Step 2	**show flowspec summary**
	Example:
	`# show flowspec summary`
	`FlowSpec Manager Summary:`
	`  Tables:  2`
	`  Flows:  1`
	`RP/0/3/CPU0:RA01_R4#`
		Provides a summary of the flowspec rules present on the entire node. In this example, the 2 table indicate that IPv4 and IPv6 has been enabled, and a single flow has been defined across the entire table.

Step 3	**show flowspec vrf** *vrf_name*	**all** { **afli-all**	**ipv4**	**ipv6** }
				Example:
				`# show flowspec vrf default ipv4 summary`
				`Flowspec VRF+AFI table summary:`
				`VRF: default`
				`  AFI: IPv4`
				`  Total Flows:  1`
					In order to obtain more granular information on the flowspec, you can filter the show commands based on a particular address-family or by a specific VRF name. In this example, 'vrf default' indicates that the flowspec has been defined on the default table. The 'IPv4 summary' shows the IPv4 flowspec rules present on that default table. As there are no IPv6s configured, the value shows 'zero' for ipv6 summary 'Table Flows' and 'Policies' parameters. 'VRF all' displays information across all the VRFs configured on

	Command or Action	Purpose
	Total Service Policies: 1 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf default ipv6 summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf all afi-all summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv4 Total Flows: 1 Total Service Policies: 1 VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 --- # show flowspec vrf default ipv4 Dest:110.1.1.0/24, Source:10.1.1.0/24,DPort:>=120&<=130, SPort:>=25&<=30,DSCP:=30 detail AFI: IPv4 Flow :Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30 Actions :Traffic-rate: 0 bps (bgp.1) Statistics (packets/bytes) Matched : 0/0 Transmitted : 0/0 Dropped : 0/0	the table and afli-all displays information for all address families (IPv4 and IPv6). The **detail** option displays the 'Matched', 'Transmitted, ' and 'Dropped' fields. These can be used to see if the flowspec rule you have defined is in action or not. If there is any traffic that takes this match condition, it indicates if any action has been taken (that is, how many packets were matched and whether these packets have been transmitted or dropped.
Step 4	**show bgp ipv4 flowspec** **Example:** # show bgp ipv4 flowspec Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 BGP routing table entry for Dest:110.1.1.0/24, Source:10.1.1.0/24,Proto:=47,DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 <snip> Paths: (1 available, best #1) Advertised to update-groups (with more than one peer): 0.3 Path #1: Received by speaker 0 Advertised to update-groups (with more than one peer): 0.3 Local 0.0.0.0 from 0.0.0.0 (3.3.3.3) Origin IGP, localpref 100, valid, redistributed, best, group-best Received Path ID 0, Local Path ID 1, version 42	Use this command to verify if a flowspec rule configured on the controller router is available on the BGP side. In this example, 'redistributed' indicates that the flowspec rule is not internally originated, but one that has been redistributed from the flowspec process to BGP. The extended community (BGP attribute used to send the match and action criteria to the peer routers) you have configured is also displayed here. In this example, the action defined is to rate limit the traffic.

	Command or Action	Purpose
	`Extended community: FLOWSPEC Traffic-rate:100,0`	

Supported Match and Set Operations—ABF, ePBR/Flowspec, and PBR

The following table illustrates the match/set criteria that is supported by ABF, ePBR/Flowspec, and PBR:

Table 10: Supported Match and Set Operations

match/set criteria	ABF	ePBR/Flowspec	PBR
source ip	match	match	match
destination ip	match	match	match
source protocol/port	match	match	match
destination protocol/port	match	match	match
nexthop ip	set	set	set
nexthop vrf	set	set	set
nexthop ip+vrf	set	NA	set
dscp	NA	match/set	NA
forward-class	NA	NA	set
police	NA	set	NA
access-group	NA	NA	match
flow-tag	NA	NA	match
fragment-type	NA	match	NA
packet length	NA	match	NA
ip protocol	match	match	match
tcp-flag	match	match	match
ipv4/ipv6 icmp-type	NA	match	NA
ipv4/ipv6 icmp-code	NA	match	NA
port	NA	match	NA
port-range	match	match	match

Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

Related Topic	Document Title
the Cisco ASR 9000 Series Router Transport Stack commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Transport Stack Commands in the IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*MPLS Label Distribution Protocol Commands in the MPLS Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router OSPF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*OSPF Commands in the Routing Command Reference for Cisco ASR 9000 Series Routers*
MPLS Label Distribution Protocol feature information	*Implementing MPLS Label Distribution Protocol in the MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
OSPF feature information	*Implementing OSPF in the Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

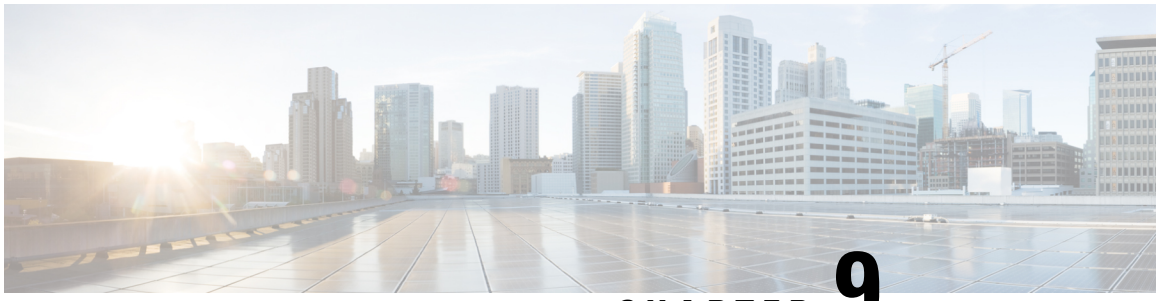
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 9

Implementing Video Monitoring

Configuring Video Monitoring is a four-step procedure, which includes configuring the relevant class-maps and policy maps, and binding the video monitoring policy to an interface.

Prerequisites for Implementing Video Monitoring

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must install and activate packages for advanced video services. For detailed information about optional package installation, see *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*.
- You must install and activate a package for the multicast routing software and enable multicast routing on the system. Video monitoring is supported on interfaces that are multicast-enabled. For detailed information about multicast routing, refer to the chapter Implementing Layer 3 Multicast Routing on Cisco ASR 9000 Series Routers.

Information About Implementing Video Monitoring

Video Monitoring

Poor video experience is a major cause for concern among service providers in terms of service costs and loss of revenue. To avoid the service costs of help desk time, NOC (network operation center) troubleshooting resources, and truck rolls, the capability of monitoring video traffic is essential. On Cisco IOS XR software, problems in video flows can be easily diagnosed by video monitoring.

Introduction to Video Monitoring

Packet loss is one common cause of video quality degradation. Its impact is more significant on compressed video flows. The video traffic transported through the service provider IP network is mostly compressed video – MPEG or similar encoding. Because of the way compression occurs, the traffic is extremely loss-sensitive. The video is encoded with an independent frame (I-frame) every few seconds, with subsequent frames being deltas from the I-frame. If the loss is in an I-frame, a 3 ms loss of traffic (roughly one IP packet) can result in a viewing degradation for up to 1.2 seconds.

Jitter is a key flow characteristic that requires careful buffer provisioning in the end device. The set top box (STB) that displays the media on a screen needs to decode the video in real-time. It buffers the incoming video stream so that it can decode and display the image smoothly. Large network jitter can lead to buffer underrun or overrun on the STB. Depending on how large the jitter is, this will create a visual distortion or a freezing of the video at display.

End-to-end delay in transmission is not significant for a broadcast-only application. However, as the video applications get to be more interactive, the end-to-end latency (delay) becomes a critical Quality of Experience (QoE) component. Data loss is a major contributor for poor QoE.

Three main contributors to poor QoE can be summed up as:

- Packet Loss
- Jitter
- Delay

Video Monitoring plays a very significant role in improving video quality, and thus, in enhancing the QoE. Video monitoring is implemented on the routers and enables network operators to measure and track video transport performance on a per-flow basis. The video packets flow through a router. We can use the packet headers and compute a metric that gives us a measure of the network performance impacting the quality of the video. This information from multiple routers is compared for the same flow to get a clear end-to-end picture of the video issues in the network and the affected flows.

Problems in video flows (and more generally, any streaming flow) can be diagnosed by video monitoring. The purpose of video monitoring is to detect perturbations and anomalies introduced by the network that cause a degraded QoE; that is, it measures the transport performance for streaming (video) traffic. Encoding errors, audio-video-lag, and other errors too cause poor QoE. However, these are introduced by the encoding device and not the network. These latter errors are not monitored.

Key Features Supported on Video Monitoring

Direct Measurements from Data Plane

Video monitoring plays a significant role in improving video quality and therefore enhances the QoE. Video monitoring implemented on Cisco ASR 9000 Series Routers enable the network operator to measure and track video transport performance on a per-flow basis in real time. In contrast to the conventional traffic monitoring solutions, (where sampled flows have to be sent to the control plane or additional hardware, such as dedicated blade on the router), video monitoring on Cisco ASR 9000 Series Router performs the monitoring operation on the data plane itself. This enables video monitoring to analyze forwarded packets in real time, to compute a metric that provides a measure of the network performance impacting the quality of the video.

Local Storage and Remote Access

Video monitoring measures packet loss and jitter at wire-speed, and stores collected information on the router, in order that the network operator can access it through a user interface. Furthermore, the performance metrics measured and stored on multiple routers can be accessed through standard SNMP from a remote operation center. These metrics provide a clear end-to-end picture of the video flow that can be composed and analyzed.

Proactive and Reactive Usages

Video monitoring on Cisco ASR 9000 Series Routers serve both reactive and proactive usage for service providers. It can be used to verify the quality of video service, before scaling up the service coverage to new customers. Also, it is a powerful tool for analysis and can be used to troubleshoot customer calls. Network operators can configure video monitoring to raise an alarm for various events such as variation in packet loss, jitter, flow rate, number of flows, and so on. Such an alarm can be configured to get triggered at any possible value or range.

Flow on Video Monitoring

Video monitoring uses four pieces of packet header fields to distinguish a unique flow - source IP address, destination IP address, source UDP port, and destination UDP port (this implies protocol ID is always UDP).

Unicast and Multicast

Video monitoring supports not only the monitoring of flows with IPv4 multicast destination address in the IP header, but also supports the monitoring of flows with unicast destination addresses. The support for video monitoring functionality for unicast flows provides backward compatibility to ASR 9000 Ethernet Line Card, and is also available on ASR 9000 Enhanced Ethernet Line Card .

Flow Rate Types and Protocol Layer

Video monitoring monitors CBR (constant bit rate) flows at the IP layer. In other words, video monitoring can monitor CBR-encoded media streams (for example, MPEG-2) encapsulated in UDP datagram, inside an IPv4 packet. Video monitoring allows users to configure packet rate at IP layer, or bit rate at media layer (along with the number and size of media packets).

Metrics

Video monitoring supports both packet loss and jitter metrics that follow MDI (media delivery index, RFC 4445) definition at the IP-UDP level. The MDI metrics are MLR (media loss rate) and DF (delay factor). Video monitoring uses MRV (media rate variation) which is an extension of MDI MLR; that is, MLR captures only loss, while MRV captures both loss and excess. Video monitoring DF is the same as MDI definition, where DF represents one nominal packet inter-arrival time in addition to the monitored MDI jitter. Along with the two key metrics, Video monitoring supports packet count, byte count, packet rate, bit rate, packet size, TTL (Time to Live) field in IP header, number of flows, raised alarms, and time stamp for various events.

Note The term MDI jitter, is used to signify the correctness of DF metric measured by Video monitoring. MDI jitter is measured by comparing the actual packet arrival time against the nominal arrival reference, while simple inter-packet jitter is measured by the time difference between two consecutive packet arrivals. The former captures the performance of CBR flow more precisely than the latter.

Number of Flows

In the current release, video monitoring on Cisco ASR 9000 Series Router supports 1024 flows per NP(network processor) on ASR 9000 Ethernet Line Card and a maximum of 4096 flows per NP on ASR 9000 Enhanced Ethernet Line Card, for combined unicast and multicast traffic. The number of maximum flows for each line card or for each system varies, depending on the number of NPs on the line card and the number of line cards on the system. Per-chassis flow scale depends on the number of NPs on the chassis.

For example, if you have a Cisco ASR 9000 Series Router box with 4 ASR 9000 Ethernet Line Cards, and if each LC has 8 NPs, per-chassis flow scales up to 1K*8 = 8K flows for each chassis.

High Availability Features

Video monitoring on Cisco ASR 9000 Series Router supports high availability at various levels. It supports process OIR (online insertion and removable), line card OIR, RSP (route switch processor) fail over, and router reload. Configuration is persistent for all high availability scenarios. Monitored statistics data are preserved at process OIR and RSP FO.

Interface Types and Direction

To activate video monitoring, you must configure video monitoring service policy on an interface. There are four types of interfaces to which you can attach the video monitoring policy; these are main interface, subinterface, ethernet bundle interface, and ethernet bundle subinterface. Video monitoring supports only layer 3 interfaces and not layer 2 interfaces. Video monitoring can be configured only on the input direction of the interface.

Flow Rate and DF Precision

Video monitoring on Cisco ASR 9000 Series Router offers DF metric performance of 1 ms precision.

Video monitoring supports standard definition (SD) video traffic (mostly compressed) of up to 100 Mbps flow rate. For uncompressed video streams, flow rate of max 3 Gbps is supported.

User Interface for Input

Video monitoring supports traditional CLI (command line interface) input for configuration that follows MQC (modular QoS configuration) syntax. You can configure video monitoring by configuring access control list (ACL), class map, and policy map; it can be activated by attaching the service policy to an interface. In-place policy modification is not supported. Once attached to an interface, the configured service policy can be modified only after detaching it from the interface.

User Interface for Output

Video monitoring offers various show and clear commands for retrieving the monitored statistics. Refer the Video Monitoring Commands on Cisco ASR 9000 Series Routers module in the *Multicast Command Reference for Cisco ASR 9000 Series Routers* for a detailed description of the video monitoring commands.

You can configure TCA (threshold crossing alert) as a part of the policy map to enable video monitoring to generate syslog message for various conditions. You can also retrieve standing alarms by using **show** command or through a SNMP pull. XML is supported by video monitoring.

Number of Class Maps and Policy Maps

To use video monitoring, you must configure class map and policy map that acts as a filter to determine which flow to monitor on the data plane. Video monitoring supports a maximum of 1024 class maps per policy-map, and a maximum of 1024 class maps per system. It supports a maximum of 256 policy maps on the system.

Video PIE Installation

Video monitoring requires video PIE installation. Depending on the RSP type, the video pie name has two versions:

- asr9k-video-p.pie (RSP2 version)
- asr9k-video-px.pie (RSP3 version)

Video Monitoring Trap and Clone

Trap and clone is an extension to the basic performance monitoring service feature, where the packets from a selected number of flows can be filtered (trapped), duplicated (cloned), and sent to a remote device on the network for a more fine-grained analysis of the video quality. The cloned packets are replicated by the multicast forwarding process to the interface specified in the performance traffic clone profile. The remote device can perform a deeper analysis of the data at the MPEG layer level. This device can be used both as a debugging and a monitoring tool. Also, this device can act as a service engine blade on the same router. For multicast flows, the trap and clone functionality is fully backward-compatible; however, for unicast flows, it is supported with Layer 3 Switched Port Analyzer (SPAN) on Typhoon LCs.

Note L3 SPAN does not support SNMP. For more information on L3 SPAN, refer to Configuring SPAN.

Video Monitoring Terminology

To implement and configure video monitoring service on Cisco ASR 9000 Series Routers, you must first understand video monitoring terminology and concepts.

Interval duration and interval updates

Video monitoring analyzes continuously all packets on the data plane for a time period called interval duration, which is configured by the user. Statistics are exported periodically at the end of each interval duration. These exported statistics are called interval updates. The status of a video monitoring flow and its transition is described solely in reference to these interval updates. Also, all exported video monitoring flow statistics are stored in terms of these interval updates.

The interval duration is a vital video monitoring parameter. Video monitoring configuration anchors upon interval duration for functions such as frequency of export, number of exports to store, time to delete inactive flows, and so on. All video monitoring functionalities, including raising alarm (for stopped flows and flows with performance degradation), are based on the contents of interval updates.

Video monitoring flows

A video monitoring flow is an instance of a packet stream whose header fields match the configured class map (and its associated access control list). A unique flow is local to the interface to which a video monitoring service policy is attached. A video monitoring flow is composed of a series of stored interval updates. A

unique flow that is created on video monitoring after a monitoring interval is called a new flow. Therefore, a packet stream that lives for a period shorter than one monitoring interval is not exported as a video monitoring flow, and is therefore not stored.

Flow stop

If the router stops receiving packets on a monitored flow for one full interval update or longer, the monitored flow is considered as being stopped.

Flow resumption

When a stopped video monitoring flow resumes receiving packets, a normal interval update is exported in the next monitoring interval. A resumed flow has one or more zero intervals, followed by a normal interval update.

Flow switchover

A video monitoring flow on an ethernet bundle interface, or on an ethernet bundle sub-interface, may move from one physical member interface to another; that is, the packet stream stops flowing on one interface and starts flowing on another interface. This is defined as a flow switchover. In such a case, if both interfaces are on the same line card, video monitoring treats the pre-switchover flow and the post-switchover flow as the same flow. Otherwise, it treats them as two different flows.

Flow deletion

If a stopped video monitoring flow continues to export zero intervals for a configured timeout (in terms of the number of monitoring intervals), the flow is considered dead and is marked for deletion. The duration for which the user can control inactive flows is indicated using the timeout parameter. The actual deletion for all the marked flows takes place after some delay by the periodic sweeping function, which is executed every 150 seconds for Trident LC, and executed every 60 seconds for Typhoon LC. Once deleted, all exported statistics (series of interval updates including zero intervals) are completely removed from storage.

Implementing Video Monitoring

Configuring Video Monitoring is a four-step procedure, which includes configuring the relevant class-maps and policy maps, and binding the video monitoring policy to an interface.

Creating IPv4 Access Lists

This step is similar to typical IPv4 access list creation and configuration. An example configuration of ACL for video monitoring is presented here for quick reference. For more details, refer to the *Implementing Access lists and Prefix lists chapter* of the *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers*.

This task configures a standard IPv4 access list.

Standard access lists use source addresses for matching operations.

Note Video Monitoring policy allows **deny** statements in ACL configuration, but **deny** statements are treated as **permit**. Also, log or log-input is not supported in ACL configuration.

SUMMARY STEPS

1. **configure**
2. **ipv4 access-list** *name*
3. [*sequence-number*] **remark** *remark*
4. [*sequence-number*] **permit udp** *source* [*source-port*] **destination** [*destination-port*]
5. Repeat Step 4 as necessary, adding statements by sequence number. Use the **no** *sequence-number* command to delete an entry.
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 access-list** *name* **Example:** `RP/0/RSP0/CPU0:router# ipv4 access-list acl_1`	Enters IPv4 access list configuration mode and configures access list acl_1.
Step 3	[*sequence-number*] **remark** *remark* **Example:** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out`	(Optional) Allows you to comment on the **permit** statement that follows in the named access list. • The remark can be up to 255 characters; anything longer is truncated. • Remarks can be configured before or after **permit** statements, but their location details should be consistent.
Step 4	[*sequence-number*] **permit udp** *source* [*source-port*] **destination** [*destination-port*] **Example:** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit udp 172.16.0.0/24 eq 5000 host 225.0.0.1 eq 5000`	Allows you to specify the source and destination ports with these conditions. • Video monitoring supports only udp. • Use the *source* keyword to specify the network or host number from which the packet is being sent. • Use the optional *source-wildcard* argument to specify the wildcard bits to be applied to the source. • Use the *destination* keyword to specify the network or host number to which the packet is being sent.

	Command or Action	Purpose
		• Use the optional *destination-wildcard* argument to specify the wildcard bits to be applied to the destination.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number. Use the **no** *sequence-number* command to delete an entry.	Allows you to revise an access list.
Step 6	**commit**	

Configuring class-map

This task sets up the flow classifier. This may match either an individual flow, or it may be an aggregate filter matching several flows.

SUMMARY STEPS

1. **configure**
2. **class-map type traffic** *class-map-name*
3. **match access-group ipv4** *acl-name*
4. **end-class-map**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**class-map type traffic** *class-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# class-map type traffic class1`	Enters the class-map mode. The class-map type must always be entered as traffic.
Step 3	**match access-group ipv4** *acl-name* **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# match access-group ipv4 acl1`	Enter the ACL to be matched for this class. Only one ACL can be matched per class.
Step 4	**end-class-map** **Example:**	Completes the class-map configuration.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-cmap)# end-class-map`	
Step 5	**commit**	

Configuring policy-map

The policy map for video monitoring is of the performance-traffic type. Only one level of hierarchy is supported for video monitoring policy-maps. This means that no hierarchical policy map configuration is supported for video monitoring.

The policy map configuration for video monitoring has these three parts:

- Flow parameters configuration: Specifies the different properties of the flow that are monitored such as interval duration, required history intervals, timeout, etc.
- Metric parameters configuration: Specifies the metrics that need to be calculated for the flow that are monitored.
- React parameters configuration: Specifies the parameters, based on which, alerts are generated for the flow.

The configuration hierarchy is from *policy* to *class* to *flow*. This means that all the parameters that are specified above are applied to all flows that match a particular class, in the policy-map. While specifying flow and react parameters for flows matching a given class is optional, its metric parameters is mandatory.

Configuring policy-map with metric parameters

The metric parameters in a policy map can be:

- Layer 3 packet rate or
- Media bit rate (with the number of media packet counts and size in the UDP payload specified).

Note Layer 3 packet rate and Media rate have mutually exclusive configuration commands.

The configuration for each metric parameter is described in this section.

Layer 3 packet-rate

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate layer3 packet** *packet-rate* **pps**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor metric ip-cbr** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric ip-cbr`	Enters the IP-CBR metric monitor submode. **Note** Currently only ip-cbr metric monitoring is supported for video monitoring.
Step 5	**rate layer3 packet** *packet-rate* **pps** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# rate layer3 packet packet-rate pps`	Specifies the IP layer3 packet rate in packets per second (pps).
Step 6	**commit**	

Media bit-rate

The metric parameters for media bit-rate consist of the media bit rate, media packet count and packet size. The rate media option enables the user to specify the number of media payload packets (that is MPEG-2 datagrams) that is present in one UDP packet, and the size of each of such media payload. It is mandatory to specify the media bit rate.There are no defaults for packet count and packet size in Cisco IOS XR Software Release 3.9.1. These values must be configured.

Note With the media bit rate configured to 1052800 bps, media packet count to 7, and media packet size to 188 bytes, the media packet rate is 100 pps at layer 3. The calculation is: 1052800 / (7 *188*x 8) = 100 pps.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate media** *bit -rate* **{bps|kbps|mbps|gbps}**
6. **media packet count in-layer3** *packet-count*
7. **media packet size packet-size**
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enters the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor metric ip-cbr** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric ip-cbr`	Enters the IP-CBR metric monitor submode. **Note** Currently only ip-cbr metric monitoring is supported for video monitoring.
Step 5	**rate media** *bit -rate* **{bps|kbps|mbps|gbps}** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-ipcbr)# rate media 100 mbps`	Specifies the media bit rate for the flow in bps, kbps, mbps or gbps. The configuration can be committed here. Optional parameters can also be specified. **Note** The default unit of media bit-rate is kbps.
Step 6	**media packet count in-layer3** *packet-count* **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-ipbr)# media packet count in-layer3 10`	Specifies the number of media packets for each IP payload.
Step 7	**media packet size packet-size** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-ipcbr)# media packet size 188`	Specifies the size in bytes for each media packet in the IP payload.

	Command or Action	Purpose
Step 8	**commit**	

Configuring policy-map with flow parameters

The flow parameters in a policy map are optional.

For video monitoring, the data plane continuously monitors the flows and the metrics that are exported at the end of every interval. The duration of this interval and the number of such intervals that need to be stored for each flow (history) can also be optionally specified by the user. You can specify these flow parameters for each flow:

- Interval Duration: The time interval at whose end, metrics are exported. This is specified in multiples of 5 (any value between 10 and 300 seconds). The default value is 30.
- History: The number of intervals containing flow information (flow ID, metrics, etc.) that needs be stored for each flow. This can be any value between 1 and 60. The default value is 10.
- Timeout: The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60. The default value is 0. (Note: the timeout value of 0 has a special meaning: the flow will never be timed out and is therefore a static flow).
- Max Flows per class: The maximum number of flows that need to be monitored for each class in the policy. This can be any value between 1 and 1024. The default value is 1024.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. monitor parameters
5. {**interval duration** *duration* | **flows** *number of flows* | **history** *intervals* | **timeout** *duration*}
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:**	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	
Step 4	monitor parameters **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor parameters`	Enters the flow monitor submode.
Step 5	{**interval duration** *duration* | **flows** *number of flows* | **history** *intervals* | **timeout** *duration*} **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-fparm)# interval duration 10`	• Select the **interval duration** option to specify the interval duration per flow; range is 10 to 300 (must be in multiples of 5). The default value is 30. • Select the **history** option to specify the maximum number of interval data that will be stored per flow. It can be any value between 1 and 60. The deafult value is 10. • Select the **timeout** option to specify the timeout in multiples of the interval duration after which an inactive flow will be marked for deletion. Range is between 2 and 60. The default value is 0, indicating a static flow. • Select the **flows** option to specify the maximum number of flows that can be monitored per class. Range is between 1 and 1024. The default valueis 1024.
Step 6	**commit**	

Configuring policy-map with react parameters

The react parameters in a policy map are optional.

The react parameters are a direct reference for the user to indicate the flow quality. The flow is continuously monitored, and at the end of the interval duration, the statistics are examined to determine whether the threshold specified by the user for the specific parameter has exceeded. If it has, a syslog alarm is generated on the console. Once the alarm is set, no further syslog notifications are issued for the condition.

The following react parameters are used to configure the policy-map:

- Media Rate variation (MRV): video monitoring reacts and generates an alarm if the MRV statistic of the flow crosses the user-specified threshold.
- Delay Factor: video monitoring reacts and generates an alarm if the Delay Factor statistic of the flow crosses the user-specified threshold.
- Media-Stop: video monitoring reacts and generates an alarm if a flow stops; this is to indicate that no packets were received for the flow during one full monitoring interval.

- Packet-Rate: video monitoring reacts and generates an alarm if the packet rate of the flow crosses the user-specified threshold.
- Flow-Count: video monitoring reacts and generates an alarm if the flow count for each class crosses the user-specified threshold.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **react react-id** {**mrv** | **delay-factor** | **packet-rate** | **flow-count** | **media-stop**}
5. **threshold type immediate**
6. **threshold value** {**ge** | **gt** | **le** | **lt** | **range**} *limit*
7. **action syslog**
8. **alarm severity** {**error** | **critical** | **alert** | **emergency**}
9. **alarm type** {**discrete** | **grouped**}
10. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**react react-id** {**mrv**	**delay-factor**	**packet-rate**	**flow-count**	**media-stop**} **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# react 1 mrv`	Enters the react parameter configuration submode. The react ID specified here needs to be unique for each class. **Note** For the media-stop react parameter, the threshold-type and threshold-value options are not applicable. For the flow-count react parameter, the alarm-type option is not applicable.

	Command or Action	Purpose
Step 5	**threshold type immediate** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold type immediate`	Specifies the trigger type for the threshold. Currently, the available threshold type is immediate.
Step 6	**threshold value** {**ge** | **gt** | **le** | **lt** | **range**} *limit* **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold value ge 50`	Specifies the trigger value range for the threshold.
Step 7	**action syslog** **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# action syslog`	The **action** keyword specifies the action to be taken if the threshold limit is surpassed. Currently, syslog action is the only option available.
Step 8	**alarm severity** {**error** | **critical** | **alert** | **emergency**} **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm severity critical`	Specifies the alarm severity for syslog.
Step 9	**alarm type** {**discrete** | **grouped**} **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm type discrete`	Specifies the alarm type. Discrete alarm is raised for all the flows that exceed the threshold value. Grouped alarm is raised when a certain number or percentage of the flows exceeds the threshold value.
Step 10	**commit**	

Video Monitoring Metrics

Video monitoring supports RTP, MDI and MPLS metrics in this release.

- The variations of RTP supported are RTP-MMR, RTP-Voice, RTP-J2k, and RTP-Custom
- The variations of MDI supported are MDI-MPEG, and MDI-MPEG over RTP
- The variations of MPLS supported are RSVP-TE, P2MP-TE, LDP, and MLDP

Configuring policy-map with rtp metric parameters

The configuration for each rtp metric parameter is described in this section.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor** *parameters*
5. **timeout** *duration*
6. **exit**
7. **monitor metric**[**rtp** | **rtp-j2k** | **rtp-mmr** | **rtp-voice**]
8. **clock-rate** *value*
9. **max-dropout** *value*
10. **max-misorder** *value*
11. **min-sequential** *value*
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor** *parameters* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# monitor parameters`	Enters the flow monitor submode.
Step 5	**timeout** *duration* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# timeout 2`	The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60.

