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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2012 Cisco Systems, Inc. All rights reserved.
CHAPTER 4
Implementing the Dynamic Host Configuration Protocol 89
  Prerequisites for Configuring DHCP Relay Agent 90
  Information About DHCP Relay Agent 90
  How to Configure and Enable DHCP Relay Agent 91
    Configuring and Enabling the DHCP Relay Agent 91
      Configuring a DHCP Relay Profile 91
    Configuring the DHCPv6 (Stateless) Relay Agent 92
    Enabling DHCP Relay Agent on an Interface 93
    Disabling DHCP Relay on an Interface 94
    Enabling DHCP Relay on a VRF 95
    Configuring the Relay Agent Information Feature 95
    Configuring Relay Agent Giaddr Policy 97
  Configuring a DHCP Proxy Profile 98
  DHCPv4 Client 99
    Enabling DHCP Client on an Interface 100
  DHCPv6 Relay Agent Notification for Prefix Delegation 101
    Configuring DHCPv6 Stateful Relay Agent for Prefix Delegation 101
CHAPTER 5 Implementing Host Services and Applications

Prerequisites for Implementing Host Services and Applications

Information About Implementing Host Services and Applications

Network Connectivity Tools

Ping
Traceroute

Domain Services
TFTP Server
File Transfer Services
RCP

Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide, Release 4.2.x
FTP 120
TFTP 120
Cisco inetd 120
Telnet 120

How to Implement Host Services and Applications 120
Checking Network Connectivity 121
Checking Network Connectivity for Multiple Destinations 121
Checking Packet Routes 122
Configuring Domain Services 123
Configuring a Router as a TFTP Server 124
Configuring a Router to Use `r`p Connections 125
Configuring a Router to Use FTP Connections 126
Configuring a Router to Use TFTP Connections 128
Configuring Telnet Services 129
Configuring syslog source-interface 130

Configuration Examples for Implementing Host Services and Applications 131
Checking Network Connectivity: Example 131
Configuring Domain Services: Example 132
Configuring a Router to Use `r`p, FTP, or TFTP Connections: Example 133

Additional References 133

CHAPTER 6

Implementing HSRP 135
Prerequisites for Implementing HSRP 136
Restrictions for Implementing HSRP 136
Information About Implementing HSRP 136

HSRP Overview 136
HSRP Groups 136
HSRP and ARP 139
Preemption 139
ICMP Redirect Messages 139

How to Implement HSRP 139
Enabling HSRP 139
Enabling HSRP for IPv6 141
Configuring HSRP Group Attributes 142
Configuring the HSRP Activation Delay 146
Enabling HSRP Support for ICMP Redirect Messages 148
Multiple Group Optimization (MGO) for HSRP 149
  Customizing HSRP 149
Configuring a Primary Virtual IPv4 Address 152
Configuring a Secondary Virtual IPv4 Address 153
Configuring a slave follow 154
Configuring a slave primary virtual IPv4 address 156
Configuring a Secondary Virtual IPv4 address for the Slave Group 157
Configuring a slave virtual mac address 158
Configuring an HSRP Session Name 159
BFD for HSRP 160
  Advantages of BFD 161
  BFD Process 161
  Configuring BFD 161
    Enabling BFD 161
    Modifying BFD timers (minimum interval) 162
    Modifying BFD timers (multiplier) 163
Enhanced Object Tracking for HSRP and IP Static 164
  Configuring object tracking for HSRP 165
Hot Restartability for HSRP 166
Configuration Examples for HSRP Implementation on Software 166
  Configuring an HSRP Group: Example 166
  Configuring a Router for Multiple HSRP Groups: Example 166
Additional References 167

CHAPTER 7

Implementing LPTS 169
  Prerequisites for Implementing LPTS 169
  Information About Implementing LPTS 169
    LPTS Overview 170
    LPTS Policers 170
  Configuring LPTS Policer with IP TOS Precedence 170
    Configuring LPTS Policers 171
  Configuration Examples for Implementing LPTS Policers 172
    Configuring LPTS Policers: Example 173
Additional References 177
CHAPTER 8

Implementing Network Stack IPv4 and IPv6 179

Prerequisites for Implementing Network Stack IPv4 and IPv6 180
Restrictions for Implementing Network Stack IPv4 and IPv6 180
Information About Implementing Network Stack IPv4 and IPv6 180

Network Stack IPv4 and IPv6 Exceptions 180
IPv4 and IPv6 Functionality 180
IPv6 for Cisco IOS XR Software 181
Larger IPv6 Address Space 181
IPv6 Address Formats 181
IPv6 Address Type: Unicast 182
  Aggregatable Global Address 183
  Link-Local Address 184
  IPv4-Compatible IPv6 Address 185
Simplified IPv6 Packet Header 185
IPv6 Neighbor Discovery 190
  IPv6 Neighbor Solicitation Message 190
  IPv6 Router Advertisement Message 192
  IPv6 Neighbor Redirect Message 193
ICMP for IPv6 194
Address Repository Manager 195
  Address Conflict Resolution 195
    Conflict Database 195
    Multiple IP Addresses 195
    Recursive Resolution of Conflict Sets 195
  Route-Tag Support for Connected Routes 196
How to Implement Network Stack IPv4 and IPv6 197
Assigning IPv4 Addresses to Network Interfaces 197
IPv4 Addresses 197
  IPv4 Virtual Addresses 198
Configuring IPv6 Addressing 199
IPv6 Virtual Addresses 199
Assigning Multiple IP Addresses to Network Interfaces 200
  Secondary IPv4 Addresses 200
Configuring IPv4 and IPv6 Protocol Stacks 201
Enabling IPv4 Processing on an Unnumbered Interface 202
   IPv4 Processing on an Unnumbered Interface 202
Configuring ICMP Rate Limiting 203
   IPv4 ICMP Rate Limiting 203
   IPv6 ICMP Rate Limiting 204
Configuring IPARM Conflict Resolution 205
   Static Policy Resolution 205
   Longest Prefix Address Conflict Resolution 206
   Highest IP Address Conflict Resolution 206
Generic Routing Encapsulation 207
   IPv4/IPv6 Forwarding over GRE Tunnels 208
   IPv6 forwarding over GRE tunnels 208
Configuration Examples for Implementing Network Stack IPv4 and IPv6 208
   Assigning an Unnumbered Interface: Example 208
Configuring VRF mode big 209
Additional References 209

CHAPTER 9

Configuring Transports 213
   Prerequisites for Configuring NSR, TCP, UDP, Transports 213
   Information About Configuring NSR, TCP, UDP Transports 214
      NSR Overview 214
      TCP Overview 214
      UDP Overview 214
   How to Configure Failover as a Recovery Action for NSR 215
      Configuring Failover as a Recovery Action for NSR 215
Additional References 216

CHAPTER 10

Implementing VRRP 219
   Prerequisites for Implementing VRRP on Cisco IOS XR Software 220
   Restrictions for Implementing VRRP on Cisco IOS XR Software 220
   Information About Implementing VRRP 220
      VRRP Overview 220
      Multiple Virtual Router Support 221
      VRRP Router Priority 222
      VRRP Advertisements 222
### Benefits of VRRP 222

**How to Implement VRRP on Cisco IOS XR Software** 223
**Customizing VRRP** 223
**Enabling VRRP** 226
**Verifying VRRP** 228
**Clearing VRRP Statistics** 228

**Configuration Examples for VRRP Implementation on Cisco IOS XR Software** 229
*Configuring accept-mode* 229
*Configuring a Global Virtual IPv6 Address* 230
*Configuring a Primary Virtual IPv4 Address* 232
*Configuring a Secondary Virtual IPv4 Address* 233
*Configuring a Virtual Link-Local IPv6 Address* 235
*Disabling State Change Logging* 236

**MIB support for VRRP** 237
*Configuring SNMP server notifications for VRRP events* 237

**Hot Restartability for VRRP** 238
**Configuration Examples for VRRP Implementation on Cisco IOS XR Software** 238
*Configuring a VRRP Group: Example* 238
*Clearing VRRP Statistics: Example* 240

**Additional References** 240

---

### Implementing Video Monitoring 243

**Prerequisites for Implementing Video Monitoring** 243

**Information About Implementing Video Monitoring** 243

**Video Monitoring** 243
*Introduction to Video Monitoring* 244
*Key Features Supported on Video Monitoring* 244

**Video Monitoring Terminology** 247

**Implementing Video Monitoring** 248

**Creating IPv4 Access Lists** 248

**Configuring class-map** 250

**Configuring policy-map** 251
*Configuring policy-map with metric parameters* 251
*Media bit-rate* 252
*Configuring policy-map with flow parameters* 254
Preface

The Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide preface contains these sections:

- Changes to This Document, page xv
- Obtaining Documentation and Submitting a Service Request, page xv

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Table 1: Changes to This Document

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>OL-26068-04</td>
<td>April 2014</td>
<td>Configuring ARP chapter was updated.</td>
</tr>
<tr>
<td>OL-26068-03</td>
<td>September 2012</td>
<td>Republished with documentation updates for Cisco IOS XR Release 4.2.3.</td>
</tr>
<tr>
<td>OL-26068-02</td>
<td>June 2012</td>
<td>Republished with documentation updates for Cisco IOS XR Release 4.2.1.</td>
</tr>
<tr>
<td>OL-26068-01</td>
<td>December 2011</td>
<td>Initial release of this document.</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.
To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.
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 software features 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.

For a complete description of the access list and prefix list commands listed in this module, refer to the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Feature History for Implementing Access Lists and Prefix Lists

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>IPv6 ACL over BVI interface feature was added.</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>ACL in Class map feature was added.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing Access Lists and Prefix Lists, page 2
- Restrictions for Implementing Access Lists and Prefix Lists, page 2
- Hardware Limitations, page 3
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:

- IPv4 ACLs are not supported for loopback and interflex interfaces.
- IPv6 ACLs are not supported for loopback, interflex and L2 Ethernet Flow Point (EFP) main or subinterfaces.
- 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:
  1. Remove the ACL from the interface.
  2. Reconfigure the ACL.
  3. Reapply the ACL to the interface.

Note

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.

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

- 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, deny ACE with 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.

**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.
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.

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 cannot 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
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.

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

**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 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.

### 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.

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. 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.

However, you can use the `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.

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you set the <code>update-number</code> 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 is not recommended because the volume of log messages could overwhelm the system.</td>
</tr>
</tbody>
</table>

| Even if you use the `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 is when a threshold is not specified. |

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 should not be used as a billing tool or as an accurate source of the number of matches to an access list.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>If the Access-List Entry has...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| ...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.
If the Access-List Entry has... | Then...
---|---
...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 14” 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 forwarding 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.

**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)
IPSLA support for Object tracking

The OT-module interacts with the IPSLA-module to get reachability information. With IPSLA, the routers perform periodic measurements.

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 linecards, 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>{ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl_1</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv6 access-list acl_2</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>[sequence-number] remark remark</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10</td>
</tr>
<tr>
<td></td>
<td>remark Do not allow user1 to telnet out</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• [sequence-number]{permit</td>
</tr>
<tr>
<td></td>
<td>• [sequence-number]{permit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10</td>
</tr>
<tr>
<td></td>
<td>permit 172.16.0.0 0.0.255.255</td>
</tr>
</tbody>
</table>

(Original) 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.

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.

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 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.
### Applying Access Lists

After creating an access list, you must apply it to a line or interface. See the Applying Access Lists, on page 14 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.

#### 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 14 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.
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface type interface-path-id</td>
<td></td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/2/0/2</td>
<td>- The <em>type</em> argument specifies an interface type. For more information on interface types, use the question mark (?) online help function.</td>
</tr>
<tr>
<td></td>
<td>- The <em>instance</em> argument specifies either a physical interface instance or a virtual instance.</td>
</tr>
<tr>
<td></td>
<td>- The naming notation for a physical interface instance is <em>rack/slot/module/port</em>. The slash (/) between values is required as part of the notation.</td>
</tr>
<tr>
<td></td>
<td>- The number range for a virtual interface instance varies depending on the interface type.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> Do one of the following:</td>
<td>Controls access to an interface.</td>
</tr>
<tr>
<td>• `ipv4 access-group access-list-name {ingress</td>
<td>egress} [hardware-count] [interface-statistics]`</td>
</tr>
<tr>
<td>• `ipv6 access-group access-list-name {ingress</td>
<td>egress} [interface-statistics]`</td>
</tr>
<tr>
<td>Example:</td>
<td>• Use the <code>hardware-count</code> keyword to enable hardware counters for the IPv4 access group.</td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-in-filter in</code></td>
<td>• Hardware counters are automatically enabled for IPv6 access groups.</td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-out-filter out</code></td>
<td>• Use the <code>interface-statistics</code> keyword to specify per-interface statistics in the hardware.</td>
</tr>
<tr>
<td><strong>Step 4</strong> commit</td>
<td>This example applies filters on packets inbound and outbound from GigabitEthernet interface 0/2/0/2.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Specifies either the auxiliary, console, default, or a user-defined line template and enters line template configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> line `{aux</td>
<td>console</td>
</tr>
<tr>
<td>Example: <code>RP/0/RSP0/CPU0:router(config)# line default</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>{ipv4 | ipv6} prefix-list <em>name</em></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 prefix-list pfx_1 or RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list pfx_2</td>
</tr>
<tr>
<td></td>
<td>Enters either IPv4 or IPv6 prefix list configuration mode and configures the named prefix list.</td>
</tr>
<tr>
<td></td>
<td>- To create a prefix list, you must enter at least one permit or deny clause.</td>
</tr>
<tr>
<td></td>
<td>- Use the no {ipv4 | ipv6} prefix-list <em>name</em> command to remove all entries in a prefix list.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>[sequence-number] remark <em>remark</em></td>
</tr>
<tr>
<td>Example:</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>(Optional) Allows you to comment about the following permit or deny statement in a named prefix list.</td>
</tr>
<tr>
<td></td>
<td>- The remark can be up to 255 characters; anything longer is truncated.</td>
</tr>
<tr>
<td></td>
<td>- Remarks can be configured before or after permit or deny statements, but their location should be consistent.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>[sequence-number] {permit | deny} network/length [ge value] [le value] [eq value]</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ipv6_pfx)# 20 deny 128.0.0.0/8 eq 24</td>
</tr>
<tr>
<td></td>
<td>Specifies one or more conditions allowed or denied in the named prefix list.</td>
</tr>
<tr>
<td></td>
<td>- This example denies all prefixes matching /24 in 128.0.0.0/8 in prefix list pfx_2.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Repeat Step 4 as necessary. Use the no sequence-number command to delete an entry.</td>
</tr>
<tr>
<td></td>
<td>Allows you to revise a prefix list.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>commit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>- show prefix-list ipv4 <em>name</em> [sequence-number]</td>
</tr>
<tr>
<td></td>
<td>- show prefix-list ipv6 <em>name</em> [sequence-number] [summary]</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show prefix-list ipv4 pfx_1 or RP/0/RSP0/CPU0:router# show prefix-list ipv6 pfx_2 summary</td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays the contents of current IPv4 or IPv6 prefix lists.</td>
</tr>
<tr>
<td></td>
<td>- Use the name argument to display the contents of a specific prefix list.</td>
</tr>
<tr>
<td></td>
<td>- Use the sequence-number argument to specify the sequence number of the prefix-list entry.</td>
</tr>
<tr>
<td></td>
<td>- Use the summary keyword to display summary output of prefix-list contents.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>clear {ipv4 | ipv6} prefix-list <em>name</em> [sequence-number]</td>
</tr>
<tr>
<td></td>
<td>(Optional) Clears the hit count on an IPv4 or IPv6 prefix list.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Enters IPv4 access list configuration mode and configures access list acl_1.</td>
</tr>
<tr>
<td>Step 2 ipv4 access-list name</td>
<td>(Optional) Allows you to comment about the following permit or deny statement in a named access list.</td>
</tr>
<tr>
<td>Example:</td>
<td>• The remark can be up to 255 characters; anything longer is truncated.</td>
</tr>
<tr>
<td></td>
<td>• Remarks can be configured before or after permit or deny statements, but their location should be consistent.</td>
</tr>
</tbody>
</table>
### Command or Action

| Step 4 | [sequence-number] [permit | deny] source [source-wildcard] [log | log-input] |
|--------|---------------------------------------------------------------|

**Example:**

RP/0/RSP0/CPU0:router(config-ipv4-ac1)# 20 permit 172.16.0.0 0.0.255.255

or

RRP/0/RSP0/CPU0:router(config-ipv4-ac1)# 30 deny 192.168.34.0 0.0.0.255

- **Purpose**
  - 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.
  - 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.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Repeat Step 4 as necessary, adding statements by sequence number where you planned. Use the <code>no sequence-number</code> command to delete an entry.</th>
</tr>
</thead>
</table>

- **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 14 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a copy of an existing IPv4 or IPv6 access list.</td>
</tr>
<tr>
<td>`copy access-list {ipv4</td>
<td>ipv6}source-acl destination-acl`</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# copy ipv6 access-list list-1 list-2</td>
<td>• Use the <code>destination-acl</code> argument to specify where to copy the contents of the source access list.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>`show access-lists {ipv4</td>
<td>ipv6}[access-list-name hardware {ingress</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# show access-lists ipv4 list-2</td>
<td></td>
</tr>
</tbody>
</table>

**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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>resequence access-list {ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router# resequence access-list ipv4 acl_3 20 15</td>
</tr>
<tr>
<td></td>
<td>(Optional) Resequences the specified IPv4 or IPv6 access list using the starting sequence number and the increment of sequence numbers.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>{ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list acl_1</td>
</tr>
<tr>
<td>or</td>
<td>RP/0/RSP0/CPU0:router(config)# ipv6 access-list acl_2</td>
</tr>
<tr>
<td></td>
<td>Enters either IPv4 or IPv6 access list configuration mode and configures the named access list.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• [sequence-number] {permit</td>
</tr>
<tr>
<td></td>
<td>Specifies one or more conditions allowed or denied in IPv4 access list acl_1.</td>
</tr>
</tbody>
</table>
Implementing Access Lists and Prefix Lists

Sequencing Access-List Entries and Revising the Access List

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`[precedence precedence] [dscp dscp] [fragments] [log</td>
<td>log-input]`</td>
</tr>
<tr>
<td>• `[sequence-number] {permit</td>
<td>deny} protocol `</td>
</tr>
<tr>
<td>{source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td>`source-ipv6-address} [operator</td>
<td>port</td>
</tr>
<tr>
<td>`{destination-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td>`[destopts] [fragments] [log</td>
<td>log-input]`</td>
</tr>
</tbody>
</table>

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-ipv4-acl)# 20 permit icmp any any
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 deny tcp any any gt 5000

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` | (Optional) Displays the contents of a named IPv4 or IPv6 access list. |
| `{ingress | egress} [interface type interface-path-id]` | • Review the output to see that the access list includes the updated information. |
| `{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