	Command or Action	Purpose
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# exit`	Exits from the flow monitor submode.
Step 7	**monitor metric**[**rtp** | **rtp-j2k** | **rtp-mmr** | **rtp-voice**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric rtp`	• Enters the corresponding rtp metric monitor submode. The available options are: • rtp - This option is used for custom rtp traffic. • rtp-j2k -This option is used to monitor RTP JPEG 2000 traffic. • rtp-mmr - This option is used to monitor Microsoft Mediaroom traffic. • rtp-voice - This option is used to monitor RTP voice traffic. **Note** When rtp-j2k, rtp-mmr and rtp-voice metrics are used for monitoring, frequency mapping in the dynamic range is configured automatically for specific frequencies. The rtp metric parameter is used for custom rtp traffic. You need to configure the frequency mapping dynamically for the rtp metric parameter. • Enters the flow monitor submode.
Step 8	**clock-rate** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-rtp)# clock-rate 97`	This option is available with the rtp monitor metric only. Enter the dynamic payload type value. Range is from 96 to 27. The RTP clock rate used for generating the RTP timestamp is independent of the number of channels and encoding. The RTP clock rate equals the number of sampling periods per second. The clock frequency for most video streams is 90 kHz. RTP supports all static payload type codes and allows a user to configure dynamic payload type frequency mapping. The available payload type values are: • 8kHz frequency • 16kHz frequency • 11.025kHz frequency • 22.050kHz frequency • 44.1kHz frequency • 48kHz frequency

	Command or Action	Purpose
		• 90kHz frequency (default frequency for RTP) • 27000kHz frequency • 148500kHz frequency • 148.5/1.001MHz frequency
Step 9	**max-dropout** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-rtp)# max-dropout 20`	This option is available with the rtp monitor metric only. Enter the maximum dropout value for RTP flow. The range enforced at policy map creation time is from 1 to 65536. The range enforced at bind time is from 0 to 255. In order to identify an out-of-order packet, a sliding window is maintained to accept non-sequential packets as long as they are with-in the window. Max-dropout provides the look-ahead configuration for sliding window. A packet with sequence number x is considered valid if x is no more than max-dropout ahead of current sequence number. For RTP, 128 clock frequency-payload type mapping tables are supported.
Step 10	**max-misorder** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-rtp)# max-misorder 20`	This option is available with the rtp monitor metric only. Enter the maximum misorder value. The range enforced at policy map creation time is from 1 to 65536. The range enforced at bind time is from 0 to 255. A packet with sequence number x is considered valid if x is no more than max-misorder behind the current sequence number. A sequence number is considered valid only if it is neither more than max-dropout ahead of max seq (currently seen maximum sequence number) nor more than max-misorder behind.
Step 11	**min-sequential** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-rtp)# min-sequential 20`	This option is available with the rtp monitor metric only. Enter the minimum sequential value. The range enforced at policy map creation time is from 1 to 65536. The range enforced at bind time is from 0 to 255. Since UDP header does not have any protocol specific information, there is no way to uniquely identify an RTP packet. Instead, a heuristic way of examining RTP headers of N packet is used in PD to identify the flow. The number of packets is defined by metric parameter of min-sequential.
Step 12	**commit**	

Configuring policy-map with rtp react parameters

The configuration for each rtp metric with react parameter is described in this section.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor** *parameters*
5. **timeout** *duration*
6. **exit**
7. **monitor metric**[**rtp** | **rtp-j2k** | **rtp-mmr** | **rtp-voice**]
8. **react react-id** {**rtp-loss-fraction** | **rtp-jitter** | **rtp-out-of-order** | **rtp-loss-pkts** | **rtp-transport-availability** | **rtp-error-seconds** | **flow-count** | **packet-rate**}
9. **action** [**snmp** | **syslog** | **clone**]
10. **alarm type** [**discrete** | **grouped** { **count** *number* | **percent** *percentage*}]
11. **alarm severity** [**alert** | **critical** | **emergency** | **error**]
12. **threshold** {**ge** | **gt** | **le** | **lt** | **range**} *limit*
13. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor** *parameters* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# monitor parameters`	Enters the flow monitor submode.
Step 5	**timeout** *duration* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)#`	The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60.

	Command or Action	Purpose
	`timeout 2`	
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# exit`	Exits from the flow monitor submode.
Step 7	**monitor metric**[**rtp** | **rtp-j2k** | **rtp-mmr** | **rtp-voice**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric rtp`	• Enters the corresponding rtp metric monitor submode. The available options are: • rtp - This option is used for custom rtp traffic. • rtp-j2k -This option is used to monitor RTP JPEG 2000 traffic. • rtp-mmr - This option is used to monitor Microsoft Mediaroom traffic. • rtp-voice - This option is used to monitor RTP voice traffic. **Note** When rtp-j2k, rtp-mmr and rtp-voice metrics are used for monitoring, frequency mapping in the dynamic range is configured automatically for specific frequencies. The rtp metric parameter is used for custom rtp traffic. You need to configure the frequency mapping dynamically for the rtp metric parameter. • Enters the flow monitor submode.
Step 8	**react react-id** {**rtp-loss-fraction** | **rtp-jitter** | **rtp-out-of-order** | **rtp-loss-pkts** | **rtp-transport-availability** | **rtp-error-seconds** | **flow-count** | **packet-rate**} **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# react 1 rtp-loss-fraction`	Enters the react parameter configuration submode. The react ID specified here needs to be unique for each class. The available options are: • rtp-error-seconds - This option is used for RTP error seconds. Error seconds signifies the amount of time the stream was errored. • rtp-jitter - This option is used for RTP jitter. RTP jitter signifies the average interpacket jitter based on RTP timestamp. • rtp-loss-fraction - This option is used for RTP loss fraction. Loss fraction signifies the percentage of packets that are lost. • rtp-loss-pkts - This option is used for RTP loss packets. Loss pakets signifies the number of packets that are lost.

	Command or Action	Purpose
		• rtp-max-jitter -This option is used for RTP max jitter. Maximum instantaneous jitter during an time interval. • rtp-out-of-order - This option is used for RTP out-of-order packets. Out-of-order packets signifies the number of misordered packets. • rtp-transport-availability - This option is used for RTP transport availability. Transport availability signifies the percentage of time during which the stream does not have any errors. For example, if the RTP error seconds is zero, the RTP transport availablity is hundred percent. • flow-count - This option is used for Flow Count. Flow count signifies the number of flows on a policy. • packet-rate - This option is used for Packet Rate. Packet rate signifies the number of packets during a given time interval.
Step 9	**action** [**snmp** | **syslog** | **clone**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# action snmp`	The action keyword specifies the action to be taken if the threshold limit is surpassed.
Step 10	**alarm type** [**discrete** | **grouped** { **count** *number* | **percent** *percentage*}] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm type discrete`	Specifies the alarm type. Discrete alarm is raised for all the flows that exceed the threshold value. Count alarms are grouped based on number of flows. Percent alarms are grouped based on percentage of flows.
Step 11	**alarm severity** [**alert** | **critical** | **emergency** | **error**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm severity critical`	Specifies the alarm severity for syslog.
Step 12	**threshold** {**ge** | **gt** | **le** | **lt** | **range**} *limit* **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold value ge 50`	Specifies the trigger value range for the threshold.
Step 13	**commit**	

Configuring policy-map with mdi metric parameters

The configuration for each mdi metric parameter is described in this section.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *class-map-name*
4. **monitor** *parameters*
5. **timeout** *duration*
6. **exit**
7. **monitor metric**[**mdi mpeg** | **mdi mpeg rtp**]
8. **max-dropout** *value*
9. **monitor pids** *id*
10. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *class-map-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor** *parameters* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# monitor parameters`	Enters the flow monitor submode.
Step 5	**timeout** *duration* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)#`	The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60.

	Command or Action	Purpose
	`timeout 2`	
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# exit`	Exits from the flow monitor submode.
Step 7	**monitor metric**[**mdi mpeg** | **mdi mpeg rtp**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric mdi mpeg`	Enters the corresponding mdi metric monitor submode. The mdi mpeg rtp option signifies the presence of an rtp header beofre the mpeg header. A maximum of 7 mpeg packets per IP packet are allowed. If a packet contains more than 7 mpeg packets, then the ip packet is ignored. If encapusulation does not match, the flows will not be learned.
Step 8	**max-dropout** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mdi)# max-dropout 20`	Enables packet filtering based on lower bound of stream rate. Range is 1 to 4294967294.
Step 9	**monitor pids** *id* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mdi)# monitor pids 200`	Enable static PID monitoring. The range enforced at policy map creation time is from 1 to 65536. The range enforced at bind time is from 16 to 8191.
Step 10	**commit**	

Configuring policy-map with mdi react parameters

The configuration for each mdi metric with react parameter is described in this section.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor** *parameters*
5. **timeout** *duration*
6. **exit**
7. **react react-id** {**mdi-mlr** | **mdi-mdc** | **mdi-transport-availability** | **mpeg-loss-pkts** | **mdi-error-seconds** | **rtp-error-seconds** | **flow-count** | **mdi-jitter** | **packet-rate** | **media-stop**}
8. **action** [**snmp** | **syslog** | **clone**]
9. **alarm type** [**discrete** | **grouped** { **count** *number* | **percent** *percentage*}]
10. **alarm severity** [**alert** | **critical** | **emergency** | **error**]

11. **threshold** {**ge** | **gt** | **le** | **lt** | **range**} *limit*
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type** *performance-traffic policy-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	**class type** *traffic class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	**monitor** *parameters* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# monitor parameters`	Enters the flow monitor submode.
Step 5	**timeout** *duration* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# timeout 2`	The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60.
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c-mparm)# exit`	Exits from the flow monitor submode.
Step 7	**react react-id** {**mdi-mlr** | **mdi-mdc** | **mdi-transport-availability** | **mpeg-loss-pkts** | **mdi-error-seconds** | **rtp-error-seconds** | **flow-count** | **mdi-jitter** | **packet-rate** | **media-stop**} **Example:**	Enters the react parameter configuration submode. The react ID specified here needs to be unique for each class. The available options are: • mdi-error-seconds - MDI error seconds • mdi-mdc - MDI Media Disc. Count

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config- pmap-c)# react 1 rtp-loss-fraction`	• mdi-mlr - MDI Media Loss Rate • mdi-transport-availability - MDI transport availability • mpeg-loss-pkts - MPEG loss packets • flow-count - Flow Count • mdi-jitter - MDI Jitter • packet-rate - Packet Rate • media-stop - Media Stop Event
Step 8	**action** [**snmp** | **syslog** | **clone**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# action snmp`	The action keyword specifies the action to be taken if the threshold limit is surpassed.
Step 9	**alarm type** [**discrete** | **grouped** { **count** *number* | **percent** *percentage*}] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm type discrete`	Specifies the alarm type. Discrete alarm is raised for all the flows that exceed the threshold value. Count alarms are grouped based on the number of flows and percent alarms are grouped based on the percentage of flows.
Step 10	**alarm severity** [**alert** | **critical** | **emergency** | **error**] **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm severity critical`	Specifies the alarm severity for syslog.
Step 11	**threshold** {**ge** | **gt** | **le** | **lt** | **range**} *limit* **Example:** `RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold value ge 50`	Specifies the trigger value range for the threshold.
Step 12	**commit**	

Configuring flow monitor

Perform this step to configure flow monitor.

SUMMARY STEPS

1. **configure**

2. **flow monitor-map performance-traffic** *monitor-name*
3. **exporter** *exporter-map-name*
4. **record** { **default-rtp | default-mdi** }
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**flow monitor-map performance-traffic** *monitor-name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# flow monitor-map performance-traffic m1`
	`RP/0/RSP0/CPU0:router(config-fmm)#`
		Configures the flow monitor map.

Step 3	**exporter** *exporter-map-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-fmm)# exporter e1`
	`RP/0/RSP0/CPU0:router(config-fmm)#`
		Enter the flow exporter map name.

Step 4	**record** { **default-rtp	default-mdi** }
		Example:
		`RP/0/RSP0/CPU0:router(config-fmm)# record default-rtp`
		`RP/0/RSP0/CPU0:router(config-fmm)#`
			Enter the flow record map name. The available options are:
			• default-rtp - Default MDI record format
			• default-mdi - Default RTP record format

Step 5	**commit**	

Configuring service policy on an interface

The configured policy-map must be attached to an interface in ingress direction in order to enable the Video Monitoring service.

For ethernet bundle interface, service policy can be attached to only the bundle parent interface and not to the physical member interfaces. For ethernet bundle sub-interfaces, it can be attached to only sub-interfaces. For VLAN sub-interfaces, the service policy cannot be attached to the main interface.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **service-policy type performance-traffic input** *policy-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface type interface-path-id`	Configures an interface and enters interface configuration mode. • The type argument specifies an interface type. For more information on interface types, use the question mark (?) online help function. • The instance argument specifies either a physical interface instance or a virtual instance. • The naming notation for a physical interface instance is rack/slot/module/port. The slash (/) between values is required as part of the notation. • The number range for a virtual interface instance varies, depending on the interface type.
Step 3	**service-policy type performance-traffic input** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-if)# service-policy type performance-traffic input policy1`	Attaches the policy to the interface in the ingress direction.
Step 4	**commit**	

Configuring Trap and Clone on an interface

As trap and clone is an extension of the existing video monitoring service, the current control plane infrastructure can be extended to accommodate the configurations for trap and clone.

You can use the flow tuple information (source and destination IP addresses) to install the trap, which eventually leads the matched packets to be further analyzed by a remote device or a local probe.

These steps show how the trap and clone process works in a generic video monitoring scenario:

- You must enable video monitoring by installing the appropriate packages (multicast and video PIEs) and configure ACL, class map, policy map, and bind the policy map to an interface.

- You must configure trap and clone by specifying which flows to clone by specifying the source and the destination of the flows.
- The trap gets installed in the data plane by the VidMon control plane and VidMon data plane starts cloning the packets for the specified flows.
- The cloned packets are forwarded to the remote monitoring device for further analysis.

Note You can use the **show performance traffic clone profile** command to verify the installed traps. The video monitoring trap and clone feature is supported only for multicast traffic, and for unicast flows the user is required to configure SPAN. In multicast, the video monitoring trap and clone feature is implemented using static IGMP groups on the clone interface. The clone interface can be on a dedicated port connected to a local probe.

SUMMARY STEPS

1. **configure**
2. **performance traffic clone profile** *profile_name*
3. **interface** *type interface-path-id*
4. **flow ipv4 source** <*source-ip*> **destination** <*destination-ip*>
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**performance traffic clone profile** *profile_name* **Example:** `RP/0/RSP0/CPU0:router(config)# performance traffic clone profile profile1`	Enters the performance traffic clone profile mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# interface GigabitEthernet 0/0/0/1`	Configures the egress interface to a clone profile.
Step 4	**flow ipv4 source** <*source-ip*> **destination** <*destination-ip*> **Example:**	Configures the traffic flows that needs to be cloned, to the clone profile.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# flow ipv4 source 23.1.1.1 destination 224.2.2.2`	**Note** Multiple flows can be associated with a single clone profile. Similarly, a single flow can be associated with the multiple clone profiles.
Step 5	**commit**	

Configuration Examples for Implementing Video Monitoring

Scenario-1

An ethernet bundle interface has three physical members over which multicast video traffic is flowing at 300 pps for each flow.

Use video monitoring to monitor all the flows on this ethernet bundle, and raise a critical-level alarm, if the per-flow traffic load is over 10 % of expected rate. Raise an error-level alarm if the delay factor is greater than 4 ms. Report the collected statistics every 10 seconds. As long as the flow is active, keep the reported statistics for 10 minutes. Remove flow statistics if no packets are received for 30 seconds.

Example

```
ipv4 access-list sample-acl
 10 permit udp any any
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   interval duration 10
   history 60
   timeout 3
  !
  monitor metric ip-cbr
   rate layer3 packet 300 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value gt 10.00
   action syslog
   alarm severity error
   alarm type discrete
  !
  react 101  delay-factor
   threshold type immediate
   threshold value gt 4.00
   action syslog
   alarm severity error
   alarm type discrete
  !
 !
 end-policy-map
!
```

```
interface Bundle-Ether10
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
interface TenGigE0/6/0/0
 bundle id 10 mode on
!
interface TenGigE0/6/0/1
 bundle id 10 mode on
!
interface TenGigE0/6/0/2
 bundle id 10 mode on
!
```

Scenario-2

A VLAN subinterface is carrying 100 video streams with a common multicast group address of 225.0.0.1 and varying UDP port numbers. The expected packet rate at IP layer is unknown, but the media bit rate is known to be 1052800 bps. The media payload is known to contain MPEG-2 encoded CBR flows and default packetization is used (that is, in one UDP payload, there are seven MPEG packets, where each packet is 188 bytes long).

Do not monitor over 100 flows. Do not timeout and delete any flow even if flow stops, but raise an error-level alarm if the percentage of the stopped flows is over 90 %.

Example

```
ipv4 access-list sample-acl
 10 permit udp any host 225.0.0.1
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   flows 100
!
  monitor metric ip-cbr
   rate media 1052800 bps
  !
  react 100 media-stop
   action syslog
   alarm severity error
   alarm type grouped percent 90
  !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 no shutdown
!
interface GigabitEthernet0/0/0/0.1
 encapsulation dot1q 500
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

Under **monitor metric ip-cbr**, these two lines need not be configured as they are defaults:

- media packet count in-layer3 7
- media packet size 188

However, if these parameters are different from default values, they need to be configured.

Scenario-3

A main interface has three groups of multicast streams where the first group has UDP destination port of 1000, the second group has 2000, and the third group has 3000 and 4000. These three groups of streams flow at 100 pps, 200 pps, and 300 pps respectively.

Limit the maximum number of flows in each group to 300 flows and raise the error-level alarm, when they reach 90 % of the provisioned flow capacity.

Example

```
ipv4 access-list sample-acl-1
 10 permit udp any any eq 1000
!
ipv4 access-list sample-acl-2
 10 permit udp any any eq 2000
!
ipv4 access-list sample-acl-3
 10 permit udp any any eq 3000
 20 permit udp any any eq 4000
!
class-map type traffic match-any sample-class-1
 match access-group ipv4 sample-acl-1
 end-class-map
!
class-map type traffic match-any sample-class-2
 match access-group ipv4 sample-acl-2
 end-class-map
!
class-map type traffic match-any sample-class-3
 match access-group ipv4 sample-acl-3
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class-1
  monitor parameters
   interval duration 10
   history 60
   timeout 3
   flows 300
  !
  monitor metric ip-cbr
   rate layer3 packet 100 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
class type traffic sample-class-2
  monitor parameters
   interval duration 10
   history 60
   timeout 3
```

```
   flows 300
  !
  monitor metric ip-cbr
   rate layer3 packet 200 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
class type traffic sample-class-1
  monitor parameters
   interval duration 10
   history 60
   timeout 3
   flows 300
  !
  monitor metric ip-cbr
   rate layer3 packet 300 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
 !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

Scenario-4

A 10GE main interface receives six high definition (HD) video streams from the digital contents manager (DCM), directly connected to six HD cameras in a sports stadium. Each HD video stream is uncompressed and its bandwidth is as high as 1.611 Gbps at layer 2, which is equivalent to 140625 pps. These six streams are received with multicast groups of 225.0.0.1 through 225.0.0.6, and the UDP port number is 5000.

Raise a critical-level alarm when the delay factor of any flow is above 2 ms, or media loss ratio is above 5 %. Use 10s interval and keep maximum history. Do not monitor more than 6 flows on this interface. Do not time out inactive flows.

Example

```
ipv4 access-list sample-acl
 10 permit udp any eq 5000 225.0.0.0/24 eq 5000
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   interval duration 10
   history 60
```

```
   flows 6
  !
  monitor metric ip-cbr
   rate layer3 packet 140625 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value gt 5.00
   action syslog
   alarm severity critical
   alarm type discrete
  !
  react 200 delay-factor
   threshold type immediate
   threshold value gt 2.00
   action syslog
   alarm severity critical
   alarm type discrete
  !
 end-policy-map
!
interface TenGigE0/2/0/0
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

Scenario-5

An ethernet interface is configured on a Cisco ASR 9000 Series Routers over which multicast video traffic is flowing. Use video monitoring to monitor the performance of all video flows on this ethernet interface. Use the video monitoring trap and clone feature to trap these flow packets and clone (or duplicate) them to a specified egress interface.

Configure a trap and clone profile containing flows that are to be cloned to the specified egress interface. Add a description to the profile.

Example

```
Performance traffic clone profile profile1
   Description video flows monitored by vidmon
   Interface GigE 0/1/1/1
   flow ipv4 source 23.1.1.1 destination 231.2.2.2
```

Scenario-6

A 100GE main interface is receiving 5 high definition (HD) video streams of unicast traffic. Each HD video stream is uncompressed and its bit rate is 3 Gbps. It is known that each stream is CBR flow and has packet rate of 284954 pps. The source of these streams is known as 192.1.1.2 and destinations are from 10.1.1.1 through 10.1.1.5. UDP port 7700 is used for both source and destination.

Raise a critical-level alarm when the delay factor of any of the flow is above 5 ms or CBR flow rate drops over 10% of expected nominal rate. Use 30 s interval and keep 10 intervals as history. Since this port is known to receive additional low rate VoD flows in near future, allow maximum flow count as 4000. Monitor the streams destined to 10.1.1.0/24 subnet only. When quality degradation is detected, report the alarm to NMS system in addition to the syslog output.

Example

```
ipv4 access-list sample-acl
 10 permit udp 192.1.1.2/32 eq 7700 10.1.1.0/24 eq 7700
!
class-map type traffic match-any sample-class  match access-group ipv4 sample-acl
end-class-map
!
policy-map type performance-traffic sample-policy  class type traffic sample-class
  monitor parameters
   interval duration 30
   history 10
   flows 4000
  !
  monitor metric ip-cbr
   rate layer3 packet 284954 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value lt 10.00
   action syslog
   action snmp
   alarm severity critical
   alarm type discrete
  !
  react 200 delay-factor
   threshold type immediate
   threshold value gt 5.00
   action syslog
   action snmp
   alarm severity critical
   alarm type discrete
  !
 end-policy-map
!
interface HundredGigE0/1/0/1
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

Scenario-7

Use video monitoring to monitor all the vidmon-rtp traffic.

Example

```
ipv4 access-list uc
 10 permit udp any 20.0.0.0/24
!
class-map type traffic match-any ucast
 match access-group ipv4 uc
 end-class-map
!
interface TenGigE0/2/0/10
 ipv4 address 10.0.0.1 255.255.255.0
 service-policy type performance input vidmon-rtp
 load-interval 30
!
policy-map type performance-traffic vidmon-rtp
```

```
 class type traffic ucast
  monitor parameters
   interval duration 10
   history 60
   timeout 2
  !
  monitor metric rtp
   clock-rate 96  48kHz
   clock-rate 97  27000kHz
   clock-rate 99  148500kHz
   clock-rate 100  148351.648kHz
  !
 !
 react 101  flow-count
   threshold type immediate
   threshold value gt 0
   action syslog
   alarm severity alert
  !
  react 102  media-stop
   action syslog
   alarm severity critical
   alarm type discrete
  !
 !
 end-policy-map
!
```

Scenario-8

Use video monitoring to monitor all the vidmon-rtp-j2k traffic.

Example

```
policy-map type performance-traffic vidmon-rtp-j2k
 class type traffic ucast
  monitor parameters
   interval duration 10
   history 60
   timeout 2
  !
  monitor metric rtp-j2k
 !
 end-policy-map
!
```

Scenario-9

Use video monitoring to monitor all the mdi mpeg traffic.

Example

```
policy-map type performance-traffic ipcbr-mdi
 class type traffic ucast
  monitor parameters
   interval duration 10
```

```
   history 60
   timeout 2
  !
  monitor metric mdi mpeg
   filter packet-rate 22 pps
  !
 !
 end-policy-map
!
```

Scenario-10

Use video monitoring to monitor all the mdi mpeg rtp traffic.

Example

```
policy-map type performance-traffic rtp-mdi
 class type traffic ucast
  monitor parameters
   interval duration 10
   history 60
   timeout 2
  !
  monitor metric mdi mpeg rtp
  !
 !
 end-policy-map
!
```

Additional References

Related Documents

Related Topic	Document Title
Multicast command reference document	*Multicast Command Reference for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Modular quality of service command reference document	*Modular Quality of Service Command Reference for Cisco ASR 9000 Series Routers*

MIBs

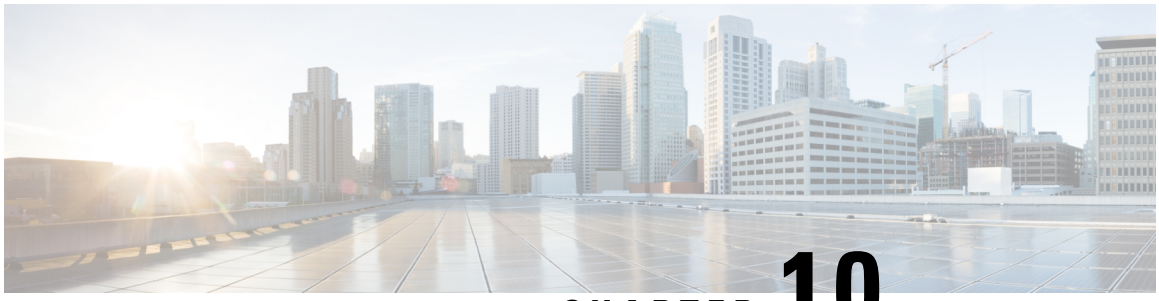
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
RFC4445	Proposed Media Delivery Index (MDI)

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



CHAPTER 10

Implementing Cisco Express Forwarding

Cisco Express Forwarding (CEF) is advanced, Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive web-based applications, or interactive sessions.

This module describes the tasks required to implement CEF on your Cisco ASR 9000 Series Aggregation Services Router.

Note For complete descriptions of the CEF commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference*.

Feature History for Implementing CEF

Release	Modification
Release 3.7.2	This feature was introduced.
Release 6.0.1	IPv6 Flow Label Field for Hashing feature was introduced.

Prerequisites for Implementing Cisco Express Forwarding

The following prerequisites are required to implement Cisco Express Forwarding:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Implementing Cisco Express Forwarding Software

To implement Cisco Express Forwarding features in this document you must understand the following concepts:

Key Features Supported in the Cisco Express Forwarding Implementation

The following features are supported for CEF on Cisco IOS XR software:

- Border Gateway Protocol (BGP) policy accounting
- Reverse path forwarding (RPF)
- Virtual interface support
- Multipath support
- Route consistency
- High availability features such as packaging, restartability, and Out of Resource (OOR) handling
- OSPFv2 SPF prefix prioritization
- BGP attributes download

Benefits of CEF

CEF offers the following benefits:

- Improved performance—CEF is less CPU-intensive than fast-switching route caching. More CPU processing power can be dedicated to Layer 3 services such as quality of service (QoS) and encryption.
- Scalability—CEF offers full switching capacity at each line card.
- Resilience—CEF offers an unprecedented level of switching consistency and stability in large dynamic networks. In dynamic networks, fast-switched cache entries are frequently invalidated due to routing changes. These changes can cause traffic to be process switched using the routing table, rather than fast switched using the route cache. Because the Forwarding Information Base (FIB) lookup table contains all known routes that exist in the routing table, it eliminates route cache maintenance and the fast-switch or process-switch forwarding scenario. CEF can switch traffic more efficiently than typical demand caching schemes.

CEF Components

Cisco IOS XR softwareCEF always operates in CEF mode with two distinct components: a Forwarding Information Base (FIB) database and adjacency table—a protocol-independent adjacency information base (AIB).

CEF is a primary IP packet-forwarding database for Cisco IOS XR software. CEF is responsible for the following functions:

- Software switching path
- Maintaining forwarding table and adjacency tables (which are maintained by the AIB) for software and hardware forwarding engines

The following CEF forwarding tables are maintained in Cisco IOS XR software:

- IPv4 CEF database
- IPv6 CEF database
- MPLS LFD database
- Multicast Forwarding Table (MFD)

The protocol-dependent FIB process maintains the forwarding tables for IPv4 and IPv6 unicast in the Route Switch Processor (RSP) and each MSC.

The FIB on each node processes Routing Information Base (RIB) updates, performing route resolution and maintaining FIB tables independently in the RSP and each MSC. FIB tables on each node can be slightly different. Adjacency FIB entries are maintained only on a local node, and adjacency entries linked to FIB entries could be different.

Border Gateway Protocol Policy Accounting

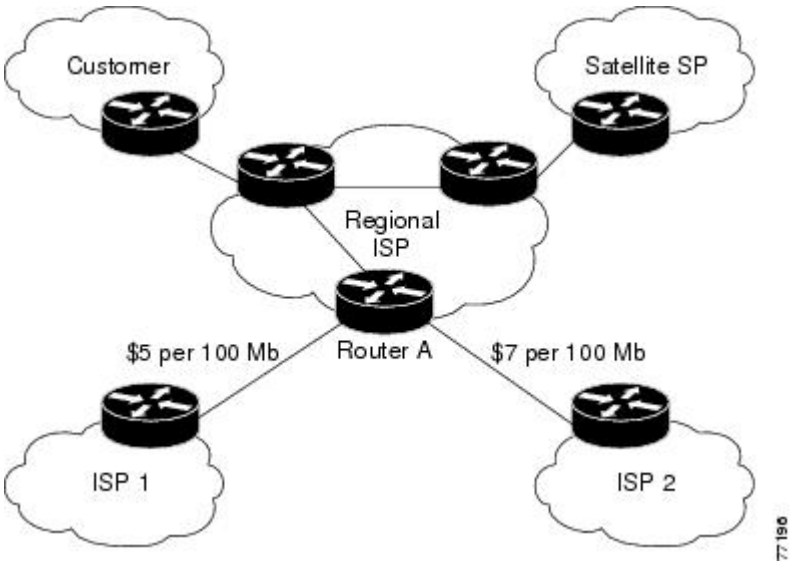
Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an individual input or output interface basis, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

Note There are two types of route policies. The first type (regular BGP route policies) is used to filter the BGP routes advertised into or out from the BGP links. This type of route policy is applied to the specific BGP neighbor. The second type (specific route policy) is used to set up a traffic index for the BGP prefixes. This route policy is applied to the global BGP IPv4 address family to set up the traffic index when the BGP routes are inserted into the RIB table. BGP policy accounting uses the second type of route policy.

Using BGP policy accounting, you can account for traffic according to the route it traverses. Service providers can identify and account for all traffic by customer and bill accordingly. In Figure 16: Sample Topology for BGP Policy Accounting, on page 262, BGP policy accounting can be implemented in Router A to measure packet and byte volumes in autonomous system buckets. Customers are billed appropriately for traffic that is routed from a domestic, international, or satellite source.

Note BGP policy accounting measures and classifies IP traffic for BGP prefixes only.

Figure 16: Sample Topology for BGP Policy Accounting



Based on the specified routing policy, BGP policy accounting assigns each prefix a traffic index (bucket) associated with an interface. BGP prefixes are downloaded from the RIB to the FIB along with the traffic index.