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 14” 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> copy prefix-list {ipv4</td>
<td>ipv6} source-name destination-name</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# copy prefix-list ipv6 list_1 list_2</td>
<td>• Use the <code>source-name</code> argument to specify the name of the prefix list to be copied and the <code>destination-name</code> argument to specify where to copy the contents of the source prefix list.</td>
</tr>
<tr>
<td></td>
<td>• The <code>destination-name</code> argument must be a unique name; if the <code>destination-name</code> argument name exists for a prefix list, the prefix list is not copied.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Do one of the following:</td>
<td>(Optional) Displays the contents of current IPv4 or IPv6 prefix lists.</td>
</tr>
<tr>
<td>• <code>show prefix-list ipv4 [name] [sequence-number] [summary]</code></td>
<td>• Review the output to see that prefix list list_2 includes the entries from list_1.</td>
</tr>
<tr>
<td>• <code>show prefix-list ipv6 [name] [sequence-number] [summary]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# show prefix-list ipv6 list_2</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>(Optional) Resequences the named IPv4 prefix list using the starting sequence number and the increment of sequence numbers.</td>
</tr>
<tr>
<td>resequence prefix-list ipv4 name [base [increment]]</td>
<td>* This example resequences a prefix list named pfx_1. The starting sequence number is 10 and the increment is 15.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# resequence prefix-list ipv4 pfx_1 10 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters either IPv4 or IPv6 prefix list configuration mode and configures the named prefix list.</td>
</tr>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies one or more conditions allowed or denied in the named prefix list.</td>
</tr>
<tr>
<td>{ipv4</td>
<td>ipv6} prefix-list name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list pfx_2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>[sequence-number] {permit</td>
<td>deny} network/length [ge value] [le value] [eq value]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ipv6_pfx)# 15 deny 128.0.0.0/8 eq 24</td>
<td></td>
</tr>
</tbody>
</table>
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 {pfiler location node-id}]}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
</tbody>
</table>
### Implementing Access Lists and Prefix Lists

- **Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters IPv4 access list configuration mode and configures the specified access list.</td>
</tr>
<tr>
<td>ipv4 access-list name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list security-abf-acl</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the conditions for an IPv4 access list. The configuration example shows how to configure ACL-based forwarding with security ACL.</td>
</tr>
<tr>
<td>[sequence-number]</td>
<td>*permit protocol source source-wildcard destination destination-wildcard [precedence precedence] [[default] nexthop1 [ipv4 ipv4-address]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# 15 permit ipv4 30.2.1.0 0.0.0.255 any</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# 25 permit ipv4 any any</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the information for ACL software.</td>
</tr>
<tr>
<td>commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>show access-list ipv4 [[access-list-name hardware {ingress</td>
<td>egress} [interface type interface-path-id] [sequence number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router# show access-lists ipv4 security-abf-acl</td>
</tr>
</tbody>
</table>

### Implementing IPSLA-OT

In this section, the following procedures are discussed:

- Enabling track mode, on page 28
- Configuring track type, on page 28
- Configuring tracking type (line protocol), on page 28
- Configuring track type (list), on page 29
- Configuring tracking type (route), on page 30
- Configuring tracking type (rtr), on page 31
Enabling track mode

SUMMARY STEPS

1. configure
2. track track-name
3. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 track track-name</td>
<td>Enters track configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# track t1</td>
<td></td>
</tr>
<tr>
<td>Step 3 commit</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track track-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters track configuration mode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# track t1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>type line-protocol state interface type interface-path-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Sets the interface which needs to be tracked for state change notifications.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-track)# type line-protocol state interface tengige 0/4/4/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

Configuring track type (list)

List is a boolean 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track <code>track-name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# track t1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>type list boolean and</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-track)# type list boolean and</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track <code>track-name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# track t1</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track track-name</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>type rtr ipsla operation id reachability</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>
**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 [ vrf vrf-name1 ] [ipv6 ipv6-address1 ] [ nexthop2 [ vrf vrf-name2 ] [ipv6 ipv6-address2 ] [nexthop3 [ vrf vrf-name3 ] [ipv6ipv6-address3 ]]]
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters IPv6 access list configuration mode and configures the specified access list.</td>
</tr>
<tr>
<td><strong>Step 2</strong> {ipv6 } access-list name</td>
<td>Sets the conditions for an IPv6 access list. The configuration example shows how to configure pure ACL-based forwarding for ACL.</td>
</tr>
</tbody>
</table>

Example:

```plaintext
RP/0/RSP0/CPU0:router(config)# ipv6 access-list security-abf-acl
```

**Step 3**

```plaintext
[ 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 [ vrf vrf-name1 ] [ipv6 ipv6-address1 ] [ nexthop2 [ vrf vrf-name2 ] [ipv6 ipv6-address2 ] [nexthop3 [ vrf vrf-name3 ] [ipv6ipv6-address3 ]]]
```

Example:

```plaintext
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
```

**Step 4** 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 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
```
Adding Entries with Sequence Numbers: Example

In the following example, a new entry is added to IPv4 access list acl_5.

```plaintext
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
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.

```plaintext
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 10.1.0.0 0.0.0.255 any
20 permit ip 10.2.0.0 0.0.0.255 any
30 permit ip 10.3.0.0 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 10.1.0.0 0.0.0.255 any
20 permit ip 10.2.0.0 0.0.0.255 any
30 permit ip 10.3.0.0 0.0.0.255 any
40 permit ip 10.4.0.0 0.0.0.255 any
```

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
end-class-map

show qos-ea km policy p.aclv6 vmr interface tenGigE 0/1/0/6.10 hw
```

---

Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide, Release 4.2.x
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  F1 : flags
F2: L2 flags  F4: L4 flags  SP/DP: L4 ports
T : IP TTL  D : DFS class#  L : leaf class#
---------------------------------------------------------------------
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 00 00 00 00 11111111:00000000:00000000:00000000
22222222:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FFFF FFFF FFFF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=0 11800200 00010000 00000000 00000000 00000000 00000000 00000000 00000000
22000000:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FFFF FFFF FFFF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=0 11800200 00010000 00000000 00000000 00000000 00000000 00000000 00000000
V|200D 00 0000 0000 00 00 00 00 00 00 00 00 00 00 11111111:00000000:00000000:00000000
22222222:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FFFF FFFF FFFF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=0 11800200 00010000 00000000 00000000 00000000 00000000 00000000 00000000
V|200D 00 0000 0000 00 00 00 00 00 00 00 00 00 00 11111111:00000000:00000000:00000000
22222222:00000000:00000000:00000000
M|0000 FF FFFF FFFF FF FF FF FF FF FFFF FFFF FFFF 00000000:00000000:00000000:00000000
00000000:00000000:00000000:00000000
R| C=0 11800200 00010000 00000000 00000000 00000000 00000000 00000000 00000000
```
IPv4/IPv6 ACL over BVI interface

In Release 4.2.1, IPv4/IPv6 ACL is enabled over BVI interfaces on the ASR 9000 Enhanced Ethernet Line Cards.

For ACL over BVI interfaces, the defined direction is:

- L2 interface - ingress direction
- L3 interface - egress direction

On the A9K-SIP-700 and ASR 9000 Ethernet Line Cards, ACLs on BVI interfaces are not supported.

Note

For ASR 9000 Ethernet linecards, ACL 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
```

Additional References

The following sections provide references related to implementing access lists and prefix lists.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access list commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Access List Commands module in Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>Prefix list commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Prefix List Commands module in Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>Terminal services commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Terminal Services Commands module in Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</td>
</tr>
</tbody>
</table>
## Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
CHAPTER 2

Configuring 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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference. To locate documentation of other commands that appear in this module, use the command reference master index, or search online.

Feature History for Configuring ARP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

- Prerequisites for Configuring ARP, page 41
- Restrictions for Configuring ARP, page 42
- Information About Configuring ARP, page 42
- How to Configure ARP, page 45
- Configuration Examples for ARP Configuration on Cisco IOS XR Software, page 52
- Additional References, page 53

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.
- ARP throttling is not supported.

**Note**

ARP throttling is the rate limiting of ARP packets in Forwarding Information Base (FIB).

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.

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 a 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.

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
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>interface type number</td>
<td></td>
</tr>
<tr>
<td>proxy-arp</td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring ARP

#### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface type number</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/0/0/0</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>local-proxy-arp</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-if)# local-proxy-arp</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>commit</code></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface type interface-path-id</td>
<td>Enters interface configuration mode and configures an interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> arp dagr</td>
<td>Enters DAGR configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> peer ipv4 address</td>
<td>Creates a new DAGR group for the virtual IP address.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>route distance normal</strong></td>
</tr>
<tr>
<td></td>
<td><code>normal- distance priority priority-distance</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>route distance normal 140 priority 3</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>route metric normal</strong></td>
</tr>
<tr>
<td></td>
<td><code>normal- metric priority priority-metric</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>route metric normal 84 priority 80</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>timers query standby</strong></td>
</tr>
<tr>
<td></td>
<td><code>query-time standby-time</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>timers query 2 standby 19</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>priority-timeout</strong></td>
</tr>
<tr>
<td></td>
<td><code>time</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>priority-timeout 25</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• end</td>
</tr>
<tr>
<td></td>
<td>• commit</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td><code>commit</code></td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the <strong>commit</strong> command to save the configuration changes to the running configuration file and remain within the configuration session.</td>
</tr>
</tbody>
</table>

### Step 10

**show arp drag [ interface [ IP-address ]]**

(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.

**Example:**

```
RP/0/RSP0/CPU0:router# show arp drag
```

---

## 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 adjacency (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. **commit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/
```
### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Example: RP/0/RSP0/CPU0:router# configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Example: RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Example: RP/0/RSP0/CPU0:router(config-if)# arp timeout 100</td>
<td>Sets the ARP cache timeout interval.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Do one of the following:</td>
<td>Saves configuration changes.</td>
</tr>
</tbody>
</table>
### Command or Action

- end
- commit

### Purpose

- 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.

### Configuration Examples for ARP Configuration on Cisco IOS XR Software

#### Creating a Static ARP Cache Entry: Example

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

```plaintext
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:

```plaintext
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:

```plaintext
configure
arp 192.168.8.20 0800.0900.1723 arp
```
Enabling Proxy ARP: Example

The following is an example of enabling proxy ARP:

```configure
interface MgmtEth 0/RSP0/CPU0/0
/CP0/0
proxy-arp```

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

Additional References

The following sections provide references related to ARP.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP commands</td>
<td><em>ARP Commands</em> module in <em>Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</em></td>
</tr>
<tr>
<td>Getting started material</td>
<td><em>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</em></td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Quality of Service Commands module in Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
<tr>
<td>Class-based traffic shaping, traffic policing, low latency queuing, and MDDR</td>
<td>Configuring Modular Quality of Service Congestion Management module in Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 826</td>
<td>Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware</td>
</tr>
<tr>
<td>RFC 1027</td>
<td>Using ARP to implement transparent subnet gateways</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
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.

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. To locate documentation for other commands that might appear in the course of executing a configuration task, search online in the master command index.

Feature History for Implementing CEF

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 4.2.3</td>
<td>CEF load-balancing algorithm feature was introduced.</td>
</tr>
</tbody>
</table>

- **Prerequisites for Implementing Cisco Express Forwarding**, page 57
- **Information About Implementing Cisco Express Forwarding Software**, page 58
- **How to Implement CEF**, page 61
- **Configuration Examples for Implementing CEF on Routers Software**, page 72
- **Additional References**, page 86

Prerequisites for Implementing Cisco Express Forwarding

The following prerequisites are required to implement Cisco Express Forwarding:
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 software CEF 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.

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 1: Sample Topology for BGP Policy Accounting, on page 60, 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.
BGP policy accounting measures and classifies IP traffic for BGP prefixes only.

**Figure 1: 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.

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.
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.

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.

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.

## 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.

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Displays the IPv4 or IPv6 CEF table. The next hop and forwarding interface are displayed for each prefix.</td>
</tr>
<tr>
<td>show cef {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays a summary of the IPv4 or IPv6 CEF table.</td>
</tr>
<tr>
<td>show cef {ipv4</td>
<td>ipv6} summary</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays detailed IPv4 or IPv6 CEF table information.</td>
</tr>
<tr>
<td>show cef {ipv4</td>
<td>ipv6} detail</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays detailed adjacency information, including Layer 2 information for each interface.</td>
</tr>
<tr>
<td>show adjacency detail</td>
<td>Example: RP/0/RSP0/CPU0:router# show adjacency detail</td>
</tr>
</tbody>
</table>

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 *Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference* 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 *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide* 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
16. Do one of the following:
   - end
   - commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters policy configuration mode.</td>
</tr>
<tr>
<td>as-path-set</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# as-path-set as107</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-as)# ios-regex '107$'</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-as)# end-set</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# as-path-set as108</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-as)# ios-regex '108$'</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-as)# end-set</td>
<td></td>
</tr>
</tbody>
</table>
### Implementing Cisco Express Forwarding

#### Configuring BGP Policy Accounting

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-as)# exit</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>prefix-set name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# prefix-set RT-65</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Defines the prefix list.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pfx)# exit</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>route-policy policy-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# route-policy rp501b</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Specifies the route-policy name.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-rpl)# end</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td></td>
<td>• When you issue the end command, the system prompts you to commit changes:</td>
</tr>
<tr>
<td></td>
<td><strong>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</strong></td>
</tr>
<tr>
<td></td>
<td>• Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</td>
</tr>
<tr>
<td></td>
<td>• Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>router bgp autonomous-system-number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config)# router bgp 1</code></td>
</tr>
<tr>
<td>Step 10</td>
<td>`address-family ipv4 {unicast</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast</code></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>table policy policy-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-af)# table-policy set-traffic-index</code></td>
</tr>
<tr>
<td>Step 12</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-af)# end</code></td>
</tr>
<tr>
<td>Step 13</td>
<td><code>configure</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# configure</code></td>
</tr>
<tr>
<td>Step 14</td>
<td><code>interface type interface-path-id</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/0/2</code></td>
</tr>
<tr>
<td>Step 15</td>
<td>Command or Action</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-if)# ipv4 bgp policy accounting output destination-accounting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do one of the following:</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td></td>
<td>• end</td>
<td>• When you issue the end command, the system prompts you to commit changes:</td>
</tr>
</tbody>
</table>
|         | • commit | 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 62.
## 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>show route bgp</code></td>
<td>Displays all BGP routes with traffic indexes.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show route bgp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show bgp summary</code></td>
<td>Displays the status of all BGP neighbors.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show bgp summary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>show bgp ip-address</code></td>
<td>Displays BGP prefixes with BGP attributes.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show bgp 40.1.1.1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show route ipv4 ip-address</code></td>
<td>Displays the specific BGP route with the traffic index in the RIB.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show route ipv4 40.1.1.1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show cef ipv4 prefix</code></td>
<td>Displays the specific BGP prefix with the traffic index in the RP FIB.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show cef ipv4 40.1.1.1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show cef ipv4 prefix detail</code></td>
<td>Displays the specific BGP prefix with detailed information in the RP FIB.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router# show cef ipv4 40.1.1.1 detail</code></td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action 
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cef purge-delay seconds</td>
<td>Configures a delay in purging routes when the Routing Information Base (RIB) or other related processes experience a failure.</td>
</tr>
</tbody>
</table>

Example: RP/0/RSP0/CPU0:router(config)# cef purge-delay 180

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>interface type interface-path-id</code></td>
<td>Enables IPv4 or IPv6 uRPF checking.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/1/0/0
```