There are a total of 63 (1 to 63) traffic indexes (bucket numbers) that can be assigned for BGP prefixes. Internally, there is an accounting table associated with the traffic indexes to be created for each input (ingress) and output (egress) interface. The traffic indexes allow you to account for the IP traffic, where the source IP address, the destination IP address, or both are BGP prefixes.

Note Traffic index 0 contains the packet count using Interior Gateway Protocol (IGP) routes.

Reverse Path Forwarding (Strict and Loose)

Unicast IPv4 and IPv6 Reverse Path Forwarding (uRPF), both strict and loose modes, help mitigate problems caused by the introduction of malformed or spoofed IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. Unicast RPF does this by doing a reverse lookup in the CEF table. Therefore, Unicast Reverse Path Forwarding is possible only if CEF is enabled on the router.

IPv6 uRPF is supported with ASR 9000-SIP-700 LC, ASR 9000 Ethernet LC and ASR 9000 Enhanced Ethernet LC.

Note Unicast RPF allows packets with 0.0.0.0 source addresses and 255.255.255.255 destination addresses to pass so that Bootstrap Protocol and Dynamic Host Configuration Protocol (DHCP) will function properly.

Note In Unicast RPF, the loose mode allows IGMPv3 reports with 0.0.0.0 source addresses, whereas the strict mode does not.

When strict uRPF is enabled, the source address of the packet is checked in the FIB. If the packet is received on the same interface that would be used to forward the traffic to the source of the packet, the packet passes the check and is further processed; otherwise, it is dropped. Strict uRPF should only be applied where there is natural or configured symmetry. Because internal interfaces are likely to have routing asymmetry, that is, multiple routes to the source of a packet, strict uRPF should not be implemented on interfaces that are internal to the network.

Note The behavior of strict RPF varies slightly by platform, number of recursion levels, and number of paths in Equal-Cost Multipath (ECMP) scenarios. A platform may switch to loose RPF check for some or all prefixes, even though strict RPF is configured.

When loose uRPF is enabled, the source address of the packet is checked in the FIB. If it exists and matches a valid forwarding entry, the packet passes the check and is further processed; otherwise, it is dropped.

Strict mode uRPF requires maintenance of uRPF interfaces list for the prefixes. The list contains only strict mode uRPF configured interfaces pointed by the prefix path. uRPF interface list is shared among the prefixes wherever possible. Size of this list is 12 for ASR 9000 Ethernet Line Cards and 64 for integrated 20G SIP cards. Strict to loose mode uRPF fallback happens when the list goes beyond the maximum supported value.

Loose and strict uRPF supports two options: **allow self-ping** and **allow default**. The **self-ping** option allows the source of the packet to ping itself. The **allow default** option allows the lookup result to match a default routing entry. When the **allow default** option is enabled with the strict mode of the uRPF, the packet is processed further only if it arrived through the default interface.

Per-Flow Load Balancing

Load balancing describes the functionality in a router that distributes packets across multiple links based on Layer 3 (network layer) and Layer 4 (transport layer) routing information. If the router discovers multiple paths to a destination, the routing table is updated with multiple entries for that destination.

Per-flow load balancing performs these functions:

- Incoming data traffic is evenly distributed over multiple equal-cost connections within a bundle interface.
- Layer 2 bundle and Layer 3 (network layer) load balancing decisions are taken on IPv4, IPv6, and MPLS flows which are supported for the 5-tuple hash algorithm.
- A 5-tuple hash algorithm provides more granular load balancing than the 3-tuple hash algorithm.
- The same hash algorithm (3-tuple or 5-tuple) is used for load balancing over multiple equal-cost Layer 3 (network layer) paths. The Layer 3 (network layer) path is on a physical interface or on a bundle interface. In addition, load balancing over member links can occur within a Layer 2 bundle interface.
- The **cef load-balancing fields L3 global** command allows you to select the 3-tuple hash algorithm.
- By default, 5-tuple hash algorithm is used for load balancing. If you use the **cef load-balancing fields L3 global** command, 3-tuple hash algorithm is enabled.

Layer 3 (Network Layer) Routing Information

The 3-tuple load-balance hash calculation contains these Layer 3 (Network Layer) inputs:

- Source IP address
- Destination IP address
- Router ID

Layer 4 (Transport Layer) Routing Information

The 5-tuple load-balance hash calculation contains 3-tuple inputs and these additional following Layer 4 (Transport Layer) inputs:

- Source port
- Destination port

Note In load-balancing scenarios, a line card may not use all output paths downloaded from routing protocols. This behavior varies with platform, number of recursion levels, and the fact whether MPLS is involved, or not.

Note CEF load balancing for GTP is always enabled by default on ASR9K platforms with Lightspeed line card and cannot be disabled. Therefore, the **no cef loadbalancing fields l4 gtp** command does not disable the inclusion of GTP fields in hash calculation in BE/LAG port.

Limitations for 3-Tuple Load Balance Hash Algorithm

- Load balancing is not symmetrical if the load balanced paths involve different speeds such as, 10 Gigabit Ethernet, 40 Gigabit Ethernet, or 100 Gigabit Ethernet ports.
- Because the 3-tuple hash algorithm excludes Layer 4 information and becomes dependent on Layer 3 information, load balancing is not symmetrical if the distribution of source and destination IP addresses is not varied enough, even if all ports operate at the same speed.
- You can configure 3-tuple hash algorithm only on Cisco ASR 9000 Enhanced Ethernet Line Cards.

IPv6 Flow Label Field for Hashing

You can use the 20-bit Flow Label field in the IPv6 header as an additional input field for hash algorithms to improve load balancing decisions. Use the **cef load-balancing fields ipv6 flow-label** command to enable the flow label field for IPv6 packets on Cisco ASR 9000 High Density 100GE Ethernet Line Cards and Cisco ASR 9000 Enhanced Ethernet Line Cards. The hash algorithms can use the flow label field in addition to inputs such as source IP address, destination IP address, router ID, source port, and destination port. See RFC 6437 for details about the IPv6 Flow Label Specification.

BGP Attributes Download

The BGP Attributes Download feature enables you to display the installed BGP attributes in CEF. Configure the **show cef bgp-attribute** command to display the installed BGP attributes in CEF. You can use the **show cef bgp-attribute attribute-id** command and the **show cef bgp-attribute local-attribute-id** command to look at specific BGP attributes by attribute ID and local attribute ID.

Verification

```
Router# show cef bgp-attribute
Wed Aug 21 14:05:51.772 UTC

VRF: default

_____________
Table ID: 0xe0000000. Total number of entries: 1
OOR state: GREEN. Number of OOR attributes: 0

BGP Attribute ID: 0x6, Local Attribute ID: 0x1
    Aspath      :    2
    Community   :
    Origin AS   :    2
    Next Hop AS :    2
```

How to Implement CEF

This section contains instructions for the following tasks:

Verifying CEF

This task allows you to verify CEF.

SUMMARY STEPS

1. **show cef** {**ipv4** | **ipv6**}
2. **show cef** {**ipv4** | **ipv6**} **summary**
3. **show cef** {**ipv4** | **ipv6**} **detail**
4. show adjacency detail

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show cef** {**ipv4** | **ipv6**} **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4`	Displays the IPv4 or IPv6 CEF table. The next hop and forwarding interface are displayed for each prefix. **Note** The output of the **show cef** command varies by location.

	Command or Action	Purpose
Step 2	**show cef** {**ipv4** | **ipv6**} **summary** **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4 summary`	Displays a summary of the IPv4 or IPv6 CEF table.
Step 3	**show cef** {**ipv4** | **ipv6**} **detail** **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4 detail`	Displays detailed IPv4 or IPv6 CEF table information.
Step 4	show adjacency detail **Example:** `RP/0/RSP0/CPU0:router# show adjacency detail`	Displays detailed adjacency information, including Layer 2 information for each interface. **Note** The output of the **show adjacency** command varies by location.

Configuring BGP Policy Accounting

This task allows you to configure BGP policy accounting.

Note There are two types of route policies. BGP policy accounting uses the type that is used to set up a traffic index for the BGP prefixes. The route policy is applied to the global BGP IPv4 address family to set up the traffic index when the BGP routes are inserted into the RIB table.

BGP policy accounting enables per interface accounting for ingress and egress IP traffic based on the traffic index assigned to the source IP address (BGP prefix) and destination IP address (BGP prefix). The traffic index of BGP prefixes can be assigned according to the following parameters using Routing Policy Language (RPL):

- prefix-set
- AS-path-set
- community-set

Note BGP policy accounting is supported on IPv4 prefixes only.

Two configuration tasks provide the ability to classify BGP prefixes that are in the RIB according to the prefix-set, AS-path-set, or the community-set parameters:

1. Use the **route-policy** command to define the policy for traffic index setup based on the prefix-set, AS-path-set, or community-set.
2. Use the BGP **table-policy** command to apply the defined route policy to the global BGP IPv4 unicast address family.

See the *Routing Command Reference for Cisco ASR 9000 Series Routers* for information on the **route-policy** and **table-policy** commands.

BGP policy accounting can be enabled on each interface with the following options:

- Use the ipv4 bgp policy accounting command with one of the following keyword options:
  - input source-accounting
  - input destination-accounting
  - input source-accounting destination-accounting
- Use the ipv4 bgp policy accounting command with one of the following keyword options:
  - output source-accounting
  - output destination-accounting
  - output source-accounting destination-accounting
- Use any combination of the keywords provided for the **ipv4 bgp policy accounting** command.

Before you begin

Before using the BGP policy accounting feature, you must enable BGP on the router (CEF is enabled by default). See the *Routing Configuration Guide for Cisco ASR 9000 Series Routers* for information on enabling BGP.

SUMMARY STEPS

1. configure
2. as-path-set
3. exit
4. **prefix-set** *name*
5. exit
6. **route-policy** *policy-name*
7. end
8. configure
9. **router bgp** *autonomous-system-number*
10. **address-family ipv4** {**unicast** | **multicast** }
11. **table policy** *policy-name*
12. end
13. configure
14. **interface** *type interface-path-id*
15. **ipv4 bgp policy accounting** {**input** | **output** {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}}
16. Do one of the following:
    - end
    - commit

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.

Step 2	as-path-set
	Example:
	`RP/0/RSP0/CPU0:router(config)# as-path-set as107`
	`RP/0/RSP0/CPU0:router(config-as)# ios-regex '107$'`
	`RP/0/RSP0/CPU0:router(config-as)# end-set`
	`RP/0/RSP0/CPU0:router(config)# as-path-set as108`
	`RP/0/RSP0/CPU0:router(config-as)# ios-regex '108$'`
	`RP/0/RSP0/CPU0:router(config-as)# end-set`
		Enters policy configuration mode.

Step 3	exit **Example:** `RP/0/RSP0/CPU0:router(config-as)# exit`	Returns to global configuration mode.
Step 4	**prefix-set** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# prefix-set RT-65`	Defines the prefix list.
Step 5	exit **Example:** `RP/0/RSP0/CPU0:router(config-pfx)# exit`	Returns to global configuration mode.
Step 6	**route-policy** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config)# route-policy rp501b`	Specifies the route-policy name.
Step 7	end **Example:** `RP/0/RSP0/CPU0:router(config-rpl)# end`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:` • Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

	Command or Action	Purpose
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
Step 8	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 9	**router bgp** *autonomous-system-number* **Example:** `RP/0/RSP0/CPU0:router(config)# router bgp 1`	Allows you to configure the BGP routing process.
Step 10	**address-family ipv4** {**unicast** | **multicast** } **Example:** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast`	Allows you to enter the address family configuration mode while configuring a BGP routing session.
Step 11	**table policy** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-bgp-af)# table-policy set-traffic-index`	Applies a routing policy to routes being installed into the routing table.
Step 12	end **Example:** `RP/0/RSP0/CPU0:router(config-bgp-af)# end`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:` • Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. • Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

	Command or Action	Purpose
Step 13	configure **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 14	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/0/2`	Enters interface configuration mode.
Step 15	**ipv4 bgp policy accounting** {**input** | **output** {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}} **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 bgp policy accounting output destination-accounting`	Enables BGP policy accounting.

Step 16	Do one of the following:
	• end
	• commit
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# end`
	or
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Verifying BGP Policy Accounting

This task allows you to verify BGP policy accounting.

Note BGP policy accounting is supported on IPv4 prefixes.

Before you begin

BGP policy accounting must be configured. See the Configuring BGP Policy Accounting, on page 266.

SUMMARY STEPS

1. **show route bgp**
2. **show bgp summary**
3. **show bgp** *ip-address*
4. **show route ipv4** *ip-address*
5. **show cef ipv4** *prefix*
6. **show cef ipv4** *prefix* **detail**
7. **show cef ipv4 interface** *type interface-path-id* **bgp-policy-statistics**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show route bgp** **Example:** `RP/0/RSP0/CPU0:router# show route bgp`	Displays all BGP routes with traffic indexes.
Step 2	**show bgp summary** **Example:** `RP/0/RSP0/CPU0:router# show bgp summary`	Displays the status of all BGP neighbors.
Step 3	**show bgp** *ip-address* **Example:** `RP/0/RSP0/CPU0:router# show bgp 40.1.1.1`	Displays BGP prefixes with BGP attributes.
Step 4	**show route ipv4** *ip-address* **Example:** `RP/0/RSP0/CPU0:router# show route ipv4 40.1.1.1`	Displays the specific BGP route with the traffic index in the RIB.
Step 5	**show cef ipv4** *prefix* **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4 40.1.1.1`	Displays the specific BGP prefix with the traffic index in the RP FIB.

	Command or Action	Purpose
Step 6	**show cef ipv4** *prefix* **detail** **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4 40.1.1.1 detail`	Displays the specific BGP prefix with detailed information in the RP FIB.
Step 7	**show cef ipv4 interface** *type interface-path-id* **bgp-policy-statistics** **Example:** `RP/0/RSP0/CPU0:router# show cef ipv4 interface TenGigE 0/2/0/4 bgp-policy-statistics`	Displays the BGP Policy Accounting statistics for the specific interface.

Configuring a Route Purge Delay

This task allows you to configure a route purge delay. A purge delay purges routes when the RIB or other related process experiences a failure.

SUMMARY STEPS

1. **configure**
2. **cef purge-delay** *seconds*
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**cef purge-delay** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config)# cef purge-delay 180`	Configures a delay in purging routes when the Routing Information Base (RIB) or other related processes experience a failure.
Step 3	**commit**	

Configuring Unicast RPF Checking

This task allows you to configure unicast Reverse Path Forwarding (uRPF) checking. Unicast RPF checking allows you to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. {**ipv4** | **ipv6**} **verify unicast source reachable-via** {**any** | **rx**} [**allow-default**] [**allow-self-ping**]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/0`	Enters interface configuration mode.
Step 3	{**ipv4** | **ipv6**} **verify unicast source reachable-via** {**any** | **rx**} [**allow-default**] [**allow-self-ping**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 verify unicast source reachable-via rx`	Enables IPv4 or IPv6 uRPF checking. • The **rx** keyword enables strict unicast RPF checking. If strict unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table and the output interface matches the interface on which the packet was received. • The **allow-default** keyword enables the matching of default routes. This option applies to both loose and strict RPF. • The **allow-self-ping** keyword enables the router to ping out an interface. This option applies to both loose and strict RPF. **Note** IPv6 uRPF checking is not supported on ASR 9000 Ethernet line cards.
Step 4	**commit**	

Configuring Modular Services Card-to-Route Processor Management Ethernet Interface Switching

This task allows you to enable MSC-to-RP management Ethernet interface switching.

SUMMARY STEPS

1. **configure**
2. **rp mgmtethernet forwarding**

3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rp mgmtethernet forwarding** **Example:** `RP/0/RSP0/CPU0:router(config)# rp mgmtethernet forwarding`	Enables switching from the MSC to the route processor Management Ethernet interfaces.
Step 3	**commit**	

Configuring Per-Flow Load Balancing

This section describes the following tasks to configure per-flow load balancing:

Configuring 3-Tuple Hash Algorithm

This task allows you to configure per-flow load balancing for a 3-tuple hash algorithm.

SUMMARY STEPS

1. **configure**
2. **cef load-balancing fields L3 global**
3. **commit**
4. **show running-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**cef load-balancing fields L3 global** **Example:** `RP/0/RSP0/CPU0:router(config)# cef load-balancing fields L3 global`	Configures the 3-tuple hashing algorithm for load balancing during forwarding. The **cef load-balancing fields l3 global** command configures the hash tuple with the following fields: • Source IP address. Destination IP address. • Router ID.

	Command or Action	Purpose
		The following Layer 4 fields are ignored: • Source port. Destination port. The **cef load-balancing fields l3 global** command is supported only on Cisco ASR 9000 Enhanced Ethernet Line Cards. This command is ignored on the other line cards.
Step 3	**commit**	
Step 4	**show running-config** **Example:** `RP/0/RSP0/CPU0:router# show running config`	Displays the running configuration which contains the load balancing information.

Configuring BGP Attributes Download

This task allows you to configure the BGP Attributes Download feature.

Configuring BGP Attributes Download

SUMMARY STEPS

1. **configure**
2. **cef bgp attribute** {*attribute-id* | *local-attribute-id* }
3. **commit**

DETAILED STEPS

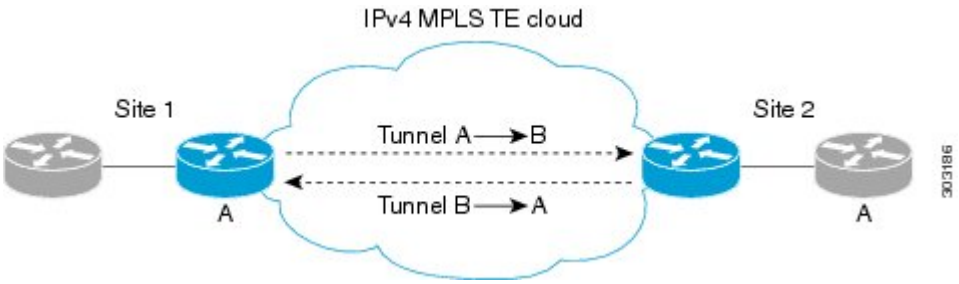
Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**cef bgp attribute** {*attribute-id*	*local-attribute-id* } **Example:** `RP/0/RSP0/CPU0:router(config)# cef bgp attribute 508`	Configures a CEF BGP attribute.
Step 3	**commit**	

IPv6 Routing over IPv4 MPLS TE Tunnels

IPv6 routing over IPv4 Multiprotocol Label Switching with Traffic Engineering (MPLS TE) tunnels in the core is achieved by configuring the TE tunnels into the IPv6 Interior Gateway Protocol (IGP) topology as IPv6 forwarding adjacencies.

Figure 17: IPv6 Routing over IPv4 MPLS TE



This figure shows two IPv4/IPv6-aware sites connected over a TE core, where TE is not IPv6-aware. Two tunnels are set up across the core, and are announced as forwarding adjacencies into the IPv6 topologies at Site 1 and Site 2. Routers at Site 1 and Site 2 can use these tunnels to compute the best IPv6 route to the other site within their IS-IS SPF.

Restrictions for Implementing IPv6 routing over IPv4 MPLS TE tunnels

The following restrictions apply to implementing IPv6 routing over IPv4 MPLS TE tunnels:

- It is supported for IS-IS only.
- IS-ISv4 and v6 must exist in a single topology.
- IS-ISv4 and v6 must be configured under the same IS-IS instance at the endpoints.

Configuring tunnel as IPV6 Forwarding-Adjacency

Perform this task to configure a tunnel as an IPv6 forwarding adjacency.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *n* **forwarding-adjacency include-ipv6**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**interface tunnel-te** *n* **forwarding-adjacency include-ipv6** **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1 forwarding-adjacency include-ipv6`	Configures tunnel as an IPV6 Forwarding-Adjacency.
Step 3	**commit**	

Configuring tunnel as IPV6 interface

Perform this task to configure a tunnel as an IPV6 interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *n* **ipv6 enable**
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *n* **ipv6 enable** **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1 ipv6 enable`	Configures tunnel as an IPV6 interface.
Step 3	**commit**	

Configuration Examples for Implementing CEF on Routers Software

This section provides the following configuration examples:

Configuring BGP Policy Accounting: Example

The following example shows how to configure BGP policy accounting.

Configure loopback interfaces for BGP router-id:

```
interface Loopback1
ipv4 address 10
.1.1.1 255.255.255.255
```

Configure interfaces with the BGP policy accounting options:

```
interface TenGigE0/2/0/2
 mtu 1514
 ipv4 address 10
.1.0.1 255.255.255.0
 proxy-arp
 ipv4 directed-broadcast
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
!
interface TenGigE0/2/0/2.1
 ipv4 address 10
.1.1.1 255.255.255.0
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
 encapsulation dot1q 1
!
interface TenGigE0/2/0/4
 mtu 1514
 ipv4 address 10
.1.0.1 255.255.255.0
 proxy-arp
 ipv4 directed-broadcast
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
!
interface TenGigE0/2/0/4.1
 ipv4 address 10
.1.2
.1 255.255.255.0
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
 encapsulation dot1q 1
!
interface GigabitEthernet 0/0/0/4
 mtu 4474
 ipv4 address 10
.1.0.40
255.255.0.0
 ipv4 directed-broadcast
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
 encapsulation ppp
 GigabitEthernet
  crc 32
 !
 keepalive disable
!
interface GigabitEthernet 0/0/0/8
 mtu 4474
 ipv4 address 18
.8
.0.1 255.255.0.0
 ipv4 directed-broadcast
 ipv4 bgp policy accounting input source-accounting destination-accounting
 ipv4 bgp policy accounting output source-accounting destination-accounting
```

```
 GigabitEthernet
  crc 32
 !
 keepalive disable
!
```

Configure controller:

```
controller GigabitEthernet 0/0/0/4
 ais-shut
 path
  ais-shut
 !
 threshold sf-ber 5
!
controller SONET0/0/0/8
 ais-shut
 path
  ais-shut
 !
 threshold sf-ber 5
!
```

Configure AS-path-set and prefix-set:

```
as-path-set as107
  ios-regex '107$'
end-set

as-path-set as108
  ios-regex '108$'
end-set

prefix-set RT-65.0
  65.0.0.0/16 ge 16 le 32
end-set

prefix-set RT-66.0
  66.0.0.0/16 ge 16 le 32
end-set
```

Configure the route-policy (table-policy) to set up the traffic indexes based on each prefix, AS-path-set, and prefix-set:

```
route-policy bpa1

  if destination in  (10
.1.1.0/24) then
    set traffic-index 1
  elseif destination in  (10
.1.2.0/24) then
    set traffic-index 2
  elseif destination in  (10
.1.3.0/24) then
    set traffic-index 3
  elseif destination in  (10
.1.4.0/24) then
    set traffic-index 4
  elseif destination in  (10
.1.5.0/24) then
    set traffic-index 5
  endif
```

```
  if destination in  (10
.1.1.0/24) then
    set traffic-index 6
  elseif destination in  (10
.1.2.0/24) then
    set traffic-index 7
  elseif destination in  (10
.1.3.0/24) then
    set traffic-index 8
  elseif destination in  (10
.1.4.0/24) then
    set traffic-index 9
  elseif destination in  (10
.1.5.0/24) then
    set traffic-index 10
  endif

  if as-path in as107 then
       set traffic-index 7
  elseif as-path in as108 then
       set traffic-index 8
  endif

  if destination in RT-65.0 then
     set traffic-index 15
  elseif destination in RT-66.0 then
     set traffic-index 16
  endif

end-policy
```

Configure the regular BGP route-policy to pass or drop all the BGP routes:

```
route-policy drop-all
  drop
end-policy
!
route-policy pass-all
  pass
end-policy
!
```

Configure the BGP router and apply the table-policy to the global ipv4 address family:

```
router bgp 100
 bgp router-id Loopback1
 bgp graceful-restart
 bgp as-path-loopcheck
 address-family ipv4 unicast
  table-policy bpa1
  maximum-paths 8
  bgp dampening
 !
```

Configure the BGP neighbor-group:

```
neighbor-group ebgp-peer-using-int-addr
  address-family ipv4 unicast
   policy pass-all in
   policy drop-all out
  !
 !
 neighbor-group ebgp-peer-using-int-addr-121
```

```
  remote-as 121
  address-family ipv4 unicast
   policy pass-all in
   policy drop-all out
  !
 !
 neighbor-group ebgp-peer-using-int-addr-pass-out
  address-family ipv4 unicast
   policy pass-all in
   policy pass-all out
  !
 !
```

Configure BGP neighbors:

```
neighbor 10
.4
.0.2
  remote-as 107
  use neighbor-group ebgp-peer-using-int-addr
 !
 neighbor 10
.8
.0.2
  remote-as 108
  use neighbor-group ebgp-peer-using-int-addr
 !
 neighbor 10
.7
.0.2
  use neighbor-group ebgp-peer-using-int-addr-121
 !
 neighbor 10
.1.7
.2
  use neighbor-group ebgp-peer-using-int-addr-121
 !
neighbor 10
.18
.0.2
  remote-as 122
  use neighbor-group ebgp-peer-using-int-addr
 !
 neighbor 10
.18
.1.2
  remote-as 1221
  use neighbor-group ebgp-peer-using-int-addr
 !
end
```

Verifying BGP Policy Statistics: Example

The following example shows how to verify the traffic index setup for each BGP prefix and BGP Policy Accounting statistics on ingress and egress interfaces. The following traffic stream is configured for this example:

- Traffic comes in from GigabitEthernet 0/2/0/4 and goes out to 5 VLAN subinterfaces under GigabitEthernet 0/2/0/2
- Traffic comes in from GigabitEthernet 0/0/08 and goes out to GigabitEthernet 0/0/0/4

```
show cef ipv4 interface GigabitEthernet 0/0/0/8 bgp-policy-statistics

GigabitEthernet0/0/0/8 is up
Input BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  7            5001160   500116000
  15          10002320  1000232000
Input BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  8            5001160   500116000
  16          10002320  1000232000
Output BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  0                 15         790
Output BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  0                 15         790

show cef ipv4 interface GigabitEthernet 0/0/0/4 bgp-policy-statistics

GigabitEthernet0/0/0/4 is up
Input BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
Input BGP policy accounting on src IP address enabled
  buckets      packets       bytes
Output BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  0                 13         653
  7            5001160   500116000
  15          10002320  1000232000
Output BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  0                 13         653
  8            5001160   500116000
  16          10002320  1000232000

show cef ipv4 interface GigabitEthernet 0/2/0/4 bgp-policy-statistics

GigabitEthernet0/2/0/4 is up
Input BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  1            3297102   329710200
  2            3297102   329710200
  3            3297102   329710200
  4            3297101   329710100
  5            3297101   329710100
Input BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  6            3297102   329710200
  7            3297102   329710200
  8            3297102   329710200
  9            3297101   329710100
  10           3297101   329710100
Output BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  0                 15         733
Output BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  0                 15         733

show cef ipv4 interface GigabitEthernet 0/2/0/2.1 bgp-policy-statistics

GigabitEthernet 0/2/0/2.1 is up
```

```
Input BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
Input BGP policy accounting on src IP address enabled
  buckets      packets       bytes
Output BGP policy accounting on dst IP address enabled
  buckets      packets       bytes
  0                 15         752
  1            3297102   329710200
  2            3297102   329710200
  3            3297102   329710200
  4            3297101   329710100
  5            3297101   329710100
Output BGP policy accounting on src IP address enabled
  buckets      packets       bytes
  0                 15         752
  6            3297102   329710200
  7            3297102   329710200
  8            3297102   329710200
  9            3297101   329710100
  10           3297101   329710100
```