**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
```

- 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.

| **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> rp mgmtethernet forwarding</td>
<td>Enables switching from the MSC to the route processor Management Ethernet interfaces.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# rp mgmtethernet forwarding</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> cef bgp attribute {attribute-id</td>
<td>local-attribute-id}</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# cef bgp attribute 508</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>
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
encapsulation dot1q 1

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 10.1.40.0/24
ipv4 directed-broadcast
ipv4 bgp policy accounting input source-accounting destination-accounting
ipv4 bgp policy accounting output source-accounting destination-accounting
encapsulation ppp
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 (10.1.0/24) then
  set traffic-index 1
 elseif destination in (10.1.2/24) then
  set traffic-index 2
 elseif destination in (10.1.3/24) then
  set traffic-index 3
 elseif destination in (10.1.4/24) then
  set traffic-index 4
 elseif destination in (10.1.5/24) then
  set traffic-index 5
 endif
 if destination in (10.1.6/24) then
  set traffic-index 6
 endif
.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 0/0/0/8 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
The following example show how to verify BGP routes and traffic indexes:

show route bgp
Verifying BGP Policy Statistics: Example

Traffic Index 1
B 10.
.1.0.0/24 [20/0] via 10.
.17.
.1.2, 00:07:09
Traffic Index 2
B 10.
.1.2.0/24 [20/0] via 10.
.17.
.1.2, 00:07:09
Traffic Index 3
B 10.
.1.3.0/24 [20/0] via 10.
.17.
.1.2, 00:07:09
Traffic Index 4
B 10.
.1.4.0/24 [20/0] via 10.
.17.
.1.2, 00:07:09
Traffic Index 5
B 10.
.1.5.0/24 [20/0] via 10.
.17.
.1.2, 00:07:09
Traffic Index 6
B 10.
.1.0/24 [20/0] via 10.
.18.
.1.2, 00:07:09
Traffic Index 7
B 10.
.2.0/24 [20/0] via 10.
.18.
.1.2, 00:07:09
Traffic Index 8
B 10.
.3.0/24 [20/0] via 10.
.18.
.1.2, 00:07:09
Traffic Index 9
B 10.
.4.0/24 [20/0] via 10.
.18.
.1.2, 00:07:09
Traffic Index 10
B 10.
.5.0/24 [20/0] via 10.
.18.
.1.2, 00:07:09
Traffic Index 15
B 10.
.1.0/24 [20/0] via 10.
.45.
.0.2, 00:07:09
Traffic Index 15
B 10.
.1.0/24 [20/0] via 10.
.45.
.0.2, 00:07:09
Traffic Index 15
B 10.
.3.0/24 [20/0] via 10.
.45.
.0.2, 00:07:09
Traffic Index 15

Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide, Release 4.2.x
Verifying BGP Policy Statistics: Example

B  10
  .65
  .65
  .0/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .5/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .6/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .7/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .8/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .9/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .65
  .10/24 [20/0] via 10
  .45
  .0.2, 00:07:09
  Traffic Index 15
B  10
  .66
  .1/24 [20/0] via 10
  .32
  .0.2, 00:07:09
  Traffic Index 16
B  10
  .66
  .2/24 [20/0] via 10
  .32
  .0.2, 00:07:09
  Traffic Index 16
B  10
  .66
  .3/24 [20/0] via 10
  .32
  .0.2, 00:07:09
  Traffic Index 16
B  10
  .66
  .4/24 [20/0] via 10
  .32
  .0.2, 00:07:09
  Traffic Index 16
B  10
  .66
  .5/24 [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
.67
.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
Verifying BGP Policy Statistics: Example
.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.

<table>
<thead>
<tr>
<th>Process</th>
<th>RecvTblVer</th>
<th>bRIB/RIB</th>
<th>SendTblVer</th>
<th>Speaker</th>
<th>Neighbor Spk</th>
<th>AS MsgRcvd MsgSent</th>
<th>TblVer</th>
<th>InQ OutQ</th>
<th>Up/Down</th>
<th>St/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>151</td>
<td>151</td>
<td>151</td>
<td>10</td>
<td>0.2</td>
<td>0 107 54 53 151 0 0 00:25:26 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.0.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 108 54 53 151 0 0 00:25:28 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.1.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 53 54 151 0 0 00:25:42 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.2.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 52 54 151 0 0 00:25:04 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.3.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 52 53 151 0 0 00:25:26 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.4.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 53 54 151 0 0 00:25:41 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.5.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 53 54 151 0 0 00:25:43 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.6.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 51 53 151 0 0 00:24:59 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.7.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 51 52 151 0 0 00:24:44 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1.8.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 121 51 52 151 0 0 00:24:49 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.1.2</td>
<td>0 122 52 54 151 0 0 00:25:21 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1221 54 54 151 0 0 00:25:43 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1222 53 54 151 0 0 00:25:38 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1223 52 53 151 0 0 00:25:17 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1224 51 52 151 0 0 00:24:57 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1225 52 53 151 0 0 00:25:14 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1226 52 54 151 0 0 00:25:04 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1227 52 54 151 0 0 00:25:13 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>.2</td>
<td></td>
<td></td>
<td>10.2</td>
<td>0 1228 53 54 151 0 0 00:25:36 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 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
  4.1.0.2 from 4.1.0.2 (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
  8.1.0.2 from 8.1.0.2 (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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet</td>
<td>0/2/0/2.1</td>
<td>0</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet</td>
<td>0/2/0/4.1</td>
<td>0</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet</td>
<td>0/0/0/4</td>
<td>0</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet</td>
<td>0/0/0/8</td>
<td>0</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet</td>
<td>0/0/0/4</td>
<td>0</td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>Hash</th>
<th>OK</th>
<th>Interface</th>
<th>Address</th>
<th>Packets (remote)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y</td>
<td>GigabitEthernet 0/0/0/8</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco Express Forwarding Commands module in Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BGP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>BGP Commands module in the Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</td>
</tr>
<tr>
<td>Link Bundling Commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Link Bundling Commands module in the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
CHAPTER 4

Implementing the Dynamic Host Configuration Protocol

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

Note

Feature History for Implementing the Dynamic Host Configuration Protocol

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

- Prerequisites for Configuring DHCP Relay Agent, page 90
- Information About DHCP Relay Agent, page 90
- How to Configure and Enable DHCP Relay Agent, page 91
- Configuring a DHCP Proxy Profile, page 98
- DHCPv4 Client, page 99
- DHCPv6 Relay Agent Notification for Prefix Delegation, page 101
- Configuration Examples for the DHCP Relay Agent, page 103
- Implementing DHCP Snooping, page 104
- Additional References, page 114
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 2: Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address, on page 90 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).
How to Configure and Enable DHCP Relay Agent

This section contains the following tasks:

Configuring and Enabling the DHCP Relay Agent

This task describes how to configure and enable DHCP relay agent.

**SUMMARY STEPS**

1. configure
2. dhcp ipv4
3. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>dhcp ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
</tr>
<tr>
<td>Step 3</td>
<td>commit</td>
</tr>
</tbody>
</table>

Configuring a DHCP Relay Profile

This task describes how to configure and enable the DHCP relay agent.

**SUMMARY STEPS**

1. configure
2. dhcp ipv4
3. profile profile-name relay
4. helper-address [vrf vrf-name] address
5. commit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> dhcp ipv4</td>
<td>Enters DHCP IPv4 configuration submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> profile profile-name relay</td>
<td>Enters DHCP IPv4 profile relay submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> helper-address [vrf vrf- name ] address</td>
<td>Forwards UDP broadcasts, including BOOTP and DHCP.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf1 10.10.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>

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.

SUMMARY STEPS

1. configure
2. dhcp ipv6
3. interface type interface-path-id relay
4. destination ipv6-address
5. commit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 dhcp ipv6</td>
<td>Enables DHCP for IPv6 and enters the DHCP IPv6 configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config) # dhcp ipv6</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6) #</td>
</tr>
<tr>
<td>Step 3 interface</td>
<td>Specifies an interface type and interface-path-id, places the router in interface configuration mode, and enables DHCPv6 relay service on the interface.</td>
</tr>
<tr>
<td>type interface-path-id relay</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6) #</td>
</tr>
<tr>
<td></td>
<td>interface tenGigE 0/5/0/0 relay</td>
</tr>
<tr>
<td>Step 4 destination</td>
<td>Specifies a destination address to which client packets are forwarded.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface is forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6-if) #</td>
</tr>
<tr>
<td></td>
<td>destination 10:10:10:10</td>
</tr>
<tr>
<td>Step 5 commit</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>dhcp ipv4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enters DHCP IPv4 configuration submode.</strong></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
<td><strong>interface type name relay profile name</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Attaches a relay profile to an interface.</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4)# interface</td>
</tr>
<tr>
<td></td>
<td>gigabitethernet 0/0/0</td>
</tr>
<tr>
<td></td>
<td>/0 relay profile client</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td></td>
<td><strong>commit</strong></td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>dhcp ipv4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enters DHCP IPv4 configuration submode.</strong></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
<td><strong>interface type name none</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Disables the DHCP relay on the interface.</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# interface</td>
</tr>
</tbody>
</table>
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

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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters DHCP IPv4 configuration submode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> dhcp ipv4</td>
<td>Enters DHCP IPv4 profile relay submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
<td>Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
<tr>
<td><strong>Step 3</strong> profile profile-name relay</td>
<td>Enters DHCP IPv4 profile relay submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 4</strong> relay information option</td>
<td>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.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option</td>
<td>The supported suboptions are:</td>
</tr>
<tr>
<td></td>
<td>* Remote ID</td>
</tr>
<tr>
<td></td>
<td>* Circuit ID</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>relay information check</td>
<td>(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.</td>
</tr>
<tr>
<td>relay information policy {drop</td>
<td>keep}</td>
</tr>
<tr>
<td>relay information option allow-untrusted</td>
<td>(Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero.</td>
</tr>
</tbody>
</table>

### 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**

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

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> dhcp ipv4</td>
<td>Enters DHCP IPv4 configuration submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> profile profile-name proxy</td>
<td>Enters DHCP IPv4 profile proxy submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client proxy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> helper-address [vrf vrf-name ] address [ giaddr gateway-address ]</td>
<td>Forwards UDP broadcasts, including BOOTP and DHCP.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-proxy-profile)# helper-address vrf1 10.10.1.1</td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Step 5</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>

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

SUMMARY STEPS

1. configure
2. interface MgmtEth rack/slot/CPU0/port
3. interface <interface_name> ipv4 address dhcp

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface MgmtEth rack/slot/CPU0/port</td>
</tr>
</tbody>
</table>

Example:

```
RP/0/RSP0/CPU0:router(config)#interface mgmtEth 0/0/CPU0/0
```
**Purpose**

Configure DHCP on the interface.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface &lt;interface_name&gt; ipv4 address dhcp</code></td>
<td>Configure DHCP on the interface.</td>
</tr>
</tbody>
</table>

### Example:

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

### Example:

```
dhcp Enable IPv4 DHCP client
```

The following example shows a sample of using IPv4 address command:

```
RP/0/0/CPU0:ios(config)#interface mgmtEth 0/0/CPU0/0 ipv4 address ?
A.B.C.D/prefix IPv4 address/prefix or IPv4 address and Mask
dhcp Enable IPv4 DHCP client
```

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enables DHCP for IPv6 and enters DHCP IPv6 configuration mode.</td>
</tr>
<tr>
<td>Step 2 dhcp ipv6</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config) # dhcp ipv6 RP/0/RSP0/CPU0:router(config-dhcpv6)#</td>
</tr>
<tr>
<td>Step 3 profile profile-name proxy</td>
<td>Enters the proxy profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6)# profile downstream proxy RP/0/RSP0/CPU0:router(config-dhcpv6-profile)#</td>
</tr>
<tr>
<td>Step 4 helper-address ipv6-address interface type interface-path-id</td>
<td>Configure the DHCP IPv6 relay agent.</td>
</tr>
<tr>
<td>Example:</td>
<td>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)</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exits from the profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# exit RP/0/RSP0/CPU0:router(config-dhcpv6)#</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables IPv6 DHCP on an interface and acts as an IPv6 DHCP stateful relay agent.</td>
</tr>
<tr>
<td><code>interface type interface-path-id proxy</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6)# interface GigabitEthernet 0/1/0/0 proxy RP/0/RSP0/CPU0:router(config-dhcpv6-if)#</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enters the profile configuration mode.</td>
</tr>
<tr>
<td><code>profile profile-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv6-if)# profile downstream RP/0/RSP0/CPU0:router(config-dhcpv6-if)#</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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:

```bash
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:

```bash
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 3: DHCP Snooping in an Aggregation Network, on page 105 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.

Figure 3: 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>dhcp ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>profile <em>untrusted-profile-name</em> snoop</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4)# exit</td>
</tr>
</tbody>
</table>
## How to Configure DHCP Snooping

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><code>dhcp ipv4</code></td>
<td>Enables DHCP for IPv4 and enters DHCP IPv4 profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>profile profile-name snoop</code></td>
<td>Configures a trusted DHCP snooping profile for the server port.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-dhcv4)# profile trustedServerProfile snoop</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>trusted</code></td>
<td>Configures a DHCP snooping profile to be trusted.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-dhcv4)# trusted</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>exit</code></td>
<td>Exits DHCP IPv4 profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-dhcv4)# exit</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>l2vpn</code></td>
<td>Enters l2vpn configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config)# l2vpn</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>bridge group group-name</code></td>
<td>Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group ccc</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>bridge-domain bridge-domain-name</code></td>
<td>Establishes a bridge domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ddd</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>interface type interface-path-id</code></td>
<td>Identifies an interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/0</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 13** dhcp ipv4 snoop profile untrusted-profile-name  
*Example:*  
RP/0/RSP10/CP00:router(config-l2vpn-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/RSP10/CP00:router(config-l2vpn-bd-ac)# gigabitethernet 0/1/0/1  
Identifies an interface.

**Step 15** dhcp ipv4 snoop profile trusted-profile-name  
*Example:*  
RP/0/RSP10/CP00:router(config-l2vpn-bd-ac)# dhcp ipv4 snoop profile trustedServerProfile  
Attaches a trusted DHCP snoop profile to the bridge port.

**Step 16** exit  
*Example:*  
RP/0/RSP10/CP00:router(config-l2vpn-bd-ac)# exit  
Exits the l2vpn bridge group bridge-domain interface configuration submode.

**Step 17** exit  
*Example:*  
RP/0/RSP10/CP00:router(config-l2vpn-bd-ac)# 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters l2vpn configuration submode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>l2vpn</td>
<td>Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# l2vpn</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>bridge group group-name</td>
<td>Establishes a bridge domain and enters l2vpn bridge group bridge-domain configuration submode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1</td>
<td></td>
</tr>
</tbody>
</table>
| Step 4 | bridge-domain bridge-domain-name | |}

<p>| Step 5 | dhcp ipv4 snoop profile profile-name | Attaches the untrusted DHCP snooping profile to the bridge domain. |
| <strong>Example:</strong> | RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile untrustedClientProfile | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td><strong>interface</strong> type interface-path-id</td>
<td>Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
</tr>
<tr>
<td><strong>dhcpp ipv4 none</strong></td>
<td>Disables DHCP snooping on the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# dhcp ipv4 none</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td></td>
</tr>
<tr>
<td><strong>interface</strong> type interface-path-id</td>
<td>Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/2</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td></td>
</tr>
<tr>
<td><strong>dhcpp ipv4 snoop profile</strong> profile-name</td>
<td>Attaches the trusted DHCP snooping profile to a port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile trustedServerProfile</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td></td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits l2vpn bridge-domain bridge group interface configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bd-bg)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td></td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits l2vpn bridge-domain submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td></td>
</tr>
<tr>
<td><strong>commit</strong></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>dhcp ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# dhcp ipv4</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>profile profile-name snoop</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>relay information option</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>relay information option allow-untrusted</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option allow-untrusted</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

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:

```conf
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:

```conf
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:

```conf
dhcp ipv4 profile trustedServerProfile snoop
tagged 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.

```conf
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 how to assign a trusted DHCP snooping profile to a bridge port:

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

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

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XR DHCP commands</td>
<td>DHCP Commands module in the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>Getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Information about user groups and task IDs</td>
<td>Configuring AAA Services module in the Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2131</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
</tbody>
</table>
**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>
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. To locate documentation of other commands that appear in this module, use the command reference master index, or search online.

Feature History for Implementing Host Services and Applications

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing Host Services and Applications, page 117
- Information About Implementing Host Services and Applications, page 118
- How to Implement Host Services and Applications, page 120
- Configuring syslog source-interface, page 130
- Configuration Examples for Implementing Host Services and Applications, page 131
- Additional References, page 133

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), and remote copy protocol (rcp) rcp clients 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. FTP, TFTP, or rcp can be used to save the core dump to a remote server. See the Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide 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 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).

Cisco inetd

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> `ping [ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td>Example:</td>
<td>If you do not enter a hostname or an IP address on the same line as the <code>ping</code> 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.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> `ping bulk ipv4 [ input cli { batch</td>
<td>inline }]`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# ping bulk ipv4 input cli</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1&lt;br&gt;traceroute [ipv4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

Example:<br>RP/0/RSP0/CPU0:router# traceroute
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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 Do one of the following:</td>
<td>Defines a default domain name used to complete unqualified hostnames.</td>
</tr>
<tr>
<td>• <code>domain name domain-name</code></td>
<td></td>
</tr>
<tr>
<td>• or</td>
<td></td>
</tr>
<tr>
<td>• <code>domain list domain-name</code></td>
<td></td>
</tr>
</tbody>
</table>

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.
**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Specifies:</td>
</tr>
<tr>
<td><strong>Step 2</strong> tftp {ipv4</td>
<td>ipv6} server {homedir tftp-home-directory} {max-servers number} [access-list name]</td>
</tr>
<tr>
<td></td>
<td>Home directory (required)</td>
</tr>
<tr>
<td></td>
<td>Maximum number of concurrent TFTP servers (required)</td>
</tr>
</tbody>
</table>

Example:

```
RP/0/RSP0/CPU0:router(config)# tftp ipv4 server access-list listA homedir disk0
```
## 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 user.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> rcp client username <em>username</em></td>
<td></td>
</tr>
</tbody>
</table>
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 Cisco ASR 9000 Series Router implementation of FTP, you can set the following FTP characteristics:

- Passive-mode FTP
- Password

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 Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference for detailed information on using rcp protocol with the `copy` command.
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

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

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
/
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 *Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference* 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>tftp client source-interface <em>type</em></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CP00:router(config)# tftp client source-interface GigabitEthernet 1/0/2/1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

**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 *Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference* 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>telnet [ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>logging source-interface interface vrf vrf-name</td>
<td>Configures the logging source interface to identify the syslog traffic, originating in a VRF from a particular router, as coming from a single device.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# logging source-interface loopback 0 vrf vrf1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# logging source-interface loopback 1 vrf default</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>show running-configuration logging</td>
<td>Verifies that the logging source is correctly configured for the VRF.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

```plaintext
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 sjc5-00lab-gw1.cisco.com (172.24.114.33) 5 msec 6 msec 6 msec
4 sjc5-0lab-gw1.cisco.com (172.24.134.89) 5 msec 5 msec 5 msec
5 sjc5-abb4-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-dcl-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 host2 10.2.0.2 192.168.7.33

Defining the Domain Name

configure
domain name cisco.com
Specifying the Addresses of the Name Servers

```plaintext
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**

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

**Using FTP**

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

**Using TFTP**

```plaintext
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**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host services and applications commands</td>
<td>Host Services and Applications Commands module in Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
</tbody>
</table>
### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC-959</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>RFC-1738 and RFC-2732</td>
<td>Uniform Resource Locators (URL)</td>
</tr>
<tr>
<td>RFC-783</td>
<td>Trivial File Transfer Protocol</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release 3.7.2</th>
<th>This feature was introduced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>Support was added for the following features:</td>
</tr>
<tr>
<td></td>
<td>• BFD for HSRP.</td>
</tr>
<tr>
<td></td>
<td>• Hot restartability for HSRP.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>Multiple Group Optimization (MGO) for HSRP feature was added.</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>Enhanced object tracking for HSRP and IP Static feature was added.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing HSRP, page 136
- Restrictions for Implementing HSRP, page 136
- Information About Implementing HSRP, page 136
- How to Implement HSRP, page 139
- BFD for HSRP, page 160
- Enhanced Object Tracking for HSRP and IP Static, page 164
- Hot Restartability for HSRP, page 166
- Configuration Examples for HSRP Implementation on Software, page 166
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 and Ethernet link bundles.

**Note**
However, only HSRP version 1 is supported in release 4.2.x.

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 an exthop 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 4: Routers Configured as an HSRP Group, on page 137 shows routers configured as members of a single 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 5: Routers Configured as Members of Multiple HSRP Groups, on page 138 shows routers configured as members of multiple HSRP groups.

**Figure 5: Routers Configured as Members of Multiple HSRP Groups**

<table>
<thead>
<tr>
<th>Group 1 Standby</th>
<th>1.0.0.1</th>
<th>2.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.2</td>
<td>Ethernet 0</td>
<td>Router A</td>
</tr>
<tr>
<td>1.0.0.3</td>
<td>Ethernet 0</td>
<td>Router B</td>
</tr>
<tr>
<td>1.0.0.4</td>
<td>Ethernet 0</td>
<td>Router C</td>
</tr>
<tr>
<td>5.0.0.1</td>
<td>Ethernet 0</td>
<td>Router D</td>
</tr>
</tbody>
</table>

In Figure 5: Routers Configured as Members of Multiple HSRP Groups, on page 138, 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router hsrp</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# router hsrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp)# interface GigabitEthernet 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> hsrp group-number version version-no</td>
<td>Enables HSRP group submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1</td>
<td><strong>Note</strong> The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
</tr>
<tr>
<td><strong>Step 6</strong> address { learn</td>
<td>address [secondary] }</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn</td>
<td>• 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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td>interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

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.
### 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> address-family ipv6</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> hsrp group-number</td>
<td>Enables HSRP group submode.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> address linklocal [autoconfig</td>
<td>ipv6-address]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# address linklocal autoconfig</code></td>
<td></td>
</tr>
<tr>
<td>• The virtual linklocal address must not match any other virtual linklocal address that is already configured for a different group.</td>
<td></td>
</tr>
<tr>
<td>• The virtual linklocal address must not match the interface linklocal IPv6 address.</td>
<td></td>
</tr>
<tr>
<td>If you use the autoconfig keyword, the linklocal address is calculated using the EUI-64 format.</td>
<td></td>
</tr>
<tr>
<td>Use the legacy-compatible keyword to be compatible with Cisco IOS and other legacy Cisco devices.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> address global ipv6-address</td>
<td>Activates HSRP on the configured interface and assigns a global IPv6 address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# address global 2001:DB8:A:B::1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 8</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# router hsrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> hsrp use-bia</td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp use-bia</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• To restore the default virtual MAC address, use the no hsrp use-bia command.</td>
</tr>
</tbody>
</table>
### Configuring HSRP Group Attributes

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
</tbody>
</table>
| 6    | `hsrp group-number version version-no` | 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. |
|      | **Example:**      | RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1 |
| 7    | `priority priority` | (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.  
- 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. |
|      | **Example:**      | RP/0/RSP0/CPU0:router(config-hsrp-gp)# priority 100 |
| 8    | `track type instance [priority-decrement]` | (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
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>preempt [delay seconds]</code></td>
<td>(Optional) Configures HSRP preemption and preemption delay.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-hsrp-gp)# preempt</td>
<td></td>
</tr>
<tr>
<td><code>authentication string</code></td>
<td>(Optional) Configures an authentication string for the Hot Standby Router Protocol (HSRP).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-hsrp-gp)# authentication company1</td>
<td></td>
</tr>
<tr>
<td><code>mac-address address</code></td>
<td>(Optional) Specifies a virtual MAC address for the HSRP.</td>
</tr>
</tbody>
</table>

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

- When you configure preemption and preemption delay with the `preempt` command, the local router attempts to assume control as the active router when 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 preemption of 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