The following example show how to verify BGP routes and traffic indexes:

```
show route bgp

B     10
.1.1.0/24 [20/0] via 10
.17
.1.2, 00:07:09
      Traffic Index 1
B     10
.1.2.0/24 [20/0] via 10
.17
.1.2, 00:07:09
      Traffic Index 2
B    10
.1.3.0/24 [20/0] via 10
.17
.1.2, 00:07:09
      Traffic Index 3
B    10
.1.4.0/24 [20/0] via 10
.17
.1.2, 00:07:09
      Traffic Index 4
B    10
.1.5.0/24 [20/0] via 10
.17
.1.2, 00:07:09
      Traffic Index 5
B    10
.18
.1.0/24 [20/0] via 10
.18
.1.2, 00:07:09
      Traffic Index 6
B    10
.18
.2.0/24 [20/0] via 10
.18
.1.2, 00:07:09
      Traffic Index 7
B    10
.18
```

```
.3.0/24 [20/0] via 10
.18
.1.2, 00:07:09
      Traffic Index 8
B    10
.28
.4.0/24 [20/0] via 10
.18
.1.2, 00:07:09
      Traffic Index 9
B    10
.28
.5.0/24 [20/0] via 10
.18
.1.2, 00:07:09
      Traffic Index 10
B    10
.65
.1.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.2.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.3.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.65
.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.5.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.6.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.7.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.8.0/24 [20/0] via 10
.45
.0.2, 00:07:09
```

```
      Traffic Index 15
B    10
.65
.9.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.65
.10.0/24 [20/0] via 10
.45
.0.2, 00:07:09
      Traffic Index 15
B    10
.66
.1.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.2.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.3.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.4.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.5.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.6.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.7.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.8.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.9.0/24 [20/0] via 10
```

```
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.66
.10.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 16
B    10
.67
.1.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.2.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.3.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.4.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.5.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.6.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.7.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.8.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.67
.9.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
```

```
.67
.10.0/24 [20/0] via 10
.32
.0.2, 00:07:09
      Traffic Index 7
B    10
.68
.1.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.2.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.3.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.4.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.5.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.6.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.7.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.8.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.9.0/24 [20/0] via 10
.8
.0.2, 00:07:09
      Traffic Index 8
B    10
.68
.10.0/24 [20/0] via 10
.8
.0.2, 00:07:09
```

```
      Traffic Index 8

show bgp summary

BGP router identifier 192
.0
.2
.0
, local AS number 100
BGP generic scan interval 60 secs
BGP main routing table version 151
Dampening enabled
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.

Process         RecvTblVer    bRIB/RIB  SendTblVer
Speaker               151         151         151

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  St/PfxRcd
10
.4
.0.2                 0     107      54      53      151    0    0 00:25:26       20
10
.1.0.2                  0   108      54      53      151    0    0 00:25:28       20
10
.1.0.2          0   121      53      54      151    0    0 00:25:42        0
10
.1.1.2          0   121      53      53      151    0    0 00:25:06        5
10
.1.2.2          0   121      52      54      151    0    0 00:25:04        0
10
.1.3.2          0   121      52      53      151    0    0 00:25:26        0
10
.1.4.2          0   121      53      54      151    0    0 00:25:41        0
10
.1.5.2          0   121      53      54      151    0    0 00:25:43        0
10
.1.6.2          0   121      51      53      151    0    0 00:24:59        0
10
.1.7.2          0   121      51      52      151    0    0 00:24:44        0
10
.1.8.2          0   121      51      52      151    0    0 00:24:49        0
10
.2
.0.2          0   122      52      54      151    0    0 00:25:21        0
10
.2
.1.2          0  1221      54      54      151    0    0 00:25:43        5
10
.2
.2.2          0  1222      53      54      151    0    0 00:25:38        0
10
.2
.3.2          0  1223      52      53      151    0    0 00:25:17        0
10
.2
.4.2          0  1224      51      52      151    0    0 00:24:57        0
10
.2
.5.2          0  1225      52      53      151    0    0 00:25:14        0
10
.2
.6.2          0  1226      52      54      151    0    0 00:25:04        0
10
```

```
.2
.7.2          0  1227      52      54      151    0    0 00:25:13        0
10
.2
.8.2          0  1228      53      54      151    0    0 00:25:36        0

show bgp 27.1.1.1

BGP routing table entry for 27.1.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               102         102
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  121
    10
.1.1.2 from 10
.1.1.2 (10
.1.1.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 27:1 121:1

show bgp 10
.1.1.1

BGP routing table entry for 10
.1.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               107         107
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  1221
      10
.2
.1.2 from 10
.2
.1.2 (18.1.1.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 28:1 1221:1

show bgp 10
.0.1.1

BGP routing table entry for 10
.0.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               112         112
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  107
    10
.1.0.2 from 10
.1.0.2 (10
.1.0.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 107:65

show bgp 10
.2
```

```
.1.1

BGP routing table entry for 10
.2
.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                122         122
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  108
    8.1.0.2 from 8.1.0.2 (8.1.0.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 108:66

show bgp 67.0.1.1

BGP routing table entry for 67.0.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                132         132
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  107
    4.1.0.2 from 4.1.0.2 (4.1.0.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 107:67

show bgp 68.0.1.1

BGP routing table entry for 68.0.1.0/24
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                142         142
Paths: (1 available, best #1)
  Not advertised to any peer
  Received by speaker 0
  108
    8.1.0.2 from 8.1.0.2 (8.1.0.2)
      Origin incomplete, localpref 100, valid, external, best
      Community: 108:68

show route ipv4 27.1.1.1

Routing entry for 27.1.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 121, type external, Traffic Index 1
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    17.1.1.2, from 17.1.1.2
      Route metric is 0
  No advertising protos.

show route ipv4 28.1.1.1

Routing entry for 28.1.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 1221, type external, Traffic Index 6
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    18.1.1.2, from 18.1.1.2
      Route metric is 0
```

```
  No advertising protos.

show route ipv4 65.0.1.1

Routing entry for 65.0.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 107, type external, Traffic Index 15
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    4.1.0.2, from 4.1.0.2
      Route metric is 0
  No advertising protos.

show route ipv4 66.0.1.1

Routing entry for 66.0.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 108, type external, Traffic Index 16
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    8.1.0.2, from 8.1.0.2
      Route metric is 0
  No advertising protos.

show route ipv4 67.0.1.1

Routing entry for 67.0.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 107, type external, Traffic Index 7
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    4.1.0.2, from 4.1.0.2
      Route metric is 0
  No advertising protos.

show route ipv4 68.0.1.1

Routing entry for 68.0.1.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 108, type external, Traffic Index 8
  Installed Nov 11 21:14:05.462
  Routing Descriptor Blocks
    8.1.0.2, from 8.1.0.2
      Route metric is 0
  No advertising protos.

show cef ipv4 27.1.1.1

27.1.1.0/24, version 263, source-destination sharing
Prefix Len 24, Traffic Index 1, precedence routine (0)
  via 17.1.1.2, 0 dependencies, recursive
    next hop 17.1.1.2/24, GigabitEthernet 0/2/0/2.1 via 17.1.1.0/24
    valid remote adjacency
  Recursive load sharing using 17.1.1.0/24

show cef ipv4 28.1.1.1

28.1.1.0/24, version 218, source-destination sharing
Prefix Len 24, Traffic Index 6, precedence routine (0)
  via 18.1.1.2, 0 dependencies, recursive
    next hop 18.1.1.2/24, GigabitEthernet0/2/0/4.1 via 18.1.1.0/24
    valid remote adjacency
  Recursive load sharing using 18.1.1.0/24
```

```
show cef ipv4 65.0.1.1

65.0.1.0/24, version 253, source-destination sharing
Prefix Len 24, Traffic Index 15, precedence routine (0)
  via 4.1.0.2, 0 dependencies, recursive
    next hop 4.1.0.2/16, GigabitEthernet0/0/0/4 via 4.1.0.0/16
    valid remote adjacency
  Recursive load sharing using 4.1.0.0/16

show cef ipv4 66.0.1.1

66.0.1.0/24, version 233, source-destination sharing
Prefix Len 24, Traffic Index 16, precedence routine (0)
  via 8.1.0.2, 0 dependencies, recursive
    next hop 8.1.0.2/16, GigabitEthernet 0/0/0/8 via 8.1.0.0/16
    valid remote adjacency
  Recursive load sharing using 8.1.0.0/16

show cef ipv4 67.0.1.1

67.0.1.0/24, version 243, source-destination sharing
Prefix Len 24, Traffic Index 7, precedence routine (0)
  via 4.1.0.2, 0 dependencies, recursive
    next hop 4.1.0.2/16, GigabitEthernet 0/0/0/4 via 4.1.0.0/16
    valid remote adjacency
  Recursive load sharing using 4.1.0.0/16

show cef ipv4 68.0.1.1

68.0.1.0/24, version 223, source-destination sharing
Prefix Len 24, Traffic Index 8, precedence routine (0)
  via 8.1.0.2, 0 dependencies, recursive
    next hop 8.1.0.2/16, GigabitEthernet0/0/0/8 via 8.1.0.0/16
    valid remote adjacency
  Recursive load sharing using 8.1.0.0/16

show cef ipv4 27.1.1.1 detail

27.1.1.0/24, version 263, source-destination sharing
Prefix Len 24, Traffic Index 1, precedence routine (0)
  via 17.1.1.2, 0 dependencies, recursive
    next hop 17.1.1.2/24, GigabitEthernet 0/2/0/2.1 via 17.1.1.0/24
    valid remote adjacency

  Recursive load sharing using 17.1.1.0/24
  Load distribution: 0 (refcount 6)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet 0/2/0/2.1          (remote)              0

show cef ipv4 28.1.1.1 detail

28.1.1.0/24, version 218, source-destination sharing
Prefix Len 24, Traffic Index 6, precedence routine (0)
  via 18.1.1.2, 0 dependencies, recursive
    next hop 18.1.1.2/24, GigabitEthernet 0/2/0/4.1 via 18.1.1.0/24
    valid remote adjacency

  Recursive load sharing using 18.1.1.0/24
  Load distribution: 0 (refcount 6)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet 0/2/0/4.1          (remote)              0
```

```
show cef ipv4 65.0.1.1 detail

65.0.1.0/24, version 253, source-destination sharing
Prefix Len 24, Traffic Index 15, precedence routine (0)
  via 4.1.0.2, 0 dependencies, recursive
    next hop 4.1.0.2/16, GigabitEthernet0/0/0/4 via 4.1.0.0/16
    valid remote adjacency

  Recursive load sharing using 4.1.0.0/16
  Load distribution: 0 (refcount 21)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet0/0/0/4               (remote)               0

show cef ipv4 66.0.1.1 detail

66.0.1.0/24, version 233, source-destination sharing
Prefix Len 24, Traffic Index 16, precedence routine (0)
  via 8.1.0.2, 0 dependencies, recursive
    next hop 8.1.0.2/16, GigabitEthernet0/0/0/8 via 8.1.0.0/16
    valid remote adjacency

  Recursive load sharing using 8.1.0.0/16
  Load distribution: 0 (refcount 21)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet 0/0/0/8               (remote)               0

show cef ipv4 67.0.1.1 detail

67.0.1.0/24, version 243, source-destination sharing
Prefix Len 24, Traffic Index 7, precedence routine (0)
  via 4.1.0.2, 0 dependencies, recursive
    next hop 4.1.0.2/16, GigabitEthernet 0/0/0/4 via 4.1.0.0/16
    valid remote adjacency

  Recursive load sharing using 4.1.0.0/16
  Load distribution: 0 (refcount 21)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet 0/0/0/4               (remote)               0

show cef ipv4 68.0.1.1 detail

68.0.1.0/24, version 223, source-destination sharing
Prefix Len 24, Traffic Index 8, precedence routine (0)
  via 8.1.0.2, 0 dependencies, recursive
    next hop 8.1.0.2/16, GigabitEthernet 0/0/0/8 via 8.1.0.0/16
    valid remote adjacency

  Recursive load sharing using 8.1.0.0/16
  Load distribution: 0 (refcount 21)

  Hash  OK  Interface                 Address  Packets
  1     Y   GigabitEthernet 0/0/0/8               (remote)               0
```

Configuring Unicast RPF Checking: Example

The following example shows how to configure unicast RPF checking:

```
configure
interface GigabitEthernet 0/0/0/1
```

```
ipv4 verify unicast source reachable-via rx
end
```

Configuring the Switching of Modular Services Card to Management Ethernet Interfaces on the Route Processor: Example

The following example shows how to configure the switching of the MSC to Management Ethernet interfaces on the route processor:

```
configure
rp mgmtethernet forwarding
end
```

Configuring Per-Flow Load Balancing: Example

The following examples show how to configure Layer 3 load-balancing for the hash algorithm from the **cef load-balancing fields L3 global** command, and how to verify summary information for the CEF table from the **show cef summary** command:

Configuring Layer 3 load-balancing

```
configure
 cef load-balancing fields L3 global
 end
 !
show cef summary
Router ID is 10.6.6.6

IP CEF with switching (Table Version 0) for node0_RSP0_CPU0

  Load balancing: L3
  Tableid 0xe0000000 (0x9cbb51b0), Vrfid 0x60000000, Vrid 0x20000000, Flags 0x2031
  Vrfname default, Refcount 577
  300 routes, 0 protected, 0 reresolve, 0 unresolved (0 old, 0 new), 21600 bytes
  212 load sharing elements, 62576 bytes, 324 references
  19 shared load sharing elements, 5388 bytes
  193 exclusive load sharing elements, 57188 bytes
  0 route delete cache elements
  622 local route bufs received, 1 remote route bufs received,  0 mix bufs received
  176 local routes, 0 remote routes
  4096 total local route updates processed
  0 total remote route updates processed
  0 pkts pre-routed to cust card
  0 pkts pre-routed to cust card
  0 pkts received from core card
  0 CEF route update drops, 96 revisions of existing leaves
  0 CEF route update drops due to version mis-match
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  82 prefixes with label imposition, 107 prefixes with label information
 95 next hops
  0 incomplete next hops

0 PD backwalks on LDIs with backup path
```

Configuring BGP Attributes Download: Example

The following example shows how to configure the BGP Attributes Download feature:

```
router configure
show cef bgp attribute {attribute-id| local-attribute-id}
```

Additional References

The following sections provide references related to implementing CEF.

Related Documents

Related Topic	Document Title
CEF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Express Forwarding Commands* module in *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
BGP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*BGP Commands* module in the *Routing Command Reference for Cisco ASR 9000 Series Routers*
Link Bundling Commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Link Bundling Commands* module in the *Interface and Hardware Component Command Reference for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

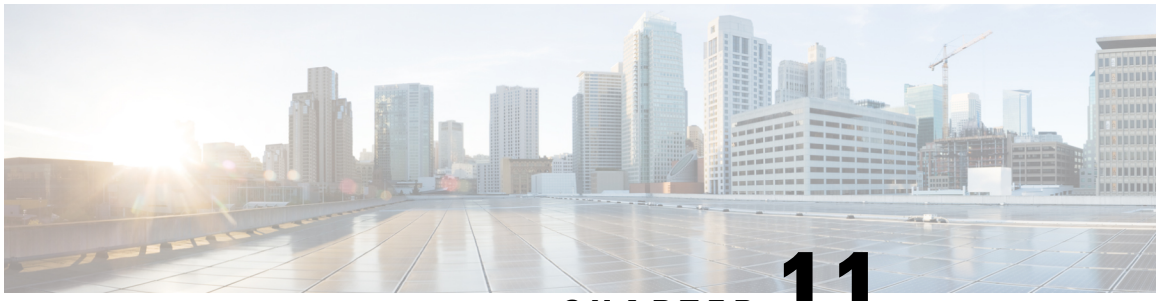
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 11

Implementing HSRP

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

Feature History for Implementing HSRP

Release 3.7.2	This feature was introduced.
Release 3.9.0	Support was added for the following features: • BFD for HSRP. • Hot restartability for HSRP.
Release 4.2.0	Multiple Group Optimization (MGO) for HSRP feature was added.
Release 4.2.1	Enhanced object tracking for HSRP and IP Static feature was added.

Note GLBP is not supported on ASR9k.

Prerequisites for Implementing HSRP

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for Implementing HSRP

HSRP is supported on Ethernet interfaces, Ethernet sub-interfaces, Ethernet link bundles, and Bridge Virtual Interfaces (BVIs).

Information About Implementing HSRP

To implement HSRP on Cisco IOS XR software software, you need to understand the following concepts:

HSRP Overview

HSRP is useful for hosts that do not support a router discovery protocol (such as Internet Control Message Protocol [ICMP] Router Discovery Protocol [IRDP]) and cannot switch to a new router when their selected router reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of routers running HSRP. The address of this HSRP group is referred to as the *virtual IP address*. One of these devices is selected by the protocol to be the *active router*. The active router receives and routes packets destined for the MAC address of the group. For *n* routers running HSRP, *n* + 1 IP and MAC addresses are assigned.

HSRP detects when the designated active router fails, at which point a selected standby router assumes control of the MAC and IP addresses of the HSRP group. A new *standby router* is also selected at that time.

Devices that are running HSRP send and receive multicast User Datagram Protocol (UDP) based hello packets to detect router failure and to designate active and standby routers.

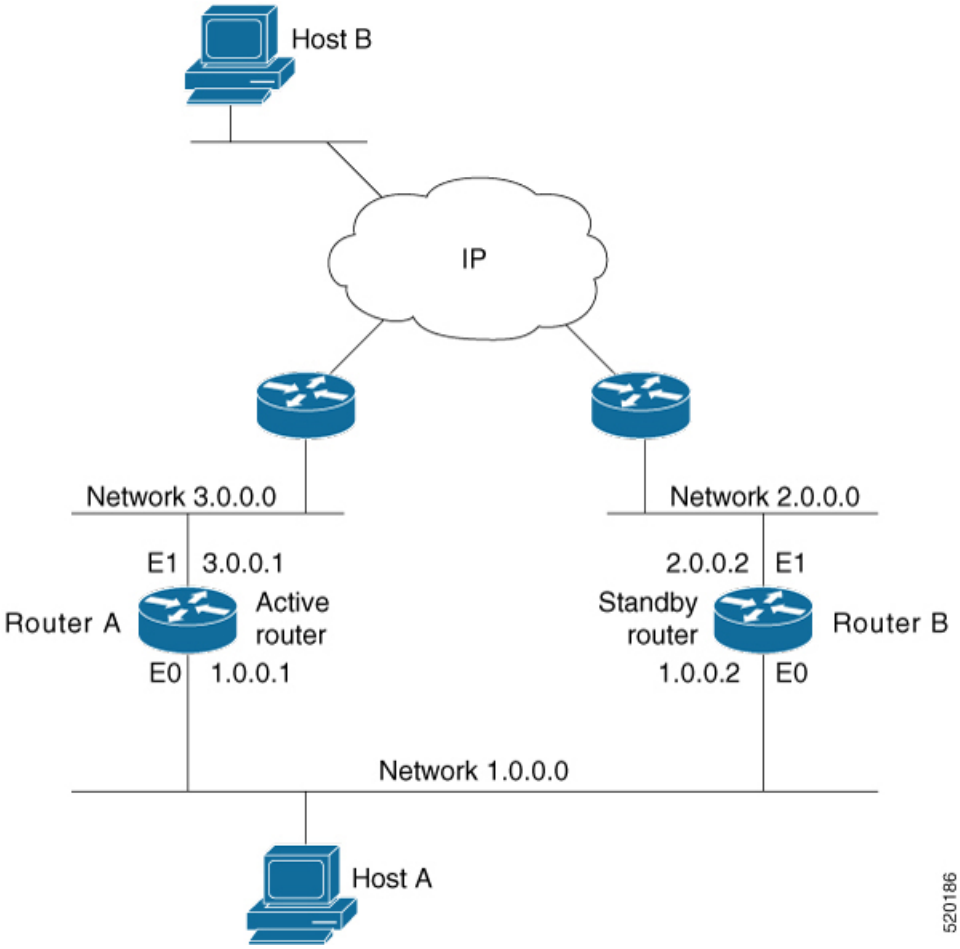
HSRP Groups

An HSRP group consists of two or more routers running HSRP that are configured to provide hot standby services for one another. HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

HSRP works by the exchange of multicast messages that advertise priority among the HSRP group. When the active router fails to send a hello message within a configurable period of time, the standby router with the highest priority becomes the active router. The transition of packet-forwarding functions between routers is completely transparent to all hosts on the network.

Figure 18: Routers Configured as an HSRP Group, on page 299 shows routers configured as members of a single HSRP group.

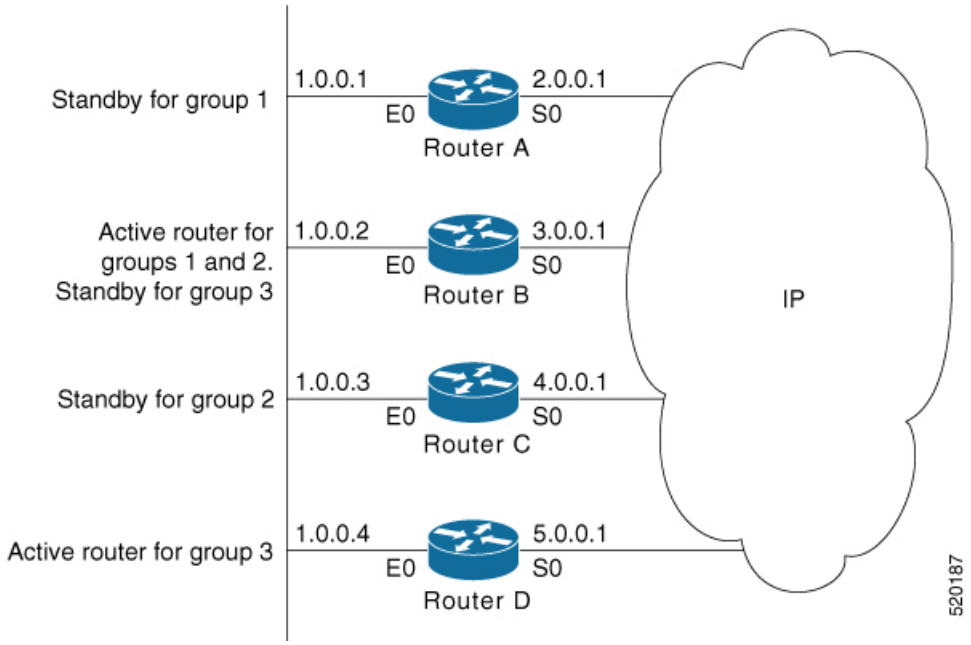
Figure 18: Routers Configured as an HSRP Group



All hosts on the network are configured to use the IP address of the virtual router (in this case, 1.0.0.3) as the default gateway.

A single router interface can also be configured to belong to more than one HSRP group. Figure 19: Routers Configured as Members of Multiple HSRP Groups, on page 300shows routers configured as members of multiple HSRP groups.

Figure 19: Routers Configured as Members of Multiple HSRP Groups



In Figure 19: Routers Configured as Members of Multiple HSRP Groups, on page 300, the Ethernet interface 0 of Router A belongs to group 1. Ethernet interface 0 of Router B belongs to groups 1, 2, and 3. The Ethernet interface 0 of Router C belongs to group 2, and the Ethernet interface 0 of Router D belongs to group 3. When you establish groups, you might want to align them along departmental organizations. In this case, group 1 might support the Engineering Department, group 2 might support the Manufacturing Department, and group 3 might support the Finance Department.

Router B is configured as the active router for groups 1 and 2 and as the standby router for group 3. Router D is configured as the active router for group 3. If Router D fails for any reason, Router B assumes the packet-transfer functions of Router D and maintains the ability of users in the Finance Department to access data on other subnets.

Note A different virtual MAC address (VMAC) is required for each sub interface. VMAC is determined from the group ID. Therefore, a unique group ID is required for each sub interface configured, unless the VMAC is configured explicitly.

Note We recommend that you disable Spanning Tree Protocol (STP) on switch ports to which the virtual routers are connected. Enable RSTP or rapid-PVST on the switch interfaces if the switch supports these protocols.

HSRP and ARP

When a router in an HSRP group goes active, it sends a number of ARP responses containing its virtual IP address and the virtual MAC address. These ARP responses help switches and learning bridges update their port-to-MAC maps. These ARP responses also provide routers configured to use the burned-in address of the

interface as its virtual MAC address (instead of the preassigned MAC address or the functional address) with a means to update the ARP entries for the virtual IP address. Unlike the gratuitous ARP responses sent to identify the interface IP address when an interface comes up, the HSRP router ARP response packet carries the virtual MAC address in the packet header. The ARP data fields for IP address and media address contain the virtual IP and virtual MAC addresses.

Preemption

The HSRP preemption feature enables the router with highest priority to immediately become the active router. Priority is determined first by the priority value that you configure, and then by the IP address. In each case, a higher value is of greater priority.

When a higher-priority router preempts a lower-priority router, it sends a coup message. When a lower-priority active router receives a coup message or hello message from a higher-priority active router, it changes to the speak state and sends a resign message.

ICMP Redirect Messages

Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides many diagnostic functions and can send and redirect error packets to the host. When running HSRP, it is important to prevent hosts from discovering the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router, and that router later fails, then packets from the host are lost.

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.

To support ICMP redirects, redirect messages are filtered through HSRP, where the next-hop IP address is changed to an HSRP virtual address. When HSRP redirects are turned on, ICMP interfaces with HSRP do this filtering. HSRP keeps track of all HSRP routers by sending advertisements and maintaining a real IP address to virtual IP address mapping to perform the redirect filtering.

How to Implement HSRP

This section contains instructions for the following tasks:

Enabling HSRP

The **hsrp ipv4** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. For HSRP to elect a designated router, at least one router in the Hot Standby group must have been configured with, or learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

SUMMARY STEPS

1. **configure**
2. **router hsrp**

3. **interface** type interface-path-id
4. **address-family ipv4**
5. **hsrp** *group-number* **version** *version-no*
6. **address** { **learn** | *address* [**secondary**] }
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** type interface-path-id **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface GigabitEthernet 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-number* **version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
Step 6	**address** { **learn**	*address* [**secondary**] } **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn`	Activates HSRP on the configured interface. • If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. **Note** If you configure HSRP for IPv6, you must configure a link local IPv6 address or enable it using the **autoconfig** keyword. If you do not configure a linklocal IPv6 address, the router does not accept the configuration when you commit your changes using the **commit** keyword.

	Command or Action	Purpose
Step 7	**commit**	

Enabling HSRP for IPv6

Use the following steps to enable HSRP for IPv6.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv6**
5. **hsrp** *group-number*
6. **address linklocal** {**autoconfig** | *ipv6-address*}
7. **address global** *ipv6-address*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv6`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-number* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.

	Command or Action	Purpose
Step 6	**address linklocal** {**autoconfig** | *ipv6-address*} **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# address linklocal autoconfig`	Activates HSRP on the configured interface and assigns a linklocal IPv6 address. • The virtual linklocal address must not match any other virtual linklocal address that is already configured for a different group. The virtual linklocal address must not match the interface linklocal IPv6 address. If you use the **autoconfig** keyword, the linklocal address is calculated using the EUI-64 format. Use the **legacy-compatible** keyword to be compatible with Cisco IOS and other legacy Cisco devices.
Step 7	**address global** *ipv6-address* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# address global 2001:DB8:A:B::1`	Activates HSRP on the configured interface and assigns a global IPv6 address. **Note** If you configure HSRP for IPv6, you must configure a link local IPv6 address or enable it using the **autoconfig** keyword. If you do not configure a linklocal IPv6 address, the router does not accept the configuration when you commit your changes using the **commit** keyword.
Step 8	**commit**	

Configuring HSRP Group Attributes

To configure other Hot Standby group attributes that affect how the local router participates in HSRP, use the following procedure in interface configuration mode as needed:

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** type interface-path-id
4. **hsrp use-bia**
5. **address-family ipv4**
6. **hsrp** *group-number* **version** *version-no*
7. **priority** *priority*
8. **track** *type* **instance** [*priority-decrement*]
9. **preempt** [**delay** *seconds*]
10. **authentication** *string*
11. **mac-address** *address*
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** type interface-path-id **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**hsrp use-bia** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp use-bia`	(Optional) Configures the HSRP to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address or the functional address. • Enter the **use-bia** command on an interface when there are devices that reject Address Resolution Protocol (ARP) replies with source hardware addresses set to a functional address. • To restore the default virtual MAC address, use the **no hsrp use-bia** command.
Step 5	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 6	**hsrp** *group-number* **version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
Step 7	**priority** *priority* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# priority 100`	(Optional) Configures HSRP priority. • The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

	Command or Action	Purpose
		• The priority of the device can change dynamically if an interface is configured with the **track** command and another interface on the device goes down. • If preemption is not enabled using the **preempt** command, the router may not become active even though it might have a higher priority than other HSRP routers. • To restore the default HSRP priority values, use the **no priority** command.
Step 8	**track** *type* **instance** [*priority-decrement*] **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# track TenGigE 0/3/0/1`	(Optional) Configures an interface so that the Hot Standby priority changes on the basis of the availability of other interfaces. • When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface configured for Hot Standby, you can configure a separate list of interfaces to be tracked. • The optional *priority-decrement* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incrementally increased by the same amount. • When multiple tracked interfaces are down and the *priority-decrement* argument has been configured, these configured priority decrements are cumulative. If tracked interfaces are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative. • The **preempt** command must be used in conjunction with this command on all routers in the group whenever the best available router should be used to forward packets. If the **preempt** command is not used, the active router stays active, regardless of the current priorities of the other HSRP routers. • To remove the tracking, use the **no preempt** command.
Step 9	**preempt** [**delay** *seconds*] **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# preempt`	(Optional) Configures HSRP preemption and preemption delay. • When you configure preemption and preemption delay with the **preempt** command, the local router attempts to assume control as the active router when

	Command or Action	Purpose
		the local router has a Hot Standby priority higher than the current active router. If the **preempt** command is not configured, the local router assumes control as the active router only if it receives information indicating that no router is currently in the active state (acting as the designated router). • When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, yet it is unable to provide adequate routing services. This problem can be solved by configuring a delay before the preempting router actually preempts the currently active router. • The preempt *delay seconds* value does not apply if there is no router currently in the active state. In this case, the local router becomes active after the appropriate timeouts (see the **timers** command), regardless of the preempt delay seconds value. • To restore the default HSRP preemption and preemption delay values, use the **no preempt** command.
Step 10	**authentication** *string* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# authentication company1`	(Optional) Configures an authentication string for the Hot Standby Router Protocol (HSRP). • The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a LAN to ensure interoperation. • Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP. • Authentication mismatch does not prevent protocol events such as one router taking over as the designated router. • To delete an authentication string, use the **no authentication** command.
Step 11	**mac-address** *address* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# mac-address 4000.1000.1060`	(Optional) Specifies a virtual MAC address for the HSRP. • We do not recommend this command, except for IBM networking environments in which first-hop redundancy is based on being able to use a virtual MAC address, and in which you cannot change the first-hop addresses in the PCs that are connected to an Ethernet switch.

	Command or Action	Purpose
		• HSRP is used to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first-hop for routing purposes. In this case, it is often necessary to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **mac-address** command to specify the virtual MAC address. • The MAC address specified is used as the virtual MAC address when the router is active. • The **mac-address** command is intended for certain APPN configurations. • In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes. • Enter the **no mac-address** command to revert to the standard virtual MAC address (0000.0C07.ACn).
Step 12	**commit**	

Configuring the HSRP Activation Delay

The activation delay for HSRP is designed to delay the startup of the state machine when an interface comes up. This give the network time to settle and avoids unnecessary state changes early after the link comes up.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **hsrp delay** [**minimum** *seconds*] [**reload** *seconds*]
5. **address-family ipv4**
6. **hsrp** *group-number* **version** *version-no*
7. **address** { **learn** | *address* [**secondary**] }
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**hsrp delay** [**minimum** *seconds*] [**reload** *seconds*] **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)#hsrp delay minimum 2 reload 10`	Delays the startup of the state machine when an interface comes up, so that the network has time to settle and there are no unnecessary state changes early after the link comes up. The reload delay is the delay applied after the first interface up event. The minimum delay is the delay that is applied after any subsequent interface up event (if the interface flaps).
Step 5	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 6	**hsrp** *group-number* **version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
Step 7	**address** { **learn** | *address* [**secondary**] } **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn`	Activates HSRP on the configured interface. • If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. **Note** If you configure HSRP for IPv6, you must configure a link local IPv6 address or enable it using the **autoconfig** keyword. If you do not configure a linklocal IPv6 address, the router does not accept the configuration when you commit your changes using the **commit** keyword.

	Command or Action	Purpose
Step 8	**commit**	

Enabling HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of ICMP redirect messages is enabled on routers running HSRP.

To configure the reenabling of this feature on your router if it is disabled, use the **hsrp redirects** command in interface configuration mode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **hsrp redirects disable**
5. **address-family ipv4**
6. **hsrp** *group-number* **version** *version-no*
7. **address** { **learn** | *address* [**secondary**] }
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**hsrp redirects disable** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp redirects`	Configures Internet Control Message Protocol (ICMP) redirect messages to be sent when the Hot Standby Router Protocol (HSRP) is configured on an interface. • The **hsrp redirects** command can be configured on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface inherits the global value. If ICMP redirects have been explicitly

	Command or Action	Purpose
		disabled on an interface, then the global command cannot reenable the functionality. • With the **hsrp redirects** command enabled, ICMP redirect messages are filtered by replacing the real IP address in the next-hop address of the redirect packet with a virtual IP address, if it is known to HSRP. • To revert to the default, which is that ICMP messages are enabled, use the **no hsrp redirects** command.
Step 5	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 6	**hsrp** *group-number* **version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
Step 7	**address** { **learn** | *address* [**secondary**] } **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn`	Activates HSRP on the configured interface. • If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. **Note** If you configure HSRP for IPv6, you must configure a link local IPv6 address or enable it using the **autoconfig** keyword. If you do not configure a linklocal IPv6 address, the router does not accept the configuration when you commit your changes using the **commit** keyword.
Step 8	**commit**	

Multiple Group Optimization (MGO) for HSRP

Multiple Group Optimization provides a solution for reducing control traffic in a deployment consisting of many subinterfaces. By running the HSRP control traffic for just one of the sessions, the control traffic is reduced for the subinterfaces with identical redundancy requirements. All other sessions are subordinates of this primary session, and inherit their states from it.

Customizing HSRP

Customizing the behavior of HSRP is optional. Be aware that as soon as you enable a HSRP group, that group is in operation.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no* **version** *version-no*
6. **name** *name*
7. **address** { **learn** | *address*}
8. **address** *address* **secondary**
9. **authentication** *string*
10. **bfd fast-detect**
11. **mac-address** *address*
12. **hsrp** *group-no* **slave**
13. **follow** *mgo-session-name*
14. **address** *ip-address*
15. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `Router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no* **version** *version-no* **Example:** `Router(config-hsrp-ipv4)# hsrp 1 version 2`	Enables HSRP group configuration mode on a specific interface. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.

	Command or Action	Purpose
Step 6	**name** *name* **Example:** `Router(config-hsrp-gp)# name s1`	Configures an HSRP session name.
Step 7	**address** { **learn** | *address*} **Example:** `Router(config-hsrp-gp)# address learn`	Enables hot standby protocol for IP. • If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router.
Step 8	**address** *address* **secondary** **Example:** `Router(config-hsrp-gp)# address 10.20.30.1 secondary`	Configures the secondary virtual IPv4 address for a router.
Step 9	**authentication** *string* **Example:** `Router(config-hsrp-gp)# authentication company1`	Configures an authentication string for the Hot Standby Router Protocol (HSRP).
Step 10	**bfd fast-detect** **Example:** `Router(config-hsrp-gp)# bfd fast-detect`	Enables bidirectional forwarding(BFD) fast-detection on a HSRP interface.
Step 11	**mac-address** *address* **Example:** `Router(config-hsrp-gp)# mac-address 4000.1000.1060`	Specifies a virtual MAC address for the Hot Standby Router Protocol (HSRP).
Step 12	**hsrp** *group-no* **slave** **Example:** `Router(config-hsrp-gp)# hsrp 2 slave`	Enables HSRP slave configuration mode on a specific interface.

	Command or Action	Purpose
Step 13	**follow** *mgo-session-name* **Example:** `Router(config-hsrp-slave)# follow s1`	Instructs the subordinate group to inherit its state from a specified group.
Step 14	**address** *ip-address* **Example:** `Router(config-hsrp-slave)# address 10.3.2.2`	Configures the primary virtual IPv4 address for the subordinate group.
Step 15	**commit**	

Configuring a Primary Virtual IPv4 Address

To enable hot standby protocol for IP, use the **address (hsrp)** command in the HSRP group submode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no***version** *version-no*
6. **address** { **learn** | *address*}
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.

	Command or Action	Purpose
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no***version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2`	Enables HSRP group configuration mode on a specific interface. **Note** • The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families. • HSRP version 2 provides an extended group range of 0-4095.
Step 6	**address** { **learn** | *address*} **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# address learn`	Enables hot standby protocol for IP.
Step 7	**commit**	

Configuring a Secondary Virtual IPv4 Address

To configure the secondary virtual IPv4 address for a router, use the **address secondary** command in the Hot Standby Router Protocol (HSRP) virtual router submode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no***version** *version-no*
6. **address** *address* **secondary**
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no***version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2`	Enables HSRP group configuration mode on a specific interface. **Note** • The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families. • HSRP version 2 provides an extended group range of 0-4095.
Step 6	**address** *address* **secondary** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# address 10.20.30.1 secondary`	Configures the secondary virtual IPv4 address for a router.
Step 7	**commit**	

Configuring the Subordinate Group to Inherit its State from a Specified Group

To instruct the subordinate group to inherit its state from a specified group, use the following steps:

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no* **slave**
6. **follow** *mgo-session-name*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `Router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no* **slave** **Example:** `Router(config-hsrp-ipv4)# hsrp 2 slave`	Enables HSRP slave configuration mode on a specific interface.
Step 6	**follow** *mgo-session-name* **Example:** `Router(config-hsrp-slave)# follow m1`	Instructs the subordinate group to inherit its state from a specified group.
Step 7	**commit**	

Configuring a Subordinate Primary Virtual IPv4 Address

To configure the primary virtual IPv4 address for the subordinate group, use the **subordinate primary virtual IPv4 address** command in the HSRP slave submode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no* **slave**
6. **address** *ip-address*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `Router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no* **slave** **Example:** `Router(config-hsrp-ipv4)# hsrp 2 slave`	Enables HSRP slave configuration mode on a specific interface.
Step 6	**address** *ip-address* **Example:** `Router(config-hsrp-slave)# address 10.2.3.2`	Configures the primary virtual IPv4 address for the subordinate group.
Step 7	**commit**	

Configuring a Secondary Virtual IPv4 address for the Subordinate Group

Perform this task to configure the secondary virtual IPv4 address for the subordinate group.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **vrrp** *group-no* **slave**
6. **address** *address* **secondary**
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `Router(config)# router vrrp`	Enables VRRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-vrrp)# interface TenGigE 0/2/0/1`	Enables VRRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-vrrp-if)# address-family ipv4`	Enables VRRP address-family configuration mode on a specific interface.
Step 5	**vrrp** *group-no* **slave** **Example:** `Router(config-vrrp-address-family)# vrrp 2 slave`	Enables VRRP slave configuration mode on a specific interface.
Step 6	**address** *address* **secondary** **Example:** `Router(config-vrrp-slave)# address 10.20.30.1 secondary`	Configures the secondary virtual IPv4 address for a router.
Step 7	**commit**	

Configuring a Subordinate Virtual MAC Address

To configure the virtual MAC address for the subordinate group, use the **subordinate virtual mac address** command in the HSRP slave submode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no* **slave**
6. **mac-address** *address*

7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `Router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no* **slave** **Example:** `Router(config-hsrp-ipv4)# hsrp 2 slave`	Enables HSRP slave configuration mode on a specific interface.
Step 6	**mac-address** *address* **Example:** `Router(config-hsrp-slave)# mac-address 10.20.30`	Configures the virtual MAC address for the subordinate group.
Step 7	**commit**	

Configuring an HSRP Session Name

To configure an HSRP session name, use the **session name** command in the HSRP group submode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** *group-no***version** *version-no*
6. **name** *name*

7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-no***version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2`	Enables HSRP group configuration mode on a specific interface. **Note** • The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families. • HSRP version 2 provides an extended group range of 0-4095.
Step 6	**name** *name* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# name s1`	Configures an HSRP session name.
Step 7	**commit**	

BFD for HSRP

Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between two forwarding engines. BFD sessions can operate in one of the two modes, namely, asynchronous mode or demand mode. In asynchronous mode, both endpoints periodically send hello packets to each other. If a number of those

packets are not received, the session is considered down. In demand mode, it is not mandatory to exchange hello packets; either of the hosts can send hello messages, if needed. Cisco supports the BFD asynchronous mode.

Advantages of BFD

- BFD provides failure detection in less than one second.
- BFD supports all types of encapsulation.
- BFD is not tied to any particular routing protocol, supports almost all routing protocols.

BFD Process

HSRP uses BFD to detect link failure and facilitate fast failover times without excessive control packet overhead.

The HSRP process creates BFD sessions as required. When a BFD session goes down, each Standby group monitoring the session transitions to Active state.

HSRP does not participate in any state elections for 10 seconds after a transition to Active state triggered by a BFD session going down.

Configuring BFD

For HSRP, configuration is applied under the existing HSRP-interface sub-mode, with BFD fast failure configurable per HSRP group and the timers (minimum-interface and multiplier) configurable per interface. BFD fast failure detection is disabled by default.

Enabling BFD

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **hsrp** [*group number*] **version** *version-no* **bfd fast-detect** [**peer** **ipv4** *ipv4-address* *interface-type interface-path-id*]
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** [*group number*] **version** *version-no* **bfd fast-detect** [**peer ipv4** *ipv4-address interface-type interface-path-id*] **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2 bfd fast-detect peer ipv4 10.3.5.2 TenGigE 0/3/4/2`	Enables fast detection on a specific interface. **Note** • The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families. • HSRP version 2 provides an extended group range of 0-4095.
Step 6	**commit**	

Modifying BFD timers (minimum interval)

Minimum interval determines the frequency of sending BFD packets to BFD peers (in milliseconds). The default minimum interval is 15ms.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **hsrp bfd minimum-interval** *interval*
5. **address-family ipv4**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**hsrp bfd minimum-interval** *interval* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd minimum-interval 20`	Sets the minimum interval to the specified period. The interval is in milliseconds; range is 15 to 30000 milliseconds.
Step 5	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 6	**commit**	

Modifying BFD timers (multiplier)

Multiplier is the number of consecutive BFD packets which must be missed from a BFD peer before declaring that peer unavailable. The default multiplier is 3.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** *type interface-path-id*
4. **hsrp bfd multiplier** *multiplier*
5. **address-family ipv4**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**hsrp bfd multiplier** *multiplier* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd multiplier 30`	Sets the multiplier to the value. Range is 2 to 50.
Step 5	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 6	**commit**	

Enhanced Object Tracking for HSRP and IP Static

A failure between the active router and the core network cannot be detected using standard HSRP failure detection mechanisms. Object tracking is used to detect such failures. When such a failure occurs, the active router applies a priority decrement to its HSRP session. If this causes its priority to fall below that of the standby router, it will detect this from the HSRP control traffic, and then use this as a trigger to preempt and take over the active role.

Cisco IOS XR software supports up to 512 tracked objects.

The enhanced object tracking for HSRP and IP Static feature provides first-hop redundancy as well as default gateway selection based on IP Service Level Agreement (IPSLA).

See the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*, for more information about enhanced object tracking for static routes.

Configuring object tracking for HSRP

To enable tracking of the named object with the specified decrement, use the following configuration in the HSRP group sub mode.

SUMMARY STEPS

1. **configure**
2. **router hsrp**
3. **interface** type interface-path-id
4. **address-family ipv4**
5. **hsrp** *group-number* **version** *version-no*
6. **track object** *name [priority-decrement]*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router hsrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router hsrp`	Enables HSRP configuration mode.
Step 3	**interface** type interface-path-id **Example:** `RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1`	Enables HSRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4`	Enables HSRP address-family configuration mode on a specific interface.
Step 5	**hsrp** *group-number* **version** *version-no* **Example:** `RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1`	Enables HSRP group submode. **Note** The **version** keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
Step 6	**track object** *name [priority-decrement]* **Example:**	Enable tracking of the named object with the specified decrement.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-hsrp-gp)# track object t1 2`	
Step 7	**commit**	

Hot Restartability for HSRP

In the event of failure of a HSRP process in one active group, forced failovers in peer HSRP active router groups should be prevented. Hot restartability supports warm RP failover without incurring forced failovers to peer HSRP routers for active groups.

Configuration Examples for HSRP Implementation on Software

This section provides the following HSRP configuration examples:

Configuring an HSRP Group: Example

The following is an example of enabling HSRP on an interface and configuring HSRP group attributes:

```
configure
router hsrp
interface TenGigE 0/2/0/1
address-family ipv4
hsrp 1
name s1
address 10.0.0.5
timers 100 200
preempt delay 500
priority 20
track TenGigE 0/2/0/2
authentication company0
use-bia
commit
hsrp 2 slave
follow s1
address 10.3.2.2
commit
```

Configuring a Router for Multiple HSRP Groups: Example

The following is an example of configuring a router for multiple HSRP groups:

```
configure
router hsrp
interface TenGigE 0/2/0/3
address family ipv4
hsrp 1
address 1.0.0.5
priority 20
preempt
```

```
authentication sclara
hsrp 2
address 1.0.0.6
priority 110
preempt
authentication mtview
hsrp 3
address 1.0.0.7
preempt
authentication svale
commit
```

Additional References

The following sections provide references related to HSRP

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Quality of Service Commands on Modular Quality of Service Command Reference for Cisco ASR 9000 Series Routers*
Class-based traffic shaping, traffic policing, low-latency queuing, and Modified Deficit Round Robin (MDRR)	*Configuring Modular Quality of Service Congestion Management on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
WRED, RED, and tail drop	*Configuring Modular QoS Congestion Avoidance on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
HSRP commands	*HSRP Commands on IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services on System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards and RFCs

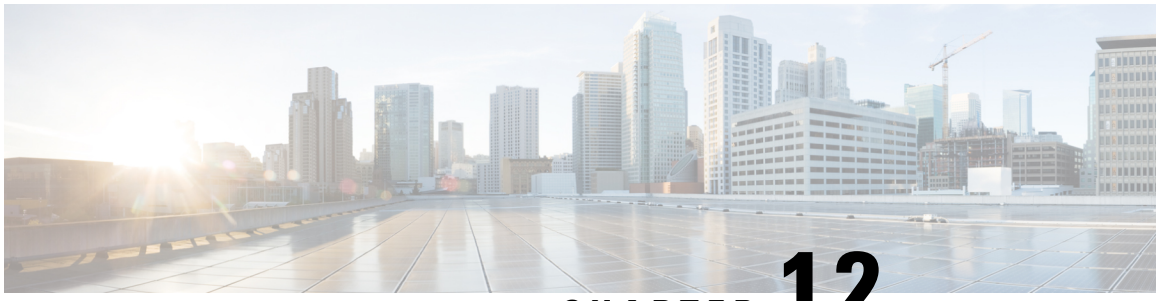
Standard/RFC	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
	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



CHAPTER 12

Implementing LPTS

Local Packet Transport Services (LPTS) maintains tables describing all packet flows destined for the secure domain router (SDR), making sure that packets are delivered to their intended destinations.

For a complete description of the LPTS commands listed in this module, refer to the LPTS Commands module of *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Feature History for Implementing LPTS

Release	Modification
Release 7.3.2	Monitor LPTS host path drops via YANG data model was introduced.
Release 5.3.2	NP LPTS Based Policer was introduced.
Release 3.9.0	LPTS was introduced.

Prerequisites for Implementing LPTS

The following prerequisites are required to implement LPTS:

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Implementing LPTS

To implement LPTS features mentioned in this document you must understand the following concepts:

LPTS Overview

LPTS uses two components to accomplish this task: the port arbitrator and flow managers. The port arbitrator and flow managers are processes that maintain the tables that describe packet flows for a logical router, known as the Internal Forwarding Information Base (IFIB). The IFIB is used to route received packets to the correct Route Processor or line card for processing.

LPTS interfaces internally with all applications that receive packets from outside the router. LPTS functions without any need for customer configuration. However, LPTS **show** commands are provided that allow customers to monitor the activity and performance of LPTS flow managers and the port arbitrator.

LPTS Policers

Table 11: Feature History Table

Feature Name	Release Information	Description
Monitor LPTS Host Path Drops via YANG Data Model	Release 7.3.2	This feature allows you to use the `Cisco-IOS-XR-lpts-pre-ifib-oper.yang` data model to monitor the policer action for Local Packet Transport Services (LPTS) flow type for all IOS XR platforms. To access this data model, see the Github repository.

In Cisco IOS XR, the control packets, which are destined to the Route Processor (RP), are policed using a set of ingress policers in the incoming line cards. These policers are programmed statically during bootup by LPTS components. The policers are applied based on the flow type of the incoming control traffic. The flow type is determined by looking at the packet headers. The policer rates for these static ingress policers are defined in a configuration file, which are programmed on the line card during bootup.

You can change the policer values based on the flow types of these set of ingress policers. You are able to configure the rate per policer per node (locally) and globally using the command-line interface (CLI); therefore, overwriting the static policer values.

Note If two different ACLs with same ACEs are applied to an LPTS Policer, only the first ACL applied takes effect. When the first ACL is removed, the second ACL does not take effect on the LPTS Policer. If you want the second ACL to take effect on the LPTS Policer, reconfigure it on the LPTS Policer.

IP TOS Precedence

By default, router allows all packets into the network. The IP table of service (TOS) precedence feature allows you to classify packets by IP precedence value. The IP precedence value can be configured for every flow. Once configured for a flow type, only packets that match the defined IP precedence value are allowed, and others are rejected.

The precedence value can either be a number or name. This table lists configurable precedence values:

Table 12: Precedence Values

Precedence Number	Precedence Name	Description
0	routine	Matches packets with routine precedence.
1	priority	Matches packets with priority precedence.
2	immediate	Matches packets with immediate precedence.
3	flash	Matches packets with flash precedence.
4	flash-override	Matches packets with flash override precedence.
5	critical	Matches packets with critical precedence.
6	internet	Matches packets with internetwork control precedence.
7	network	Matches packets with network control precedence.

ACL Based Policer

ACL based policer is a session based policer that provides secure network access based on session.

Note

- The ACL based policer feature is supported only on ASR 9000 Enhanced Ethernet Line Cards, ASR 9000 3rd Generation Line Cards, and ASR 9000 4th Generation Line Cards.
- SNMP is not supported on ASR 9000 4th Generation Line Cards. Therefore, the ACL entries configured based on LPTS are not displayed if the ACLs are configured on ASR 9000 4th Generation Line Cards.
- When multiple ACLs are configured for an LPTS policier, only the first ACL details are displayed in the LPTS statistics command output.

Benefits

These are the benefits of ACL based policer:

- Rate limit incoming packets based on session.
- Modify policer rate depending on traffic load.

- Block entire traffic based on a specific session without impacting other sessions with same flow.

Configuring LPTS Policers

This task allows you to configure the LPTS policers.

SUMMARY STEPS

1. **configure**
2. **lpts pifib hardware police** [**location** *node-id*]
3. **flow** *flow_type* {**rate** *rate*}
4. **commit**
5. **show lpts pifib hardware police** [**location** {**all** | *node_id*}]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**lpts pifib hardware police** [**location** *node-id*]
	Example:
	`RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0`
	`RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)#`
	`RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police`
	`RP/0/RSP0/CPU0:router(config-pifib-policer-global)#`
		Configures the ingress policers and enters pifib policer global configuration mode or pifib policer per node configuration mode.
		The example shows pifib policer per node configuration mode and global.

Step 3	**flow** *flow_type* {**rate** *rate*} **Example:** `RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# flow ospf unicast default rate 20000`	Configures the policer for the LPTS flow type. The example shows how to configure the policer for the ospf flow type. • Use the *flow_type* argument to select the applicable flow type. For information about the flow types, see *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*. • Use the **rate** keyword to specify the rate in packets per seconds (PPS). The range is from 0 to 4294967295.

	Command or Action	Purpose

		Note LPTS policy for ntp-default flow type, supports a flow rate of 100 pps on Cisco ASR 9000 Series Router.
		
		Starting with Cisco IOS XR Release 6.1.3, LPTS policy for ntp-default flow type, supports a flow rate higher than 100 pps on Cisco ASR 9000 Series Router.
		
		Based on the number of NTP client scale requirement, you can increase the flow rate value to allow higher packets per second (PPS). For example,
		
		`lpts pifib hardware police location 0/0/CPU0`
		`flow ntp default rate 1000`
		`flow ntp known rate 1000`

Step 4	**commit**	

Step 5	**show lpts pifib hardware police** [**location** {**all** | *node_id*}]
	
	Example:
	
	`RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/2/cpu0`
		Displays the policer configuration value set.
		
		• (Optional) Use the **location** keyword to display pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
		
		• Use the **all** keyword to specify all locations.
		
		Starting Cisco IOS XR Software Release 7.3.2, you can use `Cisco-IOS-XR-lpts-pre-ifib-oper` YANG data model across all IOS XR platforms to retrieve the policer statistics of the flow type. The following example shows the sample RPC request:
		
		`===== RPC request ======`
		`<rpc message-id="101"`
		`xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">`
		`<get>`
		`<filter>`
		`<lpts-pifib`
		`xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-lpts-pre-ifib-oper">`
		
		`<nodes>`
		`<node>`
		`<node-name>0/0/CPU0</node-name>`
		`<pifib-hw-flow-policer-stats/>`
		`</node>`
		`</nodes>`
		`</lpts-pifib>`
		`</filter>`
		`</get>`
		`</rpc>`
		`##`

	Command or Action	Purpose
		The policer stats of each flow type is the aggregate of all the NPU counters. In the example, the NPU ID of 255 indicates that the value is an aggregate of all NPU stats and provides a simplified view of policer stats per flow type.

Configuring LPTS Policer with IP TOS Precedence

This task allows you to configure the LPTS policers with IP table of service (TOS) precedence:

SUMMARY STEPS

1. **configure**
2. **lpts pifib hardware police** [**location** *node-id*]
3. **flow** *flow_type*
4. **precedence** {*number* | *name*}
5. **commit**
6. **show lpts pifib hardware police** [**location** {**all** | *node_id*}]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**lpts pifib hardware police** [**location** *node-id*]
	Example:
	`RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0`
	`or`
	`RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police`
		Configures the ingress policers. You can configure per node or all locations.
		The example shows configuration of pifib policer on an individual node and globally for all nodes respectively.

Step 3	**flow** *flow_type*
	Example:
	`RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# flow telnet default`
	`or`
	`RP/0/RSP0/CPU0:router(config-pifib-policer-global)# flow telnet default`
		Configures the policer for the LPTS flow type. The example shows how to configure the policer for the telnet flow type per node or global mode (all locations).
		• Use the *flow_type* argument to select the applicable flow type. For information about the flow types, see *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

	Command or Action	Purpose

Step 4	**precedence** {*number* | *name*}
	Example:
	`RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# precedence 5 6 7`
	or
	`RP/0/RSP0/CPU0:router(config-pifib-policer-global)# precedence 5 6 7`
		Configures IP TOS **precedence** against a flow type. You can specify either a precedence number or name. For more information about **precedence**, use the question mark (?) online help function.
		The example shows how to configure IP TOS **precedence** 5, 6, and 7 per node or global mode.

Step 5	**commit**	
Step 6	**show lpts pifib hardware police** [**location** {**all** | *node_id*}] **Example:** `RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/2/cpu0`	Displays the policer configuration value set. • (Optional) Use the **location** keyword to display policer value for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation. • Use the **all** keyword to specify all locations.

Mapping the LPTS Policer with an ACL

This task allows you to map the LPTS policer with an ACL.

Note

1. LPTS to ACL map supports only the following values:
   - Source Destination Address
   - Source and destination port
   - Protocol number
   - Object Groups (both network and port groups)
2. When multiple ACLs are configured for an LPTS policier, only the first ACL details are displayed in the LPTS statistics command output.
3. When you are applying an ACL on an LPTS entry, LPTS entry filters and ACL should be defined in the same order. So, if you want to limit incoming traffic from the host 10.10.10.10 to any router ip address you need to define LPTS ACL as permit ip from any to 10.10.10.10.

   For example, assume that 10.10.10.10 is the remote address from which traffic should be filtered. The LPTS and ACL should be defined as shown in the following table.

LPTS (local address, port, remote address, port)	ACL
(any,23, 10.10.10.10,65248)	ipv4 access-list lpts 10 permit ipv4 any host 10.10.10.10

4. You can configure a maximum of 50 ACLs per LPTS policer.
5. You can use the following commands to view the LPTS ACL Policer information:
   - **show lpts pifib hardware entry** *acl name* **statistics** *location*
   - **show lpts pifib hardware police** *location*
   - **show lpts pifib hardware entry statistics** *location*

Note The A9K-20HG-FLEX-SE, A9K-20HG-FLEX-TR, A99-32X100GE-X-SE, A99-32
A9K-8HG-FLEX-SE, and A9K-8HG-FLEX-TR line cards do not include LPTS AC
show lpts pifib hardware police location and **show lpts pifib hardware entry statis**

SUMMARY STEPS

1. **configure**
2. **lpts pifib hardware police acl** *acl-name1* **rate** *100* **vrf** *vrf1*
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**lpts pifib hardware police acl** *acl-name1* **rate** *100* **vrf** *vrf1* **Example:** `RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police acl acl-name1 rate 100 vrf vrf1`	Maps the LPTS policer with the ACL by name *acl-name1*.
Step 3	**commit**	

NP Based Policer

Network processor (NP) based policers in LPTS allow rate limit packets based on a specific NP with specific rate.

Benefits of NP based policer

- Rate limit incoming packets based on a specific NP with specific rate.
- Provides secure network access based on the context of a user or a device.

  For example, if a user does not require specific traffic on a particular NP, then the rate limit can be set to 0.
- Modify policer rate depending on traffic load.
- Full utilization of traffic through each NP depending on traffic.
- Stop or block complete traffic based on a specific NP without impacting other NPs with same flow.

Supported Features of NP Based Policer

- Supports Cisco ASR 9000 High Density 100GE Ethernet line cards (such as A9K-8x100G-LB-SE and A9K-8x100G-LB-TR) only.
- Supports ACL, global, local, NP based and static policers.

  For sample configurations, see Configuring ACL, NP, LPTS Local, LPTS Global, and LPTS Static Policers: Example, on page 341.
- Supports existing LPTS and LPTS ACL policer features.
- Supports existing scale limits of all protocols.

Configuring NP Based Policer in LPTS

This task allows you to configure NP based policer in LPTS.

SUMMARY STEPS

1. **configure**
2. **lpts pifib hardware police** [**location** *node-id*]**np** *np-number*
3. **flow** *flow_type* {**default** | **known**} {**rate** *rate*}
4. **commit**
5. **show lpts pifib hardware entry np** *np-number* **statistics** [**location** {**all** | *node_id*}]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**lpts pifib hardware police** [**location** *node-id*]**np** *np-number*
	Example:
	`RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police location 0/1/CPU0 np np3`
	`RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)#`
		Configures the NP based ingress policers and enters pifib policer per node configuration mode.

Step 3	**flow** *flow_type* {**default**	**known**} {**rate** *rate*} **Example:** `RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# flow ospf multicast known rate 100`	Configures the NP based policer for the LPTS flow type. The example shows how to configure the policer for the OSPF flow type. • Use the *flow_type* argument to select the applicable flow type. • Use the **rate** keyword to specify the rate in packets per seconds (PPS). The range is from 0 to 4294967295.
Step 4	**commit**	
Step 5	**show lpts pifib hardware entry np** *np-number* **statistics** [**location** {**all**	*node_id*}] **Example:** `RP/0/RSP0/CPU0:router# show lpts pifib hardware entry np np3 statistics location 0/1/cpu0`	Displays statistics of NP based policer in LPTS. • (Optional) Use the **location** keyword to display pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation. • Use the **all** keyword to specify all locations.

Configuring ACL, NP, LPTS Local, LPTS Global, and LPTS Static Policers: Example

This topic contains sample configurations and output examples of ACL, NP based, LPTS local, LPTS global, and LPTS static policers.