- 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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>• 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.</td>
</tr>
<tr>
<td>RP/O/RSP0/CPU0:router(config-hsrp-if)# mac-address 4000.1000.1060</td>
<td>• 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 <code>mac-address</code> command to specify the virtual MAC address.</td>
</tr>
<tr>
<td>• The MAC address specified is used as the virtual MAC address when the router is active.</td>
<td>• The <code>mac-address</code> command is intended for certain APPN configurations.</td>
</tr>
<tr>
<td>• In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the <code>mac-address</code> command in the routers to set the virtual MAC address to the value used in the end nodes.</td>
<td>• Enter the <code>no mac-address</code> command to revert to the standard virtual MAC address (0000.0C07.ACn).</td>
</tr>
</tbody>
</table>

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 gives 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>  ( \text{router hsrp} )</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config)# router hsrp} )</td>
<td>( \text{RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1} )</td>
</tr>
<tr>
<td><strong>Step 3</strong>  ( \text{interface type interface-path-id} )</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1} )</td>
<td>( \text{RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp delay minimum 2 reload 10} )</td>
</tr>
<tr>
<td><strong>Step 4</strong>  ( \text{hsrp delay [minimum seconds] [reload seconds]} )</td>
<td>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).</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp delay minimum 2 reload 10} )</td>
<td>( \text{RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1} )</td>
</tr>
<tr>
<td><strong>Step 5</strong>  ( \text{address-family ipv4} )</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4} )</td>
<td>( \text{RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# address learn} )</td>
</tr>
<tr>
<td><strong>Step 6</strong>  ( \text{hsrp group-number version version-no} )</td>
<td>Enables HSRP group submode.</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1} )</td>
<td>( \text{Note} ) ( \text{The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.} )</td>
</tr>
<tr>
<td><strong>Step 7</strong>  ( \text{address [learn</td>
<td>address [secondary]]} )</td>
</tr>
<tr>
<td>( \text{Example:} ) ( \text{RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn} )</td>
<td>( \text{Note} ) ( \text{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 link local IPv6 address, the router does not accept the configuration when you commit your changes using the commit keyword.} )</td>
</tr>
<tr>
<td><strong>Step 8</strong>  commit</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td>Step 2 router hsrp</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# router hsrp</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type interface-path-id</td>
<td>Configures Internet Control Message Protocol (ICMP) redirect messages to be sent when the Hot Standby Router Protocol (HSRP) is configured on an interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 hsrp redirects disable</td>
<td>• The <code>hsrp redirects</code> 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 disabled on an interface, then the global command cannot reenable the functionality.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp redirects</td>
<td>• With the <code>hsrp redirects</code> 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.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• To revert to the default, which is that ICMP messages are enabled, use the no hsrp redirects command.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>hsrp group-number version version-no</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 1</td>
</tr>
<tr>
<td>Enables HSRP group submode.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
</tr>
<tr>
<td>Step 7</td>
<td>address { learn</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn</td>
</tr>
<tr>
<td>Activates HSRP on the configured interface.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>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 link local IPv6 address, the router does not accept the configuration when you commit your changes using the commit keyword.</td>
</tr>
<tr>
<td>Step 8</td>
<td>commit</td>
</tr>
</tbody>
</table>

**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 slaves 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router hsrp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>hsrp group-no version version-no</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1 version 2</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong> name name</td>
<td>Configures an HSRP session name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# name s1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> address { learn</td>
<td>address}</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables hot standby protocol for IP.</td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn</code></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Step 8</strong> address address secondary</td>
<td>Configures the secondary virtual IPv4 address for a router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# address 10.20.30.1 secondary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> authentication string</td>
<td>Configures an authentication string for the Hot Standby Router Protocol (HSRP).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# authentication company1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> bfd fast-detect</td>
<td>Enables bidirectional forwarding (BFD) fast-detection on a HSRP interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# bfd fast-detect</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> mac-address address</td>
<td>Specifies a virtual MAC address for the Hot Standby Router Protocol (HSRP).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# mac-address 4000.1000.1060</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> hsrp group-no slave</td>
<td>Enables HSRP slave configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp-gp)# hsrp 2 slave</code></td>
<td></td>
</tr>
<tr>
<td>Step 13</td>
<td>Command or Action</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>follow mgo-session-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-slave)# follow s1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address ip-address</td>
<td>Configures the primary virtual IPv4 address for the slave group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-slave)# address 10.3.2.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

### 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
6. address { learn | address}
7. commit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>router hsrp</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
RP/0/RSP0/CPU0:router(config)# router hsrp
```
### 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
6. address address secondary
7. commit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config)# router hsrp
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hsrp group-no</td>
<td>Enables HSRP group configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address address secondary</td>
<td>Configures the secondary virtual IPv4 address for a router.</td>
</tr>
</tbody>
</table>

**Example:**
```
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# address 10.20.30.1 secondary
```

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a slave follow

To instruct the slave group to inherit its state from a specified group, use the **slave follow** command in HSRP slave submode mode.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
</tr>
<tr>
<td>Step 3 interface</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>type interface-path-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td>Step 4 address-family</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td>ipv4</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td>Step 5 hsrp group-no slave</td>
<td>Enables HSRP slave configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 2 slave</td>
</tr>
<tr>
<td>Step 6 follow mgo-session-name</td>
<td>Instructs the slave group to inherit its state from a specified group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-slave)# follow m1</td>
</tr>
<tr>
<td>Step 7 commit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a slave primary virtual IPv4 address

To configure the primary virtual IPv4 address for the slave group, use the `slave 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>hsrp group-no slave</td>
<td>Enables HSRP slave configuration mode on a specific interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 2 slave</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring a Secondary Virtual IPv4 address for the Slave Group

Perform this task to configure the secondary virtual IPv4 address for the slave group.

### SUMMARY STEPS

1. `configure`
2. `router hsrp`
3. `interface type interface-path-id`
4. `address-family ipv4`
5. `hsrp group-num slave`
6. `address address secondary`
7. `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>router hsrp</code></td>
</tr>
<tr>
<td><code>Example:</code></td>
<td><code>RP/0/RSP0/CPU0:router(config)# router hsrp</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface type interface-path-id</code></td>
</tr>
<tr>
<td><code>Example:</code></td>
<td><code>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</code></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 4  address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>Step 5  hsrp group-no slave</td>
<td>Enables HSRP slave configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-hsrp-address-family)# hsrp 2 slave</td>
<td></td>
</tr>
<tr>
<td>Step 6  address address secondary</td>
<td>Configures the secondary virtual IPv4 address for a router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-hsrp-slave)# address 10.20.30.1 secondary</td>
<td></td>
</tr>
<tr>
<td>Step 7  commit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a slave virtual mac address**

To configure the virtual MAC address for the slave group, use the `slave 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
</tbody>
</table>
### Implementing HSRP

#### 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
6. name name
7. commit

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><code>router hsrp</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><code>interface type interface-path-id</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td><code>address-family ipv4</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables HSRP slave configuration mode on a specific interface.</td>
</tr>
<tr>
<td><code>hsrp group-no slave</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 2 slave</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures the virtual MAC address for the slave group.</td>
</tr>
<tr>
<td><code>mac-address address</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-slave)# mac-address 10.20.30</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>hsrp group-no</td>
<td>Enables HSRP group configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>name name</td>
<td>Configures an HSRP session name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>commit</td>
<td><strong>BFD for HSRP</strong></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router hsrp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
</tr>
<tr>
<td>Enables HSRP configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>hsrp [group number] version version-no bfd fast-detect [peer ipv4 ipv4-address interface-type interface-path-id]</td>
</tr>
<tr>
<td>Example:</td>
<td>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</td>
</tr>
<tr>
<td>Enables fast detection on a specific interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• The <strong>version</strong> keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
</tr>
<tr>
<td></td>
<td>• HSRP version 2 provides an extended group range of 0-4095.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router hsrp</td>
</tr>
<tr>
<td>Step 3 interface</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>type interface-path-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td>Step 4 hsrp bfd minimum-interval</td>
<td>Sets the minimum interval to the specified period. The interval is in milliseconds; range is 15 to 30000 milliseconds.</td>
</tr>
<tr>
<td>interval</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd minimum-interval 20</td>
</tr>
<tr>
<td>Step 5 address-family</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td>ipv4</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
</tr>
<tr>
<td>Step 6 commit</td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>router hsrp</td>
<td>Enables HSRP configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

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

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type interface-path-id</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
```

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>hsrp bfd multiplier multiplier</td>
<td>Sets the multiplier to the value. Range is 2 to 50.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd multiplier 30
```

**Step 5**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
```

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

---

**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.

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 *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*, 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 submode.