ACL Based Policer

The following is a sample ACL based policer configuration. In this example, the ACL is applied to a BGP session.

```
RP/0/RSP1/CPU0:router(config)# ipv4 access-list lpts_acl_1
RP/0/RSP1/CPU0:router(config-ipv4-acl)# 10 permit tcp any host 200.0.0.1
RP/0/RSP1/CPU0:router(config-ipv4-acl)# 20 deny ipv4 any any
RP/0/RSP1/CPU0:router(config-ipv4-acl)# commit
RP/0/RSP1/CPU0:router(config-ipv4-acl)# end
RP/0/RSP1/CPU0:router(config)# lpts pifib hardware police acl lpts_acl_1 rate 1000
RP/0/RSP1/CPU0:router(config)# commit
```

The following is a show command and its sample output for the preceding policer configuration:

```
RP/0/RSP1/CPU0:router# show lpts pifib hardware entry brief  location 0/1/cpu0

             Node: 0/1/CPU0:
----------------------------------------
L3 - L3 Protocol;L4 - Layer4 Protocol; Intf - Interface;
Dest - Destination Node; V - Virtual;
na - Not Applicable or Not Available;
LU - Local chassis fabric unicast;
LM - Local chassis fabric multicast;
RU - Multi chassis fabric unicast;
RM - Multi chassis fabric multicast;
def - default

Offset L3   VRF id       L4     Intf            Dest       laddr,Port raddr,Port
acl name
------ ---- ------------ ------ --------------- ---------  ----------
-----------------------------------
8      IPV4 *            any    any             Local      any,any any,any

9      CLNS *            -      any             LU(30)     - -

10     IPV4 *            ICMP   any             Local      any,any any,ECHO

11     IPV4 *            OSPF   Optimized       LM[6]      224.0.0.5,any any,any

12     IPV4 *            OSPF   Optimized       LM[6]      224.0.0.6,any any,any

13     IPV4 *            OSPF   Optimized       LM[6]      any,any any,any

14     IPV4 default      TCP    any             LU(30)     any,65145 200.0.0.1,179
lpts_acl_1
15     IPV4 default      TCP    any             LU(30)     any,179 200.0.0.1,any
lpts_acl_1
16     IPV4 default      TCP    any             LU(30)     any,23 any,any

17     IPV4 default      UDP    any             LU(30)     any,161 any,any

18     IPV4 **nVSatellite UDP    any             LU(30)     any,161 any,any

19     IPV4 default      UDP    any             LU(30)     any,162 any,any
```

```
20      IPV4 **nVSatellite UDP    any             LU(30)     any,162 any,any
21      IPV4 default      L2TPV3 any             LU(30)     any,any any,any
22      IPV4 *            OSPF   any             LM[2]      224.0.0.5,any any,any
23      IPV4 *            OSPF   any             LM[2]      224.0.0.6,any any,any
24      IPV4 *            TCP    any             LU(30)     any,any any,179
25      IPV4 *            UDP    any             LU(30)     any,1701 any,any
26      IPV4 *            TCP    any             LU(30)     any,179 any,any
27      IPV4 *            ICMP   any             LU(30)     any,any any,ECHOREPLY
28      IPV4 *            ICMP   any             Local      any,any any,UNREACH
29      IPV4 *            ICMP   any             Local      any,any any,TIMXCEED
30      IPV4 *            ICMP   any             Local      any,any any,PARAMPROB
31      IPV4 *            ICMP   any             Local      any,any any,SRCQUENCH
32      IPV4 *            ICMP   any             Local      any,any any,REDIRECT
33      IPV4 *            ICMP   any             Local      any,any any,TSTAMP
34      IPV4 *            ICMP   any             Local      any,any any,MASKREQ
35      IPV4 *            TCP    any             LU(30)     any,any any,any
36      IPV4 *            UDP    any             LU(30)     any,any any,any
37      IPV4 *            RSVP   any             Local      any,any any,any
38      IPV4 *            OSPF   any             LM[2]      any,any any,any
39      IPV4 *            any    any             LU(30)     any,any any,any
40      IPV4 *            UDP    any             Local      any,any any,any
4       IPV6 *            any    any             Local      any,any any,any
5       IPV6 *            ICMP6  any             Local      any,any any,NDRTRSLCT
6       IPV6 *            ICMP6  any             Local      any,any any,NDRTRADV
7       IPV6 *            ICMP6  any             Local      any,any any,NDNBRSLCT
8       IPV6 *            ICMP6  any             Local      any,any any,NDNBRADV
9       IPV6 *            ICMP6  any             Local      any,any any,ECHOREQ
10      IPV6 default      UDP    any             LU(30)     any,161 any,any
11      IPV6 **nVSatellite UDP    any             LU(30)     any,161 any,any
12      IPV6 default      UDP    any             LU(30)     any,162 any,any
13      IPV6 **nVSatellite UDP    any             LU(30)     any,162 any,any
14      IPV6 default      ICMP6  any             LM[6]      any,any any,MLDLQUERY
```

```
15     IPV6 default      ICMP6  any            LM[6]      any,any any,LSTNRREPORT

16     IPV6 default      ICMP6  any            LM[6]      any,any any,MLDLSTNRDN

17     IPV6 default      ICMP6  any            LM[6]      any,any any,LSTNRREPORTv2

18     IPV6 *            OSPF   any            LU(30)     ff02::5,any any,any

19     IPV6 *            OSPF   any            LU(30)     ff02::6,any any,any

20     IPV6 *            TCP    any            LU(30)     any,any any,179

21     IPV6 *            TCP    any            LU(30)     any,179 any,any

22     IPV6 *            ICMP6  any            LU(30)     any,any any,ECHOREPLY

23     IPV6 *            ICMP6  any            Local      any,any any,UNREACH

24     IPV6 *            ICMP6  any            Local      any,any any,PAK2BIG

25     IPV6 *            ICMP6  any            Local      any,any any,TIMXCEED

26     IPV6 *            ICMP6  any            Local      any,any any,HDRBAD

27     IPV6 *            OSPF   any            LU(30)     any,any any,any

28     IPV6 *            TCP    any            LU(30)     any,any any,any

29     IPV6 *            UDP    any            LU(30)     any,any any,any

30     IPV6 *            any    any            LU(30)     any,any any,any
```

The following is another show command and its sample output:

```
RP/0/RSP1/CPU0:router# show lpts pifib hardware entry stat location 0/1/cpu0 | i IPV4 default
 | i TCP

14     IPV4 default      TCP    any            LM[6]      6/0             any,65145
200.0.0.1,179        lpts_acl_1
15     IPV4 default      TCP    any            LU(30)     0/0             any,179
200.0.0.1,any          lpts_acl_1
16     IPV4 default      TCP    any            LU(30)     0/0             any,23 any,any
```

NP Based Policer

The following is a sample NP based policer configuration:

```
RP/0/RSP0/CPU0:vkg1-lpts# lpts pifib hardware police location 0/1/CPU0
np np2 flow bgp known rate 50
np np3 flow ospf multicast known rate 100
!
lpts pifib hardware police
!
```

The following is a show command and its sample output for the preceding policer configuration:

```
RP/0/RSP1/CPU0:router# show lpts pifib hardware entry np 3 statistics location 0/1/CPU0

             Node: 0/1/CPU0:
```

```
---------------------------------------
L3 - L3 Protocol;L4 - Layer4 Protocol; Intf - Interface;
Dest - Destination Node;
LU - Local chassis fabric unicast;
LM - Local chassis fabric multicast;
RU - Multi chassis fabric unicast;
RM - Multi chassis fabric multicast;
na - Not Applicable or Not Available

Offset L3   VRD id       L4     Intf            Dest       Pkts/Drops      laddr,Port
raddr,Port          acl name
------ ---- ------------ ------ --------------- ---------- ----------------
---------------------          ----------------------------------
8      IPV4 *            any    any             Local      0/0             any,any any,any

9      CLNS *            -      any             LU(30)     0/0             - -

10     IPV4 *           ICMP   any             Local      0/0            any,any any,ECHO

11     IPV4 *            OSPF   Optimized       LU(30)     0/0             224.0.0.5,any
any,any
12     IPV4 *            OSPF   Optimized       LU(30)     0/0             224.0.0.6,any
any,any
13     IPV4 *            OSPF   Optimized       LU(30)     0/0             any,any any,any

14     IPV4 default      TCP    any             LU(30)     0/0             any,23 any,any

15     IPV4 default      L2TPV3 any             LU(30)     0/0             any,any any,any

16     IPV4 *            OSPF   any             LU(30)     0/0             224.0.0.5,any
any,any
17     IPV4 *            OSPF   any             LU(30)     0/0             224.0.0.6,any
any,any
```

The following is another show command and its sample output:

```
RP/0/RSP1/CPU0:router# show lpts pifib hardware police np np3  location 0/1/CPU0

Fri Mar 27 09:32:21.500 UTC
-------------------------------------------------------------
               Node 0/1/CPU0:
-------------------------------------------------------------
Burst = 100ms for all flow types
-------------------------------------------------------------
FlowType               Policer Type    Cur. Rate  Def. Rate  Accepted             Dropped
             TOS Value
---------------------- ------- ------- ---------- ---------- --------------------
-------------------- ----------
unconfigured-default   100     Static  2500       2500       0                    0
             01234567
L2TPv2-fragment        185     Static  10000      10000      0                    0
             01234567
Fragment               101     Static  2500       2500       0                    0
             01234567
OSPF-mc-known          102     np  100       2000       0                     0
        01234567
OSPF-mc-default        103     Static  1500       1500       0                    0
             01234567
OSPF-uc-known          104     Static  2000       2000       0                    0
             01234567
OSPF-uc-default        105     Static  1000       1000       0                    0
             01234567
ISIS-known             143     Static  2000       2000       0                    0
             01234567
```

```
ISIS-default            144     Static  1500       1500       0                   0
             01234567
BFD-known               150     Static  9600       9600       0                   0
             01234567
BFD-default             160     Static  45340      9600       0                   0
             01234567
BFD-MP-known            178     Static  11520      11520      0                   0
             01234567
BFD-MP-0                179     Static  128        128        0                   0
             01234567
BFD-BLB-known           183     Static  11520      11520      0                   0
             01234567
BFD-BLB-0               184     Static  128        128        0                   0
             01234567
BFD-SP-0                182     Static  512        512        0                   0
             01234567
```

LPTS Policer Applied for LC (Local)

The following is a sample configuration for LPTS policer applied for a line card (local):

```
RP/0/RP0/CPU0:router# lpts pifib hardware police location 0/7/CPU0
 flow ospf unicast known rate 30
!
```

The following is a show command and its sample output for the preceding policer configuration:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware police location 0/7/CPU0 | i OSPF

Fri Aug 21 03:51:36.105 UTC
OSPF-mc-known           102     Static  2000       2000       5095                0
             01234567
OSPF-mc-default         103     Static  1500       1500       0                   0
             01234567
OSPF-uc-known           104     Local   30         2000       36                  0
             01234567
OSPF-uc-default         105     Static  1000       1000       0                   0
             01234567
```

LPTS Policer (Global)

The following is a sample configuration for LPTS policer applied globally:

```
RP/0/RP0/CPU0:router# lpts pifib hardware police location 0/7/CPU0
 flow ospf unicast known rate 30
!
lpts pifib hardware police
 flow ospf multicast known rate 50
!
```

The following is a show command and its sample output for the preceding policer configuration:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware police location 0/7/CPU0 | i OSPF

Fri Aug 21 03:54:06.678 UTC
OSPF-mc-known           102     Global  50         2000       5111                0
             01234567
OSPF-mc-default         103     Static  1500       1500       0                   0
             01234567
```

```
OSPF-uc-known          104     Local   30         2000       36                  0
             01234567
OSPF-uc-default        105     Static  1000       1000       0                   0
             01234567
```

LPTS Static Policer

The following is a sample output for LPTS static policer:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware police location 0/7/CPU0 | i OSPF

Fri Aug 21 03:54:06.678 UTC
OSPF-mc-known          102     Global  50         2000       5111                0
             01234567
OSPF-mc-default        103     Static  1500       1500       0                   0
             01234567
OSPF-uc-known          104     Local   30         2000       36                  0
             01234567
OSPF-uc-default        105     Static  1000       1000       0                   0
             01234567
```

Configuration Examples for Implementing LPTS Policers

This section provides the following configuration example:

Configuring LPTS Policers: Example

The following example shows how to configure LPTS policers:

```
configure
 lpts pifib hardware police
  flow ospf unicast default rate 200
  flow bgp configured rate 200
  flow bgp default rate 100
 !
 lpts pifib hardware police location 0/2/CPU0
  flow ospf unicast default rate 100
  flow bgp configured rate 300
 !
```

The following is the show command and the sample output:

```
show lpts pifib hardware police location 0/2/CPU0
```

```
RP/0/RSP1/CPU0:rtr1#
RP/0/RSP1/CPU0:rtr1# show lpts pifib hardware police location 0/2/CPU0
-------------------------------------------------------------
                Node 0/2/CPU0:
-------------------------------------------------------------
Burst = 100ms for all flow types
-------------------------------------------------------------
FlowType                      Policer   Type     Cur. Rate   Def. Rate   Accepted
Dropped       TOS Value
----------------------        -------   -------- ----------  ----------- ----------
--------     ---------------
unconfigured-default             0      Static     2500         2500         0
  0           01234567
L2TPv2-fragment                  85     Static     10000        10000        0
  0           01234567
```

```
Fragment                         1      Static     3000          3000          0
  0           01234567
OSPF-mc-known                    2      Static     2000          2000          0
  0           01234567
OSPF-mc-default                  3      Static     1500          1500          0
  0           01234567
.                                .        .         .             .          .
  .               .
.                                .        .         .             .          .
  .               .
.                                .        .         .             .          .
  .               .
.                                .        .         .             .          .
  .               .
DHCPv4                           92     Static     4000          4000          0
  0           01234567
DHCPv6                           93     Static     4000          4000          0
  0           01234567
ONEPK                            95     Static     2500          2500          0
  0           01234567
TPA                              96     Static     2500          2500          0
  0           01234567
IETF-BOB                         97     Static     9600          9600          0
  0           01234567
------------------------
statistics:
Packets accepted by deleted entries: 0
Packets dropped by deleted entries: 0
Run out of statistics counter errors: 0

RP/0/RSP1/CPU0:rtr1#
```

Configuring LPTS policers with IP TOS Precedence: Example

- The following example shows how to configure IP TOS to telnet default flow and allow packets with precedence 3 or 4 at node 0/0/CPU0:

  ```
  configure
  lpts pifib hardware police location 0/0/CPU0
  flow telnet default
  precedence 3 4
  ```

- The following example shows how to configure IP TOS to telnet known flow to only allow packets with precedence 5 or 6 or 7 at all nodes

  ```
  configure
  lpts pifib hardware police
  flow telnet known
  precedence 5 6 7
  ```

- The following example shows how to configure IP TOS to telnet known flow to only allow packets with routine and network precedence at all nodes

  ```
  configure
  lpts pifib hardware police
  flow telnet known
  precedence routine network
  ```

Additional References

The following sections provide references related to implementing LPTS.

Related Documents

Related Topic	Document Title
Cisco IOS XR LPTS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco LPTS Commands* module in the *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

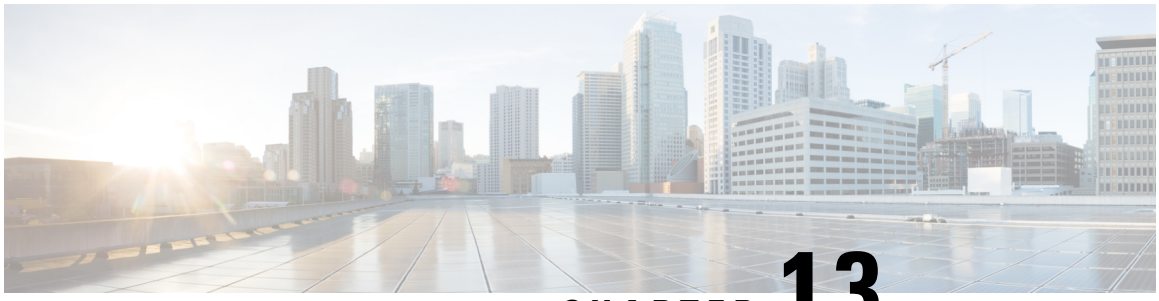
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 13

Implementing VRRP

The Virtual Router Redundancy Protocol (VRRP) feature allows for transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router.

Note For a complete description of the VRRP commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Implementing VRRP

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	• BFD for VRRP feature was added. • MIB support for VRRP feature was added.
Release 4.1.0	VRRP over IPv6 feature was added.

Prerequisites for Implementing VRRP on Cisco IOS XR Software

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for Implementing VRRP on Cisco IOS XR Software

VRRP is supported on Ethernet interfaces, Ethernet sub-interfaces and Ethernet link bundles.

The following are restrictions for implementing VRRP:

- ICMP redirects are not supported.
- Upto 4000 sessions are permitted on Ethernet sub-interfaces.
- On bundle interfaces, the number of sessions per member vary depending on the number of bundle members and their location on network processor (NP) as listed here:
  - One member on one NP: 3999 VRRP sessions
  - Two members on same NP: 1999 VRRP sessions
  - Four members on same NP: 999 VRRP sessions
  - Two members, one on each NP: 3999 VRRP sessions
  - Four members, two on each NP: 1999 VRRP sessions
- Protocol Independent Multicast (PIM) is not supported with VRRP.

Information About Implementing VRRP

To implement VRRP , you need to understand the following concepts:

VRRP Overview

A LAN client can use a dynamic process or static configuration to determine which router should be the first hop to a particular remote destination. The client examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router responds to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- IRDP (ICMP Router Discovery Protocol) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

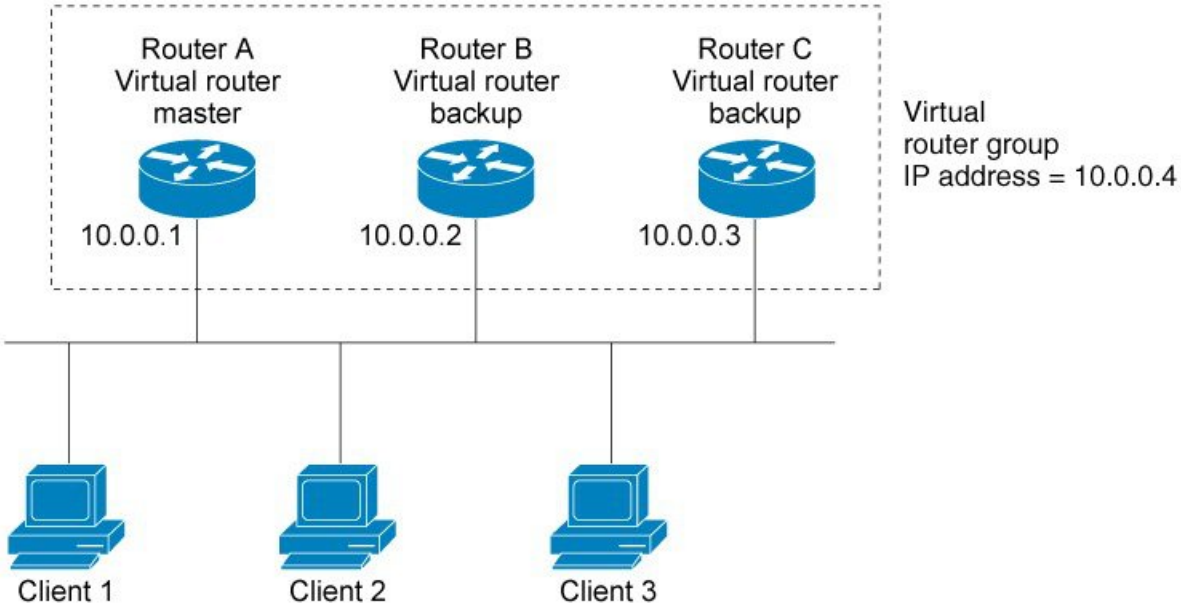
The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. VRRP enables a group of routers to form a single *virtual router* . The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a *VRRP group*.

For example, Figure 20: Basic VRRP Topology, on page 351 shows a LAN topology in which VRRP is configured. In this example, Routers A, B, and C are *VRRP routers* (routers running VRRP) that compose a virtual router. The IP address of the virtual router is the same as that configured for the interface of Router A (10.0.0.1).

Figure 20: Basic VRRP Topology



Because the virtual router uses the IP address of the physical interface of Router A, Router A assumes the role of the *IP address owner.* As the IP address owner router, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 10.0.0.1.

Routers B and C function as *backup virtual routers*. If the IP address owner router fails, the router configured with the higher priority becomes the IP address owner virtual router and provides uninterrupted service for the LAN hosts. When Router A recovers, it becomes the IP address owner virtual router again.

Note We recommend that you disable Spanning Tree Protocol (STP) on switch ports to which the virtual routers are connected. Enable RSTP or rapid-PVST on the switch interfaces if the switch supports these protocols.

Multiple Virtual Router Support

You can configure up virtual routers on a router interface. The actual number of virtual routers that a router interface can support depends on the following factors:

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

In a topology where multiple virtual routers are configured on a router interface, the interface can act as a IP address owner for one or more virtual routers and as a backup for one or more virtual routers.

VRRP Router Priority

An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the IP address owner virtual router fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router functions as a IP address owner virtual router.

If no VRRP router owns the IP address, the priority of a VRRP router, combined with the preempt settings, determines if a VRRP router functions as a IP address owner or a backup virtual router. By default, the highest priority VRRP router functions as IP address owner router, and all the others function as backups. Priority also determines the order of ascendancy to becoming a IP address owner virtual router if the IP address owner virtual router fails. You can configure the priority of each backup virtual router with a value of 1 through 254, using the **vrrp priority** command.

For example, if Router A, the IP address owner virtual router in a LAN topology, fails, an election process takes place to determine if backup virtual Routers B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become IP address owner virtual router because it has the higher priority. If Routers B and C are both configured with the priority of 100, the backup virtual router with the higher IP address is elected to become the IP address owner virtual router.

By default, a preemptive scheme is enabled whereby a higher-priority backup virtual router that becomes available takes over from the current IP address owner virtual router. You can disable this preemptive scheme using the **vrrp preempt disable** command. If preemption is disabled, the backup virtual router that is elected to become IP address owner router upon the failure of the original higher priority IP address owner router, remains the IP address owner router even if the original IP address owner virtual router recovers and becomes available again.

VRRP Advertisements

The IP address owner virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the IP address owner virtual router. The VRRP

advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

Benefits of VRRP

The benefits of VRRP are as follows:

- Redundancy— 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.
- Load Sharing—You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.
- Multiple Virtual Routers—VRRP supports up to 100 virtual routers (VRRP groups) on a router interface, subject to the platform supporting multiple MAC addresses. Cisco ASR 9000 Series Routers support up to a limit of 100 per system with default timers. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.
- Multiple IP Addresses—The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.
- Preemption—The redundancy scheme of VRRP enables you to preempt a backup virtual router that has taken over for a failing IP address owner virtual router with a higher-priority backup virtual router that has become available.
- Text Authentication—You can ensure that VRRP messages received from VRRP routers that comprise a virtual router are authenticated by configuring a simple text password.
- Advertisement Protocol—VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigns VRRP the IP protocol number 112.

Unicast VRRP

Table 13: Feature History Table

Feature Name	Release Name	Description
Unicast VRRP	Release 7.11.1	We have now enabled Layer 3 unicast transport mode in VRRP, allowing it to enhance its capacity to send data to other networks, including cloud networks. Pairwise router redundancy enables high availability in cloud network scenarios. However, a virtual IP (VIP) address is required by the default route of the cloud native function because there is no pre-designated active member in paired routers. HSRP can provide a VIP, but cloud networks do not support Layer 2 multicast or broadcast transports. You can configure VRRP to support Layer 3 unicast transport to overcome the limitation of Layer 2 multicast and broadcast transports. The feature introduces these changes: New Command: **CLI:** • **unicast-peer** Modified Commands: • **show vrrp** command is modified to support new fields: **Mcast packet in Ucast mode**, **IPv4 Unicast Peer**, and **IPv4 Unicast Peer**. **YANG Data Model:** New Xpaths for: • `Cisco-IOS-XR-ipv4-vrrp-cfg.yang` • `Cisco-IOS-XR-ipv4-vrrp-oper.yang` (see GitHub, YANG Data Models Navigator)

You can now configure VRRP to support Layer 3 unicast transport, allowing it to enhance its capacity to send data to cloud networks. Pairwise router redundancy enables high availability in cloud network scenarios. The default route of the cloud native function needs a virtual IP (VIP) address because the paired routers do not have a pre-designated active member. Though HSRP provides a VIP, the cloud networks do not support Layer 2 multicast or broadcast transports. To overcome the limitations of Layer 2 multicast and broadcast transports, configure VRRP in Layer 3 unicast mode to support Layer 3 unicast transport.

This feature also enables VRRP to communicate state transition notifications using event-driven telemetry.

Restrictions for Unicast VRRP

- When you configure the unicast-peer command, the router neither sends nor receives multicast packets.
- You can configure the unicast-peer command only once, allowing for the participation of only two physical routers in a unicast VRRP session.

Configure Unicast VRRP

Configuration Example

The following example shows how to enable unicast transport through VRRP.

```
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet0/0/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1
/* Configure the virtual IP address on the interface. */
Router(config-vrrp-virtual-router)# address 10.0.1.100
/* Configure the unicast-peer command to enable IPv4 unicast transport. */
Router(config-vrrp-virtual-router)# unicast-peer 10.0.1.1
Router(config-vrrp-virtual-router)# exit
Router(config-vrrp-address-family)# exit
Router(config-vrrp-if)# address-family ipv6
Router(config-vrrp-address-family)# vrrp 2
/* Configure the unicast-peer command to enable IPv6 unicast transport.  */
Router(config-vrrp-virtual-router)# unicast-peer FE80::260:3EFF:FE11:6770
Router(config-vrrp-virtual-router)# exit
Router(config-vrrp-address-family)# exit
```

Running Configuration

```
router vrrp
 interface GigabitEthernet0/0/0/0
  address-family ipv4
   vrrp 1
    address 10.0.0.100
    unicast-peer 10.0.1.1
   !
  !
  address-family ipv6
   vrrp 2
    unicast-peer  FE80::260:3EFF:FE11:6770
   !
  !
 !
!
```

Verification

Use the following command to verify if the unicast transport enabled in VRRP. The output shows that both IPv4 and IPv6 unicast peers have been configured, and the respective IP addresses are displayed.

```
Router# show vrrp detail
Fri Sep  8 15:02:35.268 IST
GigabitEthernet0/0/0/0 - IPv4 vrID 1
  State is Master
    2 state changes, last state change 04:00:02
    State change history:
    Sep  8 11:02:29.518 IST  Init     -> Backup   Virtual IP configured
    Sep  8 11:02:33.127 IST  Backup   -> Master   Master down timer expired
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 10.0.0.100
  Virtual MAC address is 0000.5E00.0101, state is active
  Master router is local
  Version is 2
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv4 Unicast Peer: 10.0.1.1 --> IPv4 unicast transport is enabled on VRRP.

GigabitEthernet0/0/0/0 - IPv6 vrID 2
  State is Init
    0 state changes, last state change never
    State change history:
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is ::
  Virtual MAC address is 0000.5E00.0202, state is stored
  Master router is unknown
  Version is 3
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv6 Unicast Peer: FE80::260:3EFF:FE11:6770 --> IPv6 unicast transport is enabled on VRRP.
```

Use the following command to verify detailed statistics about the Virtual Router VRRP configuration. Note that the number of multicast packets received in the VRRP instance when it's configured to function in unicast mode is zero.

```
Router# show vrrp statistics
Fri Sep  8 15:03:03.521 IST
Invalid packets:
  Invalid checksum:                     0
  Unknown/unsupported versions:         0
  Invalid vrID:                         0
  Too short:                            0
Protocol:
  Transitions to Master                 1
Packets:
  Total received:                       0
  Adverts sent:                     14476
  Bad TTL:                              0
```

```
  Short Packets:                        0
  Failed authentication:                0
  Unknown authentication:               0
  Conflicting authentication:           0
  Unknown Type field:                   0
  Conflicting Advertise time:           0
  Conflicting Addresses:                0
  Received with zero priority:          0
  Sent with zero priority:              0
 Mcast packet in Ucast mode:           0 --> Multicast packet being received in unicast
mode.
```

Configuring VRRP

This section contains instructions for configuring VRRP for IPv4 and IPv6 networks.

Note The VRRP virtual router id (vrid) has to be different for different sub-interfaces, for a given physical interface.

Configuring VRRP for IPv4 Networks

This section describes the procedure for configuring and verifying VRRP for IPv4 networks.

Configuration

Use the following configuration for configuring VRRP for IPv4 networks.

Note Certain customizations (as mentioned) are recommended to control the behavior of the VRRP group on committing the VRRP configuration on the Router. If the following customizations are not configured, then the router seizes control of the VRRP group, and immediately assumes the role of the IP address owner virtual router.

```
/* Enter the interface configuration mode and configure an IPv4 address for the interface.
 */
Router(config)# interface gigabitEthernet 0/0/0/1
Router(config-if)# ipv4 address 10.10.10.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# commit
Fri Dec  8 13:49:24.142 IST
Router:Dec  8 13:49:24.285 : ifmgr[402]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/0/0/1, changed state to Down
Router:Dec  8 13:49:24.711 : ifmgr[402]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/0/0/1, changed state to Up

Router(config-if)# exit
Router(config)# do show ip int brief
Fri Dec  8 13:50:05.505 IST

Interface                      IP-Address      Status          Protocol Vrf-Name
GigabitEthernet0/0/0/0         unassigned      Shutdown        Down     default

GigabitEthernet0/0/0/1         10.10.10.1      Up              Up       default
```

```
GigabitEthernet0/0/0/2            unassigned        Shutdown          Down        default

GigabitEthernet0/0/0/3            unassigned        Shutdown          Down        default

GigabitEthernet0/0/0/4            unassigned        Shutdown          Down        default


/* Enter the VRRP configuration mode and add the configured interface. */
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet 0/0/0/1

/* CUSTOMIZATION: Configure a delay for the startup of the state machine when the interface
 comes up. */
Router(config-vrrp)# delay minimum 2 reload 10 */

/* Configure VRRP version 3 for IPv4 */
Router(config-vrrp-if)# address-family ipv4 vrrp 100 version 3
Router(config-vrrp-virtual-router)# address 10.10.10.1

/* CUSTOMIZATION: Disable the installation of routes for the VRRP virtual addresses. */
Router(config-vrrp-virtual-Router)# accept-mode disable

/* CUSTOMIZATION: Set a priority for the virtual Router. */
Router(config-vrrp-virtual-Router)# priority 254

/* CUSTOMIZATION: Configure a preempt delay value that controls the selection of the IP
address owner virtual Router. */
Router(config-vrrp-virtual-Router)# preempt delay 15

/* CUSTOMIZATION: Configure the interval between successive advertisements by the IP address
 owner virtual Router. */
Router(config-vrrp-virtual-Router)#timer 4

/* CUSTOMIZATION: Configure VRRP to track an interface. */
Router(config-vrrp-virtual-Router)# track interface GigabitEthernet0/0/0/1 30

 /* Commit the configuration */
Router(config-vrrp-virtual-Router)# commit
```

You have successfully configured VRRP for IPv4 networks.

Validation

Use the following commands to validate the configuration.

```
/* Validate the configuration */
Router(config-vrrp-virtual-router)# do show run interface GigabitEthernet 0/0/0/1
Fri Dec  8 15:04:38.140 IST
interface GigabitEthernet0/0/0/1
 ipv4 address 10.10.10.1 255.255.255.0
!

Router(config)# show running-config router vrrp
Fri Dec  8 13:50:18.959 IST
router vrrp
 interface GigabitEthernet0/0/0/1
   delay minimum 2 reload 10
  address-family ipv4
   vrrp 100 version 3
    priority 254
```

```
    preempt delay 15
    timer 4
    track interface GigabitEthernet0/0/0/2 30
    address 10.10.10.1
    accept-mode disable
   !
  !
 !
```

```
Router(config-vrrp-virtual-router)# do show vrrp ipv4 interface gigabitEthernet 0/0/0/1
Fri Dec  8 15:02:56.952 IST
IPv4 Virtual Routers:
                     A indicates IP address owner
                     | P indicates configured to preempt
                     | |
Interface   vrID Prio A P State    Master addr     VRouter addr
Gi0/0/0/1    100  255 A P Master   local           10.10.10.1
```

```
Router(config-vrrp-virtual-router)# end
Router# show vrrp detail
Fri Dec  8 15:08:36.469 IST
GigabitEthernet0/0/0/1 - IPv4 vrID 100
  State is Master, IP address owner
    1 state changes, last state change 01:19:06
    State change history:
    Dec  8 13:49:30.147 IST  Init     -> Master   Delay timer expired
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 10.10.10.1
  Virtual MAC address is 0000.5E00.0164, state is active
  Master router is local
  Version is 3
  Advertise time 1 secs
    Master Down Timer 3.003 (3 x 1 + (1 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 255
    Configured priority 100, may preempt
      minimum delay 0 secs
```

You have successfully validated VRRP for IPv4 networks.

Configuring VRRP for IPv6 Networks

This section describes the procedure for configuring and verifying VRRP for IPv6 networks.

Configuration

The following sample includes the configuration and customization of VRRP for IPv6 networks.

Note Certain customizations (as mentioned) are recommended to control the behavior of the VRRP group on committing the VRRP configuration on the Router. If the following customizations are not configured, then the Router seizes control of the VRRP group, and immediately assumes the role of the IP address owner virtual Router.

```
/* Enter the interface configuration mode and configure an IPv6 address */
```

```
Router# interface GigabitEthernet 0/0/0/2
Router(config-if)# ipv6 address 10::1/64
Router(config-if)# no shut

/* Exit the interface configuration mode and enter the vrrp configuration mode */
Router(config-if)# exit
Router(config)# Router vrrp

/* Add the configured interface for VRRP */
Router(config-vrrp)# interface GigabitEthernet 0/0/0/2

/* CUSTOMIZATION: Configure a delay for the startup of the state machine when the interface
 comes up. */
Router(config-vrrp)# delay minimum 2 reload 10 */

/* Enable the IPv6 global and link local address family on the interface  */
Router(config-vrrp-if)# address-family ipv6 vrrp 50
Router(config-vrrp-virtual-Router)# address linklocal autoconfig

/* CUSTOMIZATION: Disable the installation of routes for the VRRP virtual addresses. */
Router(config-vrrp-virtual-Router)# accept-mode disable

/* CUSTOMIZATION: Set a priority for the virtual Router. */
Router(config-vrrp-virtual-Router)# priority 254

/* CUSTOMIZATION: Configure a preempt delay value that controls the selection of the IP
address owner virtual Router. */
Router(config-vrrp-virtual-Router)# preempt delay 15

/* CUSTOMIZATION: Configure the interval between successive advertisements by the IP address
 owner virtual Router. */
Router(config-vrrp-virtual-Router)#timer 4

/* CUSTOMIZATION: Configure VRRP to track an interface. */
Router(config-vrrp-virtual-Router)# track interface GigabitEthernet0/0/0/2 30

/* Commit the configuration */
Router(config-vrrp-virtual-Router)# commit
```

You have successfully configured VRRP for IPv6 networks.

Validation

Use the following commands to validate the configuration.

```
/* Validate the configuration */
Router(config-vrrp-virtual-router)# do show run interface GigabitEthernet 0/0/0/2
Fri Dec  8 14:55:48.378 IST
interface GigabitEthernet0/0/0/2
 ipv6 address 10::1/64
!
-------------------------------------------------------------------------------------------------
Router(config-vrrp-virtual-router)# do show running-config router vrrp
...
router vrrp
 interface GigabitEthernet0/0/0/2
  delay minimum 2 reload 10
  address-family ipv6
   vrrp 50
    priority 254
    preempt delay 15
    timer 4
```

```
    track interface GigabitEthernet0/0/0/2 30
    address linklocal autoconfig
    accept-mode disable
   !
  !
 !
!
```

```
Router(config-vrrp-virtual-router)# do show vrrp ipv6 interface gigabitEthernet 0/0/0/2
Fri Dec  8 14:59:25.547 IST
IPv6 Virtual Routers:
                     A indicates IP address owner
                     | P indicates configured to preempt
                     | |
Interface   vrID Prio A P State    Master addr     VRouter addr
Gi0/0/0/2      50  254   P Master   local
                                                 fe80::200:5eff:fe00:203
```

```
Router(config-vrrp-virtual-router)# end
Router# show vrrp detail
Fri Dec  8 15:08:36.469 IST
GigabitEthernet0/0/0/2 - IPv6 vrID 50
  State is Master
    2 state changes, last state change 00:18:01
    State change history:
    Dec  8 14:50:23.326 IST  Init     -> Backup   Virtual IP configured
    Dec  8 14:50:35.365 IST  Backup   -> Master   Master down timer expired
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is fe80::200:5eff:fe00:203
  Virtual MAC address is 0000.5E00.0203, state is active
  Master router is local

  Advertise time 4 secs
    Master Down Timer 12.031 (3 x 4 + (2 x 4/256))
  Minimum delay 2 sec, reload delay 10 sec
  Current priority 254
    Configured priority 254, may preempt
      minimum delay 15 secs
    Tracked items: 1/1 up: 0 decrement
      Object name                State     Decrement
      GigabitEthernet0/0/0/2        Up             30
```

You have successfully validated VRRP for IPv6 networks.

Clearing VRRP Statistics

Use the **clear vrrp statistics** command to clear all the software counters for the specified virtual router.

SUMMARY STEPS

1. **clear vrrp statistics** [**ipv4** | **ipv6**] [**interface***type interface-path-id* [*vrid*]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**clear vrrp statistics** [**ipv4** | **ipv6**] [**interface***type interface-path-id* [*vrid*]] **Example:** `RP/0/RSP0/CPU0:router# clear vrrp statistics`	Clears all software counters for the specified virtual router. • If no interface is specified, statistics of all virtual routers are removed.

Disabling State Change Logging

Perform this task to disable the task of logging the VRRP state change events via syslog.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **message state disable**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router vrrp`	Enables the VRRP configuration mode.

Step 3	**message state disable**
	Example:
	`RP/0/RSP0/CPU0:router(config-vrrp)# message state disable`
	`RP/0/RSP0/CPU0:router(config-vrrp)#`
		Disables the task of logging the VRRP state change events via syslog.

Step 4	**commit**	

Multiple Group Optimization for Virtual Router Redundancy Protocol

Multiple Group Optimization for Virtual Router Redundancy Protocol (VRRP) provides a solution for reducing control traffic in a deployment consisting of many subinterfaces. By running the VRRP control traffic for just one session, the control traffic is reduced for the subinterfaces with identical redundancy requirements. All other sessions are subordinates of this primary session, and inherit their states from it.

Configuring a VRRP Session Name

Perform this task to configure a VRRP session name.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **vrrp** *group-no*
6. **name** *name*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `RP/0/RSP0/CPU0:router(config)# router vrrp`	EnablesVRRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1`	Enables RP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4`	Enables VRRP address-family configuration mode on a specific interface.

	Command or Action	Purpose
Step 5	**vrrp** *group-no* **Example:** `RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1`	Enables VRRP group configuration mode on a specific interface.
Step 6	**name** *name* **Example:** `RP/0/RSP0/CPU0:router(config-vrrp-vritual-router)# name s1`	Configures a VRRP session name.
Step 7	**commit**	

Configuring the Subordinate Group to Inherit its State from a Specified Group (VRRP)

Perform this task to instruct the subordinate group to inherit its state from a specified group.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **vrrp** *group-no* **slave**
6. **follow** *mgo-session-name*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `Router(config)# router vrrp`	Enables VRRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-vrrp)# interface TenGigE 0/2/0/1`	Enables VRRP interface configuration mode on a specific interface.

	Command or Action	Purpose
Step 4	**address-family ipv4** **Example:** `Router(config-vrrp-if)# address-family ipv4`	Enables VRRP address-family configuration mode on a specific interface.
Step 5	**vrrp** *group-no* **slave** **Example:** `Router(config-vrrp-address-family)# vrrp 2 slave`	Enables VRRP slave configuration mode on a specific interface.
Step 6	**follow** *mgo-session-name* **Example:** `Router(config-vrrp-slave)# follow m1`	Instructs the subordinate group to inherit its state from a specified group.
Step 7	**commit**	

Configuring a Primary Virtual IPv4 Address for a Subordinate Group(VRRP)

Perform this task to configure the primary virtual IPv4 address for the subordinate group.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **vrrp** *group-no* **slave**
6. **address** *ip-address*
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `Router(config)# router vrrp`	Enables VRRP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:**	Enables VRRP interface configuration mode on a specific interface.

	Command or Action	Purpose
	`Router(config-vrrp)# interface TenGigE 0/2/0/1`	
Step 4	**address-family ipv4** **Example:** `Router(config-vrrp-if)# address-family ipv4`	Enables VRRP address-family configuration mode on a specific interface.
Step 5	**vrrp** *group-no* **slave** **Example:** `Router(config-vrrp-address-family)# vrrp 2 slave`	Enables VRRP slave configuration mode on a specific interface.
Step 6	**address** *ip-address* **Example:** `Router(config-vrrp-slave)# address 10.2.3.2`	Configures the primary virtual IPv4 address for the subordinate group.
Step 7	**commit**	

Configuring a Secondary Virtual IPv4 address for the Subordinate Group

Perform this task to configure the secondary virtual IPv4 address for the subordinate group.

SUMMARY STEPS

1. **configure**
2. **router vrrp**
3. **interface** *type interface-path-id*
4. **address-family ipv4**
5. **vrrp** *group-no* **slave**
6. **address** *address* **secondary**
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router vrrp** **Example:** `Router(config)# router vrrp`	Enables VRRP configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type interface-path-id* **Example:** `Router(config-vrrp)# interface TenGigE 0/2/0/1`	Enables VRRP interface configuration mode on a specific interface.
Step 4	**address-family ipv4** **Example:** `Router(config-vrrp-if)# address-family ipv4`	Enables VRRP address-family configuration mode on a specific interface.
Step 5	**vrrp** *group-no* **slave** **Example:** `Router(config-vrrp-address-family)# vrrp 2 slave`	Enables VRRP slave configuration mode on a specific interface.
Step 6	**address** *address* **secondary** **Example:** `Router(config-vrrp-slave)# address 10.20.30.1 secondary`	Configures the secondary virtual IPv4 address for a router.
Step 7	**commit**	

MIB support for VRRP

VRRP enables one or more IP addresses to be assumed by a router when a failure occurs. For example, when IP traffic from a host reaches a failed router because the failed router is the default gateway, the traffic is transparently forwarded by the VRRP router that has assumed control. VRRP does not require configuration of dynamic routing or router discovery protocols on every end host. The VRRP router controlling the IP address(es) associated with a virtual router is called the IP address owner router, and forwards packets sent to these IP addresses. The election process provides dynamic fail over(standby) in the forwarding responsibility should the IP address owner router become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts.The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host. SNMP traps provide information of the state changes, when the virtual routers(in standby) are moved to IP address owner router's state or if the standby router is made IP address owner router.

Configuring SNMP server notifications for VRRP events

The **snmp-server traps vrrp events** command enables the Simple Network Management Protocol (SNMP) server notifications (traps) for VRRP.

SUMMARY STEPS

1. **configure**
2. **snmp-server traps vrrp events**

3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**snmp-server traps vrrp events** **Example:** `RP/0/RSP0/CPU0:router(config)snmp-server traps vrrp events`	Enables the SNMP server notifications for VRRP.
Step 3	**commit**	

VRRP Support on PWHE Interfaces

Pseudowire Headend (PWHE) is a technology that allows termination of access pseudowires (PWs) into a Layer 3 (VRF or global) domain or into a Layer 2 domain. This feature enables you to configure VRRP on PWHE interfaces to provide redundancy between two routers that are connected through PWHE interfaces .

For more information about PWHE interfaces, see the chapter *Implementing Multipoint Layer 2 Services* of the *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

Configuration Example

To configure VRRP on PWHE interfaces, use the following steps:

1. Enter the VRRP configuration mode.
2. Configure a PWHE interface.
3. Configure the VRRP address family for IPv4 and IPv6.

Configuration

```
/* Enter the VRRP configuration mode. */
Router# configure
Router(config)# router vrrp

/* Configure a PWHE interface. */
Router# (config-vrrp)# interface pw-Ether 1000

/* Configure the VRRP address family for IPv4 and IPv6. */
Router(config-vrrp-if)# address-family ipv4 vrrp
Router(config-vrrp-virtual-router)# address 172.16.0.0
Router(config-vrrp-virtual-router)# vrrp 1
Router(config-vrrp-virtual-router)# commit
Router(config-vrrp-address-family)# exit
```

```
Router(config-vrrp-if)# exit
Router(config-vrrp-if)# address-family ipv6 vrrp 1
Router(config-vrrp-virtual-router)# address global 2001:DB8::1
Router(config-vrrp-virtual-router)# address linklocal autoconfig
Router(config-vrrp-virtual-router)# commit
```

Running Configuration

```
router vrrp
 interface PW-Ether1000
  address-family ipv4
   vrrp 1
    address 172.16.0.0
   !
  !
  address-family ipv6
   vrrp 1
    address global 2001:db8::1
    address linklocal autoconfig
   !
```

Verification

Use the following command to verify the configuration of VRRP on PWHE interfaces:

```
Router# show run interface pw-ether 1000
interface PW-Ether1000
ipv4 address 172.16.0.0 255.255.255.0
ipv6 address 2001:DB8::1/125
attach generic-interface-list pwhe_vrrp
!
```

Use the following command to verify the details of VRRP configuration on PWHE interfaces:

```
Router# show vrrp  interface pw-Ether 1000 detail
PW-Ether1000 - IPv4 vrID 1
  State is Backup
    1 state changes, last state change 2d08h
    State change history:
    Nov 24 11:47:16.585 IST  Init
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 172.16.0.0
  Virtual MAC address is 0000.5E00.0101, state is reserved
  Master router is 172.16.0.1, priority 100
  Version is 2
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs

PW-Ether1000 - IPv6 vrID 1
  State is Backup
    1 state changes, last state change 2d08h
    State change history:
    Nov 24 11:47:19.600 IST  Init
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 2001:DB8::1/125
    Secondary Virtual IP address is 2001:DB8:FFFF:FFFF:FFFF:FFFE:FFFF:FFFF
  Virtual MAC address is 0000.5E00.0201, state is reserved
  Master router is 2001:DB8::2
```

```
  Version is 3
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
```

Use the following command to verify VRRP state and priority of the current router:

```
Router# show vrrp  interface pw-Ether 1000
IPv4 Virtual Routers:
                     A indicates IP address owner
                     | P indicates configured to preempt
                     | |
Interface   vrID Prio A P State    Master addr     VRouter addr
PE1000         1  100   P Backup   172.16.0.1       172.16.0.0
IPv6 Virtual Routers:
                     A indicates IP address owner
                     | P indicates configured to preempt
                     | |
Interface   vrID Prio A P State    Master addr                 VRouter addr
PE1000         1  100   P Backup   2001:DB8::2    fe80::200:5eff:fe00:201
```

Hot Restartability for VRRP

In the event of failure of a VRRP process in one group, forced failovers in peer VRRP IP address owner router groups should be prevented. Hot restartability supports warm RP failover without incurring forced failovers to peer VRRP routers.

Configuration Examples for VRRP Implementation on Cisco IOS XR Software

This section provides the following VRRP configuration examples:

Configuring a VRRP Group: Example

This section provides the following configuration example of Router A and Router B, each belonging to three VRRP groups:

Router A:

```
config
interface tenGigE 0/4/0/4
ipv4 address 10.1.0.1/24
exit
router vrrp
interface tenGigE 0/4/0/4
address-family ipv4
vrrp 1 version 2
priority 120
text-authentication cisco
timer 3
```

```
address 10.1.0.10
vrrp 5 version 2
timer 30
address 10.1.0.50
vrrp 100 version 2
preempt disable
address 10.1.0.100
commit
```

Router B:

```
config
interface tenGigE 0/4/0/4
ipv4 address 10.1.0.2/24
exit
router vrrp
interface tenGigE 0/4/0/4
address-family ipv4
vrrp 1 version 2
priority 100
text-authentication cisco
timer 3
address 10.1.0.10
vrrp 5 version 2
priority 200
timer 30
address 10.1.0.50
vrrp 100 version 2
preempt disable
address 10.1.0.100
commit
```

In the configuration example, each group has the following properties:

- Group 1:
  - Virtual IP address is 10.1 .0.10 .
  - Router A will become the IP address owner router for this group with priority 120.
  - Advertising interval is 3 seconds.
  - Advertising interval is 3 seconds .
  - Preemption is enabled.
- Group 5:
  - Router B will become IP address owner router for this group with priority 200.
  - Advertising interval is 30 seconds .
  - Preemption is enabled .
- Group 100:
  - Router configured first becomes IP Address owner router for this group first, because preempt is disabled.
  - Advertising interval is the default 1 second.

- Preemption is disabled .
- Preemption is disabled.

Clearing VRRP Statistics: Example

The **clear vrrp statistics** command produces no output of its own. The command modifies the statistics given by **show vrrp statistics** command so that all the statistics are reset to zero.

The following section provides examples of the output of the **show vrrp statistics** command followed by the **clear vrrp statistics** command:

```
RP/0/RSP0/CPU0:router# show vrrp statistics
show vrrp statistics
Invalid packets:
 Invalid checksum:              0
 Unknown/unsupported versions:  0
 Invalid vrID:                  10
 Too short:                     0
Protocol:
 Transitions to Master          6
Packets:
 Total received:                155
 Bad TTL:                       0
 Failed authentication:         0
 Unknown authentication:        0
 Conflicting authentication:    0
 Unknown Type field:            0
 Conflicting Advertise time:    0
 Conflicting Addresses:         0
 Received with zero priority:   3
 Sent with zero priority:       3


RP/0/RSP0/CPU0:router# clear vrrp statistics
RP/0/RSP0/CPU0:router# show vrrp statistics
Invalid packets:
 Invalid checksum:              0
 Unknown/unsupported versions:  0
 Invalid vrID:                  0
 Too short:                     0
Protocol:
 Transitions to Master          0
Packets:
 Total received:                0
 Bad TTL:                       0
 Failed authentication:         0
 Unknown authentication:        0
 Conflicting authentication:    0
 Unknown Type field:            0
 Conflicting Advertise time:    0
 Conflicting Addresses:         0
 Received with zero priority:   0
 Sent with zero priority:       0
```

Additional References

The following sections provide references related to VRRP.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Quality of Service Commands on Modular Quality of Service Command Reference for Cisco ASR 9000 Series Routers*
Class-based traffic shaping, traffic policing, low-latency queuing, and Modified Deficit Round Robin (MDRR)	*Configuring Modular Quality of Service Congestion Management on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
WRED, RED, and tail drop	*Configuring Modular QoS Congestion Avoidance on Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*
VRRP commands	*VRRP Commands on IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services on System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

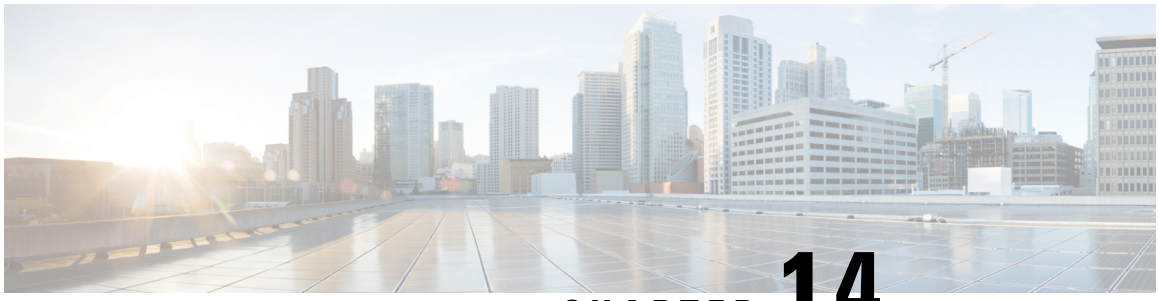
MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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



CHAPTER 14

Configuring Proxy Mobile IPv6 Local Mobility Anchor

Local Mobility Anchor (LMA) acts as the home agent for a mobile node (MN) in a Proxy Mobile IPv6 domain, which is the network where the mobility management of an MN is handled using the Proxy Mobile IPv6 (PMIPv6) protocol. LMA is the topological anchor point for the MN's home network prefix(es) and is the entity that manages the MN's binding state. This module explains how to configure LMA on Cisco ASR 9000 Series Aggregation Services Routers.

Note For a complete description of the PMIPv6 LMA configuration commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Configuring Proxy Mobile IPv6 Local Mobility Anchor on the Cisco ASR 9000 Series Router

Release	Modification
Release 5.2.2	This feature was introduced.
Release 5.3.1	Smart Licensing feature was added.

Information About Proxy Mobile IPv6 Support for LMA Functionality

Proxy Mobile IPv6 Overview

Proxy Mobile IPv6 (PMIPv6) provides network-based IP Mobility management to a mobile node (MN), without requiring the participation of the MN in any IP mobility-related signaling. The mobility entities in the network track the movements of the MN, initiate the mobility signaling, and set up the required routing state.

The major functional entities of PMIPv6 are Mobile Access Gateways (MAGs), Local Mobility Anchors (LMAs), and MNs.

Mobile Access Gateway

A Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links. MAG is the access router for the MN; that is, the MAG is the first-hop router in the localized mobility management infrastructure.

A MAG performs the following functions:

- Obtains an IP address from a Local Mobility Anchor (LMA) and assigns it to an MN
- Tunnels traffic from an MN to LMA

Local Mobility Anchor

Local Mobility Anchor (LMA) is the home agent for a mobile node (MN) in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775 and RFC 5213) along with the capabilities required for supporting the PMIPv6 protocol.

The LMA retains and shares the IP address of an MN when the MN roams across MAGs.

Smart Licensing for PMIPv6 LMA

Smart Licensing method of licensing is available for PMIPv6 LMA on the Cisco ASR 9000 Series Aggregation Services Routers. The licensing mode is soft-enforced mode. The licensing string available is A9K-SESSION-128K with maximum supported scale of 128K LMA bindings.

For more information about Smart Licensing, see *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*.

Mobile Node

A mobile node (MN) is an IP host whose mobility is managed by the network. An MN can be an IPv4-only node, an IPv6-only node, or a dual-stack node, which is a node with IPv4 and IPv6 protocol stacks. An MN

is not required to participate in any IP mobility-related signaling for achieving mobility for an IP address or a prefix that is obtained in the Proxy Mobile IPv6 (PMIPv6) domain.

How to Configure Proxy Mobile IPv6 LMA

This section contains the following tasks:

Configuring a Proxy Mobile IPv6 LMA Domain

This task enables you to configure Proxy Mobile IPv6 LMA domain:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-domain** *domain-name*
3. **auth-option spi** *hex-value* **key ascii** *string*
4. **nai** *[user]@realm*
5. **network** *network-identifier*
6. **service { ipv4 | ipv6 | dual }**
7. (Optional) **customer** *customer-name*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-domain cisco.com`	Configures a PMIPv6 domain and enters PMIPv6 domain configuration mode.
Step 3	**auth-option spi** *hex-value* **key ascii** *string* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain)# auth-option spi 67 key ascii key1`	Configures the authentication option to all MAGs in the domain that includes an SPI value specified in hexadecimal format and a shared secret key which is specified as an ASCII string.
Step 4	**nai** *[user]@realm* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain)# nai`	Configures a network access identifier (NAI) of the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain MN configuration mode. The NAI must be of form *username@realm* or just *@realm*

	Command or Action	Purpose
	`example@cisco.com`	
Step 5	**network** *network-identifier* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# network network2`	Corresponds to a network configured under LMA comprising of an IPv4 and IPv6 address/prefix pool. The Mobile Node (MN) is assigned HoA or HNP from this network. Associates a network with the LMA under which an IPv4 or IPv6 pool can be enabled.
Step 6	**service { ipv4 | ipv6 | dual }** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# service dual`	Configures the service provided to the MN within the PMIPv6 domain.
Step 7	(Optional) **customer** *customer-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# customer CUST1`	(Optional) Configures the name of the customer to which this NAI belongs. The customer is configured during LMA Mobile Local Loop service configuration as described in Configuring VRF Aware LMA, on page 387.
Step 8	**commit**	

Example: Configuring a Proxy Mobile IPv6 LMA Domain

This example shows sample configuration of PMIPv6 LMA domain:

```
ipv6 mobile pmipv6-domain cisco.com
 !
 auth-option spi 67 key ascii key1
 nai example@cisco
  network network2
 !
 nai example@ctc
  network network3
  service dual
  customer CUST1
 !
!
```

Configuring Proxy Mobile IPv6 LMA with Peer MAG

This task lists detailed configuration steps for configuring Proxy Mobile IPv6 LMA with dynamic MAG learning:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **address { ipv4 | ipv6 }** *address*

4. **hnp maximum** *number*
5. **bce maximum** *number*
6. **bce lifetime** *seconds*
7. **bce delete-wait-time** *milliseconds*
8. **replay-protection timestamp window** *seconds*
9. **default profile** *profile-name*
10. **bri delay { min | max }** *milliseconds*
11. **bri retries** *count*
12. **aaa accounting [interim** *interim-interval* **]**
13. **mag** *mag-identifier domain-name*
14. Execute one of these:
    - **ipv4 address** *address*
    - **ipv6 address** *address*
15. **auth-option spi** *hex-value* **key ascii** *value*
16. **encap {gre-ipv4 | gre-ipv6 }**
17. **tunnel interface** *interface-type node-id*
18. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-lma lma1 domain cisco.com`	Enables the LMA service on the router, configures the PMIP domain for the LMA, and enters LMA configuration mode.
Step 3	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# address ipv6 2001:DB8::1`	Configures an IPv4 or IPv6 address for the LMA.
Step 4	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.

	Command or Action	Purpose
Step 5	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.
Step 6	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.
Step 7	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.
Step 8	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# replay-protection timestamp window 18`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this configured value, then the PBU is rejected with status code 156.
Step 9	**default profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# default profile profile1`	Enables the default profile for the MN.

Step 10	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

Step 11	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.

	Command or Action	Purpose
Step 12	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server. There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting.
Step 13	**mag** *mag-identifier domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# mag mag1 dn1`	Configures the MAG for the LMA and enters LMA-MAG configuration mode.

Step 14	Execute one of these:
	• **ipv4 address** *address*
	• **ipv6 address** *address*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# ipv4 address 192.168.0.4`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# ipv6 address 2004:DC5::2`
		Configures an IPv4 address for the LMA in case the transport between the MAG and the LMA is IPv4.
		Configures an IPv6 address for the LMA in case the transport between the MAG and the LMA is IPv6.

Step 15	**auth-option spi** *hex-value* **key ascii** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# auth-option spi 87E key ascii key2`	Configures authentication for the LMA within the MAG.
Step 16	**encap {gre-ipv4 | gre-ipv6 }** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# encap gre-ipv6`	Configures a tunnel encapsulation mode type between the MAG and the LMA.
Step 17	**tunnel interface** *interface-type node-id* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# tunnel interface tunnel-ip 097`	Configures a static GRE tunnel to peering MAG. This step is required since GRE tunnel cannot be created dynamically.
Step 18	**commit**	

Example: Configuring Proxy Mobile IPv6 LMA with Peer MAG

This example shows sample configuration of Proxy Mobile IPv6 LMA with Peer MAG:

```
ipv6 mobile pmipv6-lma lma1 domain cisco.com
 address ipv6 2001:DB8::1
 hnp maximum 2
 bce maximum 2500
 bce lifetime 2500
 bce delete-wait-time 100
 replay-protection timestamp window 18
 default profile profile1
 aaa accounting interim 2
 !
 mag mag1 dn1
  ipv4 address 192.168.0.4
  auth-option spi 87E key ascii key2
  encap gre-ipv6
  tunnel interface tunnel-ip 097
 !
!
```

Configuring Proxy Mobile IPv6 LMA with Dynamic MAG Learning

This task lists detailed configuration steps for configuring Proxy Mobile IPv6 LMA with dynamic MAG learning:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **address { ipv4 | ipv6 }** *address*
4. **hnp maximum** *number*
5. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
6. **bce maximum** *number*
7. **bce lifetime** *seconds*
8. **bce delete-wait-time** *milliseconds*
9. **replay-protection timestamp window** *seconds*
10. **default profile** *profile-name*
11. **bri delay { min | max }** *milliseconds*
12. **bri retries** *count*
13. **dynamic mag learning**
14. **aaa accounting [interim** *interim-interval* **]**
15. **network** *network-name*
16. **pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]**
17. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-lma lma1 domain cisco.com`	Enables the LMA service on the router, configures the PMIPv6 domain for the LMA, and enters LMA configuration mode.
Step 3	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# address ipv6 2001:DB8::1`	Configures an IPv4 or IPv6 address for the LMA.
Step 4	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.
Step 5	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# heartbeat interval 100 retries 5 timeout 10`	Configures global LMA heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out.
Step 6	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.
Step 7	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.

	Command or Action	Purpose
Step 8	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.
Step 9	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# replay-protection timestamp window 18`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this configured value, then the PBU is rejected with status code 156.
Step 10	**default profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# default profile profile1`	Enables the default profile for the MN.

Step 11	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

Step 12	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.
Step 13	**dynamic mag learning** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dynamic mag learning`	Enables an LMA to accept Proxy Mobile IPv6 (PMIPv6) signaling messages from any Mobile Access Gateway (MAG) that is not locally configured.
Step 14	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server.

	Command or Action	Purpose
		There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting.
Step 15	**network** *network-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# network network1`	Configures the network that comprises of one or more pools from which the LMA assigns IP addresses to the Mobile Nodes.
Step 16	**pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-network)# pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8`	Configures the IPv4 or IPv6 address pool from which LMA assigns IP addresses to the mobile nodes.
Step 17	**commit**	

Example: Configuring Proxy Mobile IPv6 LMA with Dynamic MAG Learning

This example shows sample configuration of Proxy Mobile IPv6 LMA with dynamic MAG learning:

```
ipv6 mobile pmipv6-lma lma1 domain cisco.com
 address ipv6 2001:DB8::1
 hnp maximum 2
 heartbeat interval 100 retries 5 timeout 10
 bce maximum 2500
 bce lifetime 2500
 bce delete-wait-time 100
 replay-protection timestamp window 18
 default profile profile1
 dynamic mag learning
 aaa accounting interim 2
 network network1
  pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8
  pool mobile-node ipv6 start-address 2002:10::1 pool-prefix 62
 !
!
```

VRF Aware LMA

This section contains the following topics:

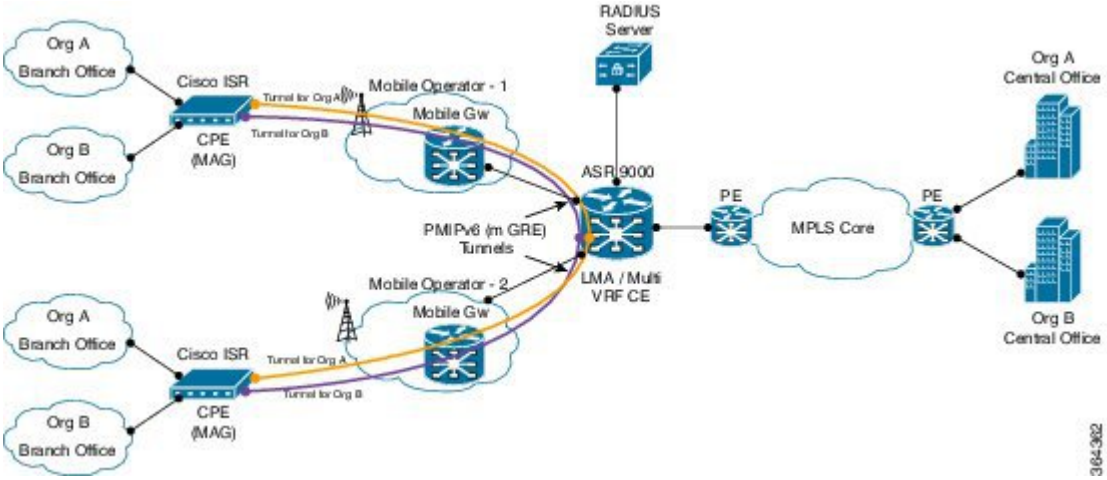
VRF Aware LMA Solution

Local Mobility Anchor (LMA) supports VRF awareness on Cisco ASR 9000 Series Aggregation Services Routers. This feature includes the following capabilities:

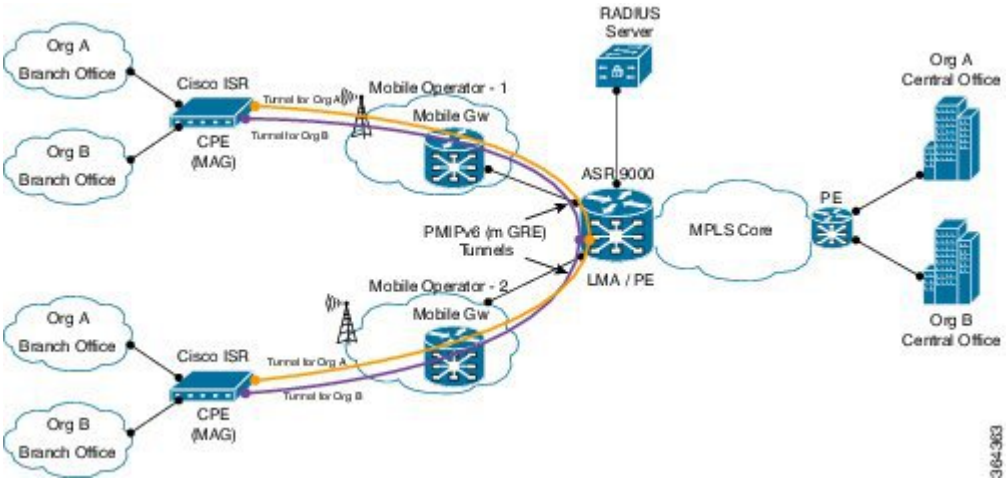
- Awareness of multiple customers belonging to different VRFs
- Peer with multiple mobile operators for transport towards the Customer Premises Equipment (CPE)/Mobile Access Gateway (MAG) devices in separate peering or transport VRFs
- AAA accounting for Mobile Nodes and tunnels

Topology

The following figure is a sample topology of Mobile Local Loop service hosted on Multiprotocol Label Switching (MPLS) multi-VRF Customer Edge (CE) routers:



The following figure is a sample topology of Mobile Local Loop service hosted on MPLS Provider Edge (PE) routers:



In these diagrams:

- Mobile Local Loop (MLL) service allows enterprises Org A and Org B to securely link their remote small branch offices over mobile networks of Mobile Operator 1 and 2 without the need for dedicated leased lines or IP Security (IPSec) VPN cloud. The topologies are examples of MLL service deployment. The service uses Proxy Mobile IPv6 (PMIPv6) based overlay transport.
- At the branch office, CPE/MAG devices such as Cisco ISR series routers are equipped with Cisco HWIC (High-Speed WAN Interface Card) 3G/4G service modules. These devices are used for IP connectivity and setting up overlay transport for service access.
- MLL service provider hosts the LMA function of PMIPv6 and the MLL service on Cisco ASR 9000 series routers which could either be MPLS Provider Edge (PE) routers or MPLS Multi-VRF Customer Edge (CE) routers. LMA can peer with multiple mobile operators (such as Mobile Operators 1 and 2) to enable service access to CPE/MAG devices that can have connectivity to the mobile operators.
- If accounting is enabled, LMA sends accounting records to AAA server with service usage counters.

Configuring VRF Aware LMA

Perform the following steps to configure VRF aware Proxy Mobile IPv6 LMA:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **hnp maximum** *number*
4. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
5. **bce maximum** *number*
6. **bce lifetime** *seconds*
7. **bce delete-wait-time** *milliseconds*
8. **replay-protection timestamp window** *seconds*
9. **bri delay { min | max }** *milliseconds*
10. **bri retries** *count*
11. **dynamic mag learning**
12. **aaa accounting [interim** *interim-interval* **]**
13. **dscp control-plane** *dscp-value* **[force]**
14. **mobility-service mobile-local-loop**
15. **customer** *customer-name* **vrf** *vrf-name*
16. **auth-option spi** *hex-value* **key ascii** *value*
17. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
18. **bce lifetime** *seconds*
19. **network** { **unauthorized | authorized** *network-name* }
20. **pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]**
21. **transport** [**vrf** *vrf-name*]
22. **address { ipv4 | ipv6 }** *address*
23. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-lma lma1 domain cisco.com`	Enables the LMA service on the router, configures the PMIPv6 domain for the LMA, and enters LMA configuration mode.
Step 3	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.
Step 4	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# heartbeat interval 100 retries 5 timeout 10`	Configures global LMA heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out.
Step 5	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.
Step 6	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.
Step 7	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.

	Command or Action	Purpose
Step 8	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# replay-protection timestamp window 18`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this configured value, then the PBU is rejected with status code 156.

Step 9	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

Step 10	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.
Step 11	**dynamic mag learning** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dynamic mag learning`	Enables an LMA to accept Proxy Mobile IPv6 (PMIPv6) signaling messages from any Mobile Access Gateway (MAG) that is not locally configured.
Step 12	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If the **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server. There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting. For information about AAA/RADIUS configuration for accounting, see the *Authentication, Authorization, and Accounting Commands* chapter in Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference.
Step 13	**dscp control-plane** *dscp-value* **[force]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dscp control-plane 45`	Configures the value of Differentiated Services Code Point (DSCP) in the outgoing PMIPv6 control plane messages. The outgoing packets include locally generated packets such as Proxy Binding Revocation Indications (PBRIs), Proxy Binding Revocation Acknowledgments (PBRAs), Heartbeat Requests, and packets sent in response to packets

	Command or Action	Purpose
		received from MAG such as Proxy Binding Acknowledgments (PBAs), PBRIs, PBRAs, and Heartbeat Responses. If *dscp-value* is not specified, then the DSCP received in a request is used in the outgoing response packet. DSCP is not set in the other outgoing packets. If *dscp-value* is specified without the **force** option: • The configured DSCP value is set in locally generated packets. • If the received packet does not have DSCP marking, the configured value is set in the outgoing packet. • If the received packet has DSCP marking that matches the configured value, then the DSCP received is set in the outgoing response packet. • If the received packet has DSCP marking that does not match the configured value, then the DSCP received is used in the outgoing response packet. If *dscp-value* is specified with the **force** option, then the configured DSCP value is set in all outgoing packets.
Step 14	**mobility-service mobile-local-loop** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# mobility-service mobile-local-loop`	Configures Mobile Loop Local (MLL) service on the LMA and enters the service configuration mode.
Step 15	**customer** *customer-name* **vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll)# customer CUST1 vrf VRF1`	Configures the name and the VRF of a customer. The command enters the customer configuration mode where other parameters of the customer are configured. Use the **no** form of this command to remove an existing customer. There can be many customers, however no two customers can be configured with the same VRF.
Step 16	**auth-option spi** *hex-value* **key ascii** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# auth-option spi 87E key ascii KEY1`	Configures customer-specific authentication for the LMA within the MLL. The authentication option includes an SPI value specified in hexadecimal format and a shared secret key which is specified as an ASCII string. This configuration overrides the global **auth-option** configuration in the PMIPv6 LMA Domain.
Step 17	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:**	Configures customer-specific heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# heartbeat interval 30 retries 10 timeout 10`	path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out. This configuration overrides the global LMA heartbeat configuration.
Step 18	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# bce lifetime 1500`	Configures customer-specific permitted lifetime of binding cache entries (BCEs) in seconds. This configuration overrides the global LMA BCE configuration.
Step 19	**network** { **unauthorized | authorized** *network-name* } **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# network authorized NETW1`	Configures customer-specific network. Use the **unauthorized** keyword to configure an unauthorized network. In this case, no network pools are configured for address assignment. The address/prefix of the Logical Mobile Node (LMN) on the MAG and the network prefixes on the Mobile Network interfaces are accepted as received in the Proxy Binding Update (PBU). Use the **authorized** keyword to configure a named network. In this case, the address/prefix of the LMN and Mobile Network prefixes are validated against the configured network pool. The uniqueness of the named network is ensured. Use the **no** form of this command to remove an existing network.
Step 20	**pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust-network)# pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8`	Perform this step only if you have configured a named network in the previous step using the **network authorized** command. Configures the IPv4 or IPv6 address pool(s) from which LMA assigns IP addresses to the mobile nodes. The pool is characterized by whether it is for Mobile Nodes or Mobile Networks for the customer, whether it is for IPv4 or IPv6 address family, the start address of the pool, the pool prefix and the network prefix of the pool.
Step 21	**transport** [**vrf** *vrf-name*] **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# transport vrf TVRF1`	Configures customer's transport options. They include peering or transport VRF and the LMA IPv4 and/or IPv6 addresses. The addresses are configured in the transport configuration mode using the **address** command. A customer can have multiple transports and can have the same addresses in all transports. However, each customer must have a unique IPv4 and/or a unique IPv6 address. **Note** If the transport is in global VRF, then VRF and *vrf-name* can be omitted in this command.

	Command or Action	Purpose
Step 22	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust-tpt)# address ipv6 2001:DB8::1`	Configures customer-specific LMA IPv4 and/or IPv6 addresses. There can only be two instances of addresses, one for IPv4 and one for IPv6.
Step 23	**commit**	

Example: Configuring VRF Aware LMA in a MLL

This example shows sample configuration of VRF aware LMA in a MLL:

```
/* Domain Configuration */

ipv6 mobile pmipv6-domain D1
 lma LMA
 !
 nai @CUST1
  lma LMA
  network CUST1
  service dual
  customer CUST1
 !
 nai @CUST2
  lma LMA
  network CUST2
  service dual
  customer CUST2
 !
!


/* AAA/RADIUS configuration for accounting */

radius-server host 10.10.10.2 auth-port 1645 acct-port 1646
 key 7 094F471A1A0A
!
aaa accounting mobile default group radius


/* LMA Configuration */

ipv6 mobile pmipv6-lma LMA domain D1
 aaa accounting interim 2
 bce maximum 128000
 dscp control-plane 45
 dynamic mag learning
 mobility-service mobile-local-loop
  customer CUST1 vrf VRF1
   bce lifetime 300
   network unauthorized
   heartbeat interval 30 retries 10 timeout 10
   auth-option spi 100 key ascii xyz123
   transport vrf CUSTSP
    address ipv4 15.15.15.2
```

```
    address ipv6 2002:15::2
   !
  !
  customer CUST2 vrf VRF2
   network authorized CUST2
   pool mobile-node ipv4 start-address 10.10.10.1 pool-prefix 24
   pool mobile-node ipv6 start-address 2002:10:10:1::1 pool-prefix 48
   pool mobile-network ipv4 start-address 20.20.20.1 pool-prefix 24 network-prefix 28
   pool mobile-network ipv6 start-address 2002:20:0:1::1 pool-prefix 40 network-prefix 64
   !
   transport vrf CUSTSP
    address ipv4 16.16.16.2
    address ipv6 2002:16::2
   !
  !
 !
!
```

Additional References

The following sections provide references related to PMIPv6 LMA

Related Documents

Related Topic	Document Title
PMIPv6 LMA commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Proxy Mobile IPv6 Local Mobility Anchor Commands IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Standards and RFCs

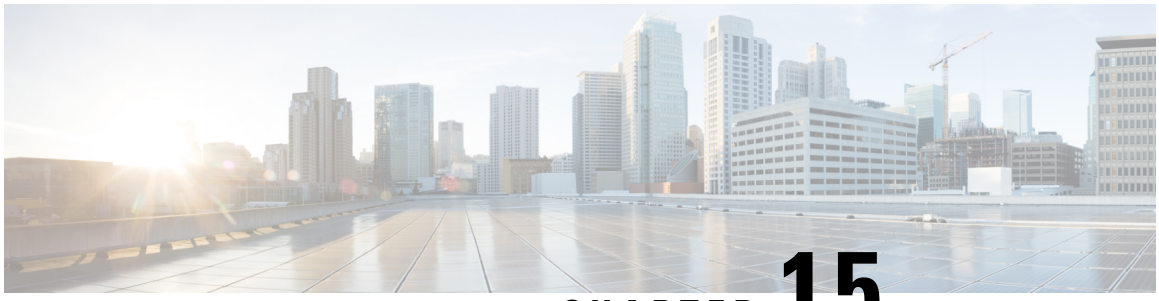
Standard/RFC	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
-	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



CHAPTER 15

Configuring Transports

This module provides information about Nonstop Routing (NSR), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) transports on Cisco ASR 9000 Series Aggregation Services Routers .

If you have specific requirements and need to adjust the NSR, TCP, or UDP values, refer to the *Transport Stack Commands on IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Note For a complete description of the transport configuration commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Configuring NSR, TCP, UDP, and UDP RAW Transports on the Cisco ASR 9000 Series Router

Release	Modification
Release 3.7.2	This feature was introduced.
Release 6.3.3	XIPC Queue Drop Detection and Correction feature was introduced for TCP.

Prerequisites for Configuring NSR, TCP, UDP, Transports

The following prerequisites are required to implement NSR, TCP, UDP, Transports:

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Configuring NSR, TCP, UDP Transports

To configure NSR, TCP, and UDP transports, you must understand the following concepts:

NSR Overview

Nonstop Routing (NSR) is provided for Open Shortest Path First (OSPF) and Label Distribution Protocol (LDP) protocols for the following events:

- Route Processor (RP) failover
- Process restart for either OSPF, LDP, or TCP
- In-service software upgrades (ISSU)

In the case of the RP failover, NSR is achieved by for both TCP and the applications (OSPF or LDP).

NSR is a method to achieve High Availability (HA) of the routing protocols. TCP connections and the routing protocol sessions are migrated from the active RP to standby RP after the RP failover without letting the peers know about the failover. Currently, the sessions terminate and the protocols running on the standby RP reestablish the sessions after the standby RP goes active. Graceful Restart (GR) extensions are used in place of NSR to prevent traffic loss during an RP failover but GR has several drawbacks.

You can use the **nsr process-failures switchover** command to let the RP failover be used as a recovery action when the active TCP or active LDP restarts. When standby TCP or LDP restarts, only the NSR capability is lost till the standby instances come up and the sessions are resynchronized but the sessions do not go down. In the case of the process failure of an active OSPF, a fault-management policy is used. For more information, refer to *Implementing OSPF on Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

TCP Overview

TCP is a connection-oriented protocol that specifies the format of data and acknowledgments that two computer systems exchange to transfer data. TCP also specifies the procedures the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently, because it handles all demultiplexing of the incoming traffic among the application programs.

Any IP protocol other than TCP or UDP is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

UDP Overview

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol that belongs to the IP family. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and TFTP.

Any IP protocol other than TCP, UDP, is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

During external port scanning on ports 19 and 20, the UDP packets dropped by Nmap tool without sending an ICMP response, cause uncertainty in identifying the true state of the ports. The port states can be open, closed, or filtered.

Due to no response from the target system, the port states might misclassify as open instead of a closed or filtered state, and can lead to a false-positive situation.

Table 14: UDP port availability for Applications

Platform	Start of Range	End of Range	Availability
Cisco IOS XR 64-bit Operating System	15000	57344	Available
Cisco IOS XR 64-bit Operating System	57345	65535	Reserved
Cisco IOS XR 32-bit Operating System	15000	65535	Available

How to Configure Failover as a Recovery Action for NSR

This section contains the following procedure:

Configuring Failover as a Recovery Action for NSR

This task allows you to configure failover as a recovery action to process failures of active instances.

When the active TCP or the NSR client of the active TCP terminates or restarts, the TCP sessions go down. To continue to provide NSR, failover is configured as a recovery action. If failover is configured, a switchover is initiated if the active TCP or an active application (for example, LDP, OSPF, and so forth) restarts or terminates.

For information on how to configure MPLS Label Distribution Protocol (LDP) for NSR, refer to the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*.

For information on how to configure NSR on a per-process level for each OSPF process, refer to the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Note Before performing this procedure, enable RP isolation using the **isolation enable** command for improved troubleshooting. Without enabling RP isolation, the failing process will not generate the logs required to find the root cause of the failure.

SUMMARY STEPS

1. **configure**
2. nsr process-failures switchover
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	nsr process-failures switchover **Example:** `RP/0/RSP0/CPU0:router(config)# nsr process-failures switchover`	Configures failover as a recovery action for active instances to switch over to a standby route processor (RP) to maintain nonstop routing (NSR.
Step 3	**commit**	

XIPC Tail Drop Detection and Correction for TCP

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Extended IPC (XIPC) Tail drop is one of the more commonly used congestion avoidance mechanisms. Tail drop treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

This feature introduces XIPC as a new policer, and culprit session falls into this bucket and is policed heavily. This feature improves the serviceability of the XIPC queues owned by TCP. To perform this, the TCP monitors and identifies the sessions that are receiving more data. TCP revisits the statistics at regular intervals, and based on the data, it decides whether the sessions need to be policed or added to default policer rate. Therefore, other sessions are given a fair chance to use the XIPC queue, and high-data sessions are throttled down at hardware.

To detect the culprit session, TCP internal queue size is considered along with rate-limit. If the overall queue size reaches the threshold value and per session rate-limit value is exceeded then the culprit sessions in that queue are detected.

After applying the dynamic policer, culprit sessions may flap. As per the TCP dumpfiles and logs, this is an expected behavior. If a culprit BGP session has aggressive timers (KA 3 sec and Hold timer 9 sec), even then the sessions may flap and we may not verify the LPTS packet drops using the **show lpts** commands.

TCP Configurations to Enable XIPC Tail Drop

The following configuration enables XIPC tail drop on TCP:

```
RP/0/0/CPU0:Router (config)# tcp num-thread Ingress-threads-TCP max-threads
RP/0/0/CPU0:Router (config)# pak-rate tcp stats-start [rate-limit packet rate | max-pkt-size
 max-pkt-size-value max-pak-rate max-pak-rate-value]
```

Verification

The following example displays the statistics of TCP packet rate.

```
RP/0/RSP0/CPU0:Router# show tcp pak-rate stats

       PR -  Number of packets in 30 sec (display, if more than Rate-limit)
       MPR - Maximum size packets in 30 sec (display, if more than Maximum packet rate)

         Time         Foreign Address    Local Address     VRF          PR        MPR
-------------------------------------------------------------------------------------------

 Nov 19 15:56:08.464   6.6.13.7:179       6.6.13.6:23898    0x60000000  18767      1502
 Nov 19 15:56:08.464   6.6.1.7:46922      6.6.1.6:179       0x60000000  107802     8932
```

Note

- These are the culprit session information and applied LPTS dynamic policer on these sessions.
- Using default BGP timers (60 sec KA and 180 sec hold timer expiry) and show commands, we can observe the number of packets received in the last 30 sec.
- After applying policer, if the number of packets received are less than the configured packet rate, after 85 sec, above details will be removed from the show command.

The following example verifies the sessions statistics at XIPC policer-index level and per-session level.

```
RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                    Accept Drop
XIPC  97  Local  1000  9600   3912960      368661   01234567

RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                    Accept Drop
  XIPC  97  Local  1000  9600      0          0       01234567
```

Note Statistics are cleared when last session under this policer index is removed.

The following example verifies the sessions statistics at XIPC policer and also provides the entries present in the hardware.

```
 RP/0/RSP0/CPU0:Router# show lpts pifib hardware entry statistics location 0/3/cpu0 | i
6.6.1.7,
                                                        Accept/Drop
1754   IPV4 default     TCP    any       LU(30)     4021290/456698  any, 179 6.6.1.7,
46922
2584   IPV4 default     TCP    any       LU(30)       0/0           any, 179 6.6.1.7,
any
```

Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

Related Topic	Document Title
the Cisco ASR 9000 Series Router Transport Stack commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Transport Stack Commands in the IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*MPLS Label Distribution Protocol Commands in the MPLS Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router OSPF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*OSPF Commands in the Routing Command Reference for Cisco ASR 9000 Series Routers*
MPLS Label Distribution Protocol feature information	*Implementing MPLS Label Distribution Protocol in the MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
OSPF feature information	*Implementing OSPF in the Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

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

MIBs

MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	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 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

TCP Dump File Converter

Table 15: Feature History Table

Feature Name	Release Information	Feature Description
TCP Dump File Converter	Release 24.2.1	You can now convert an entire TCP dump of packet traces in binary files into readable formats such as text or cap, which makes it easier to analyze them for troubleshooting using third-party or open-source tools. This feature saves time and effort by preventing the need to examine each packet for failure. This feature introduces the **tcp dump-file convert** command.

TCP dump file converter is a tool that converts tcp ios-xr dump-files in binary format to user-friendly format such as pcap or text.

It proves especially useful when you disable Non-Stop Routing (NSR) or experience a session flap on your router. During such incidents, by default, the tcp process running on the router promptly stores the latest 200 packet traces in binary format within a temporary folder.

TCPdump packet traces also includes data about the configured routing protocols and the overall network traffic traversing your system. This data equips you with the necessary insights to identify and resolve issues within your network infrastructure, facilitating proactive network troubleshooting.

You can view the packet traces binary files in the user-readable format using the following methods:

- You can use the **show tcp dump-file <binary filename>** command to view each binary file in text format manually. For more information, refer to View Binary Files in Text Format Manually, on page 402.

  This process consumes much time, as you have to view each file manually one after another.

- From Release 24.2.1, you can convert all stored packet traces in binary files into a user-readable format such as pcap, text, or both using the **tcp dump-file convert** command. For more information, refer to Convert Binary Files to Readable Format Using TCP Dump File Converter, on page 403.

  This active approach greatly improves the efficiency and ease of packet analysis during network troubleshooting.

Limitations and Restrictions for TCP Dump File Converter

- Routers only store the most recent 200 message exchanges that occurred right before the session termination, when NSR is disabled, or during a session flap.
- You can view only one binary file in text format using the **show tcp dump-file <binary filename>** command.
- When the NSR is disabled, the tcp dump files are stored only for major protocols like border gateway protocol (BGP), multicast source discovery protocol (MSDP), and multiprotocol label switching label distribution protocol (MPLS LDP).

View Binary Files in Text Format Manually

Perform the following steps to view each packet traces binary file in text format without using the TCP dump file converter:

Procedure

Step 1 View the list of packet traces in binary files stored in the tcpdump folder using the **show tcp dump-file list all** command.

Example:

```
Router# show tcp dump-file list all
total 1176
-rw-r--r-- 1 root root 5927 Nov 22 12:42 31_0_0_126.179.20966.cl.1700656933
-rw-r--r-- 1 root root 5892 Nov 22 12:42 31_0_0_127.179.35234.cl.1700656933
-rw-r--r-- 1 root root 6148 Nov 22 12:42 31_0_0_149.179.54939.cl.1700656933
-rw-r--r-- 1 root root 5894 Nov 22 12:42 31_0_0_155.179.18134.cl.1700656933
-rw-r--r-- 1 root root 6063 Nov 22 12:42 31_0_0_156.179.25445.cl.1700656933
-rw-r--r-- 1 root root 5860 Nov 22 12:42 31_0_0_161.179.30859.cl.1700656933
-rw-r--r-- 1 root root 5832 Nov 22 12:42 31_0_0_173.179.36935.cl.1700656933
-rw-r--r-- 1 root root 5906 Nov 22 12:42 31_0_0_190.179.25642.cl.1700656933
```

Step 2 View each packet traces binary file in text format using the **show tcp dump-file <binary filename>** command.

Example:

```
Router# show tcp dump-file 10_106_0_73.179.34849.cl.1707424077 location 0/RP0/CPU0
Filename: 10_106_0_73.179.34849.cl.1707424077

============================================================
Connection state is CLOSED, I/O status: 0, socket status: 103
PCB 0x00007f86bc05e3b8, SO 0x7f86bc05e648, TCPCB 0x7f86bc0c3718, vrfid 0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 1, Hash index: 1593
Local host: 10.106.0.72, Local port: 179 (Local App PID: 11354)
Foreign host: 10.106.0.73, Foreign port: 34849
(Local App PID/instance/SPL_APP_ID: 11354/1/0)

Current send queue size in bytes: 0 (max 0)
Current receive queue size in bytes: 0 (max 0)  mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 0)

Timer          Starts    Wakeups         Next(msec)
Retrans        103448          8               0
SendWnd             0          0               0
TimeWait            1          0               0
AckHold        106815     106545               0
```

```
KeepAlive           1          0               0
PmtuAger            0          0               0
GiveUp              0          0               0
Throttle            0          0               0
FirstSyn            0          0               0

   iss: 161240548   snduna: 163206936   sndnxt: 163206936
sndmax: 163206936   sndwnd: 63104       sndcwnd: 18120
   irs: 3691232436  rcvnxt: 3693473072  rcvwnd: 26099   rcvadv: 3693499171
```

The above sample displays only a part of the actual output; the actual output displays more details.

Convert Binary Files to Readable Format Using TCP Dump File Converter

Perform the following steps to convert the tcp dump packet traces in binary files into pcap and text formats:

Procedure

Step 1 Execute the **tcp dump-file convert all-formats all** command to convert the tcp dump packet traces in binary files into pcap and text formats.

Example:

```
Router# tcp dump-file convert all-formats all
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_40.154838.pcap
[OK]
```

By default, the router stored the converted files in the "decoded_dumpfiles" folder on the "hard disk".

Using the **location node-id** and **file <file path>** keywords, you can save the converted TCP dump file to your desired location.

For example, **tcp dump-file convert all-formats all location** *0/RP0/CPU0* **file** */harddisk:/demo2*.

For more information, refer to *System Management Command Reference for Cisco NCS 5500 Series Routers tcp dump-file convert* command.

```
Router# tcp dump-file convert all-formats all location 0/RP0/CPU0 file /harddisk:/demo2
ascii file is saved at : /harddisk:/demo2.txt
pcap file is saved at : /harddisk:/demo2.pcap
[OK]
```

Step 2 To view the converted text file in the CLI, use the **run cat <text file path>** command.

Example:

```
Router# run cat
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
Filename: 2024_3_19_10_8_53.462070

============================================================
Connection state is CLOSED, I/O status: 0, socket status: 103
PCB 0x0000000000f47a80, SO 0xf476d0, TCPCB 0xf6a370, vrfid 0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 255, Hash index: 563
Local host: 14:11:11::1, Local port: 47743 (Local App PID: 19579)
Foreign host: 14:11:11::2, Foreign port: 179
```

```
(Local App PID/instance/SPL_APP_ID: 19579/1/0)

Current send queue size in bytes: 0 (max 0)
Current receive queue size in bytes: 0 (max 0)  mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 0)

Timer          Starts    Wakeups         Next(msec)
Retrans            70          2                0
SendWnd             0          0                0
TimeWait            2          0                0
AckHold            66         61                0
KeepAlive           1          0                0
PmtuAger            0          0                0
GiveUp              0          0                0
Throttle            0          0                0
FirstSyn            1          1                0

   iss: 3113104891  snduna: 3113106213  sndnxt: 3113106213
sndmax: 3113106213  sndwnd: 31523       sndcwnd: 2832
   irs: 4250126727  rcvnxt: 4250128049  rcvwnd: 31448   rcvadv: 4250159497
```

The above sample displays only a part of the actual output; the actual output displays more details.

Step 3 Use remote file copy commands like **scp** from your lab server to copy the converted packet traces from the router to your local computer and view the converted pcap file.