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enables HSRP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router hsrp</td>
<td>Enables HSRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# router hsrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type interface-path-id</td>
<td>Enables HSRP address-family configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4</td>
<td>Enables HSRP group submode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> hsrp group-number version version-no</td>
<td>Enables HSRP group submode.</td>
</tr>
<tr>
<td><strong>Note</strong> The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.</td>
<td></td>
</tr>
</tbody>
</table>

The version keyword is available only if IPv4 address-family is selected. By default, version is set to 2 for IPv6 address families.
### Purpose

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Track object name [priority-decrement]</th>
<th>Enable tracking of the named object with the specified decrement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-hsrp-gp)# track object t1 2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>commit</th>
</tr>
</thead>
</table>

### 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:

```plaintext
configure
cisco
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:

```plaintext
configure
cisco
router hsrp
```

---

---
interface TenGigE 0/2/0/3
address family ipv4
hsrp 1
  address 1.0.0.5
  priority 20
  preempt
  authentication aclara
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Quality of Service Commands on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
<tr>
<td>Class-based traffic shaping, traffic policing, low-latency queuing, and Modified Deficit Round Robin (MDRR)</td>
<td>Configuring Modular Quality of Service Congestion Management on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide</td>
</tr>
<tr>
<td>WRED, RED, and tail drop</td>
<td>Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide</td>
</tr>
<tr>
<td>HSRP commands</td>
<td>HSRP Commands on Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>master command reference</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Commands Master List</td>
</tr>
<tr>
<td>getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Information about user groups and task IDs</td>
<td>Configuring AAA Services on Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide</td>
</tr>
</tbody>
</table>
### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

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

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference.

Feature History for Implementing LPTS

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>LPTS was introduced.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing LPTS, page 169
- Information About Implementing LPTS, page 169
- Configuring LPTS Policer with IP TOS Precedence, page 170
- Configuration Examples for Implementing LPTS Policers, page 172
- Additional References, page 177

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

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.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td><strong>Purpose</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> lpts pifib hardware police [location node-id]</td>
<td>&lt;br&gt;Example:&lt;br&gt;RP/0/RSP0/CPU0:router(config)# lpts pifib hardware</td>
</tr>
</tbody>
</table>
### 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}]`

---

#### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>police location 0/2/CPU0 or RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police</td>
<td>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).</td>
</tr>
</tbody>
</table>

- Use the `flow_type` argument to select the applicable flow type. For information about the flow types, see *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference*.

<table>
<thead>
<tr>
<th>Step 3 flow flow_type</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Step 4 precedence {number | name}                                           | Displays the policer configuration value set. |
|--------------------------|--------------------------------------------------------------------------|
| Example:                 | (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. |
|                         |                                                                         |
|                         |                                                                         |

<table>
<thead>
<tr>
<th>Step 5 commit</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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 |                                                                         |
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> lpts pifib hardware police [location node-id]</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)#</td>
<td></td>
</tr>
<tr>
<td>Step 3 flow flow_type {rate rate}</td>
<td>Configures the policer for the LPTS flow type. The example shows how to configure the policer for the ospf flow type.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# flow ospf unicast default rate 20000</td>
<td></td>
</tr>
<tr>
<td>Step 4 commit</td>
<td>Displays the policer configuration value set.</td>
</tr>
<tr>
<td>Step 5 show lpts pifib hardware police [location {all</td>
<td>node_id}]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/2/cpu0</td>
<td></td>
</tr>
</tbody>
</table>

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
!
  show lpts pifib hardware police location 0/2/CPU0

FT - Flow type ID; PPS - Packets per second configured rate

<table>
<thead>
<tr>
<th>FT</th>
<th>Flow type</th>
<th>Rate (PPS)</th>
<th>Accept/Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>unconfigured-default</td>
<td>101</td>
<td>0/0</td>
</tr>
<tr>
<td>1</td>
<td>Fragment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OSPF-mc-known</td>
<td>1500</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>OSPF-mc-default</td>
<td>250</td>
<td>0/0</td>
</tr>
<tr>
<td>4</td>
<td>OSPF-uc-known</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>OSPF-uc-default</td>
<td>101</td>
<td>1/0</td>
</tr>
<tr>
<td>6</td>
<td>ISIS-known</td>
<td>250 1500</td>
<td>0/0</td>
</tr>
<tr>
<td>7</td>
<td>ISIS-default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Rate</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>BGP-known</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>9</td>
<td>BGP-default cfg-peer</td>
<td>2000 17612</td>
<td>0/0</td>
</tr>
<tr>
<td>10</td>
<td>BGP-default</td>
<td>5</td>
<td>0/0</td>
</tr>
<tr>
<td>11</td>
<td>PIM-mcast</td>
<td>1500</td>
<td>0/0</td>
</tr>
<tr>
<td>12</td>
<td>PIM-ucast</td>
<td>1500</td>
<td>0/0</td>
</tr>
<tr>
<td>13</td>
<td>IGMP</td>
<td>1500</td>
<td>0/0</td>
</tr>
<tr>
<td>14</td>
<td>ICMP-local</td>
<td>1046</td>
<td>0/0</td>
</tr>
<tr>
<td>15</td>
<td>ICMP-app</td>
<td>1000</td>
<td>1046</td>
</tr>
<tr>
<td>16</td>
<td>ICMP-control</td>
<td>1000</td>
<td>0/0</td>
</tr>
<tr>
<td>17</td>
<td>ICMP-default</td>
<td>1046</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>LDP-TCP-known</td>
<td>1500</td>
<td>9965</td>
</tr>
<tr>
<td>19</td>
<td>LDP-TCP-cfg-peer</td>
<td>1500</td>
<td>0/0</td>
</tr>
<tr>
<td>20</td>
<td>LDP-TCP-default</td>
<td>5</td>
<td>0/0</td>
</tr>
<tr>
<td>21</td>
<td>LDP-UDP</td>
<td>1000</td>
<td>59759</td>
</tr>
<tr>
<td>22</td>
<td>All routers</td>
<td>1500</td>
<td>0/0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Default</td>
<td>Lower</td>
<td>Upper</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>CSS</td>
<td>default</td>
<td>500</td>
<td>0/0</td>
</tr>
<tr>
<td>RSH</td>
<td>default</td>
<td>47</td>
<td>0/0</td>
</tr>
<tr>
<td>UDP</td>
<td>default</td>
<td>49</td>
<td>0/0</td>
</tr>
<tr>
<td>TCP</td>
<td>default</td>
<td>51</td>
<td>1500</td>
</tr>
<tr>
<td>Mcast</td>
<td>default</td>
<td>53</td>
<td>653</td>
</tr>
</tbody>
</table>

Implementing LPTS

Configuring LPTS Policers: Example
Additional References

The following sections provide references related to implementing LPTS.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XR LPTS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco LPTS Commands module in the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>
## RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support</td>
<td>—</td>
</tr>
<tr>
<td>for existing RFCs has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchable technical content, including links to products, technologies,</td>
<td></td>
</tr>
<tr>
<td>solutions, technical tips, and tools. Registered Cisco.com users can</td>
<td></td>
</tr>
<tr>
<td>log in from this page to access even more content.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 8

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.

For a complete description of the Network Stack IPv4 and IPv6 commands, refer to the Network Stack IPv4 and IPv6 Commands module of the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference. To locate documentation for other commands that appear in this chapter, use the Cisco ASR 9000 Series Aggregation Services Router Commands Master List, or search online.

Feature History for Implementing Network Stack IPv4 and IPv6

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>GRE for IPv4 feature was added.</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>IPv6 over IPv4 GRE Tunnel interface feature was added.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing Network Stack IPv4 and IPv6, page 180
- Restrictions for Implementing Network Stack IPv4 and IPv6, page 180
- Information About Implementing Network Stack IPv4 and IPv6, page 180
- How to Implement Network Stack IPv4 and IPv6, page 197
- Generic Routing Encapsulation, page 207
- Configuration Examples for Implementing Network Stack IPv4 and IPv6, page 208
- Configuring VRF mode big, page 209
- Additional References, page 209
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.

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, Internet 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: \texttt{x\textsubscript{a}:x\textsubscript{b}:x\textsubscript{c}:x\textsubscript{d}:x\textsubscript{e}:x\textsubscript{f}:x\textsubscript{g}:x\textsubscript{h}}. Following are two examples of IPv6 addresses:

- \texttt{2001:0DB8:7654:3210:FEDC:BA98:7654:3210}
- \texttt{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 2: Compressed IPv6 Address Formats, on page 182 lists compressed IPv6 address formats.

A double colon may be used as part of the \texttt{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.

\begin{note}
Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros.
\end{note}
The hexadecimal letters in IPv6 addresses are not case-sensitive.

### Table 2: Compressed IPv6 Address Formats

<table>
<thead>
<tr>
<th>IPv6 Address Type</th>
<th>Preferred Format</th>
<th>Compressed Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast</td>
<td>2001:0:0:0:0:DB8:800:200C:417A</td>
<td>1080::0:DB8:800:200C:417A</td>
</tr>
<tr>
<td>Multicast</td>
<td>FF01:0:0:0:0:0:0:0:101</td>
<td>FF01::101</td>
</tr>
<tr>
<td>Loopback</td>
<td>0:0:0:0:0:0:0:1</td>
<td>::1</td>
</tr>
<tr>
<td>Unspecified</td>
<td>0:0:0:0:0:0:0:0:0</td>
<td>::</td>
</tr>
</tbody>
</table>

The loopback address listed in Table 2: Compressed IPv6 Address Formats, on page 182 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 2: Compressed IPv6 Address Formats, on page 182 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 6: Aggregatable Global Address Format, on page 183 shows the structure of an aggregatable global address.

Figure 6: Aggregatable Global Address Format

```
<table>
<thead>
<tr>
<th>Provider</th>
<th>Site</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>45 bits</td>
<td>16 bits</td>
</tr>
<tr>
<td>64 bits</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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 (11111110 111010) 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 7: Link-Local Address Format, on page 184 shows 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 7: 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 8: IPv4-Compatible IPv6 Address Format, on page 185 shows the structure of an IPv4-compatible IPv6 address and a few acceptable formats for the address.

**Figure 8: IPv4-Compatible IPv6 Address Format**

![IPv4-Compatible IPv6 Address Format](image)

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 9: IPv4 Packet Header Format, on page 185)

**Figure 9: IPv4 Packet Header Format**

![IPv4 Packet Header Format](image)

The basic IPv6 packet header has 8 fields with a total size of 40 octets (320 bits). (See Figure 10: IPv6 Packet Header Format, on page 186.) 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 10: IPv6 Packet Header Format**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>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.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>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.</td>
</tr>
<tr>
<td>Flow Label</td>
<td>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.</td>
</tr>
<tr>
<td>Payload Length</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Next Header</td>
<td>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 11: IPv6 Extension Header Format, on page 188.</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>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.</td>
</tr>
<tr>
<td>Source Address</td>
<td>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.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 11: IPv6 Extension Header Format, on page 188 shows the IPv6 extension header format.

Figure 11: IPv6 Extension Header Format

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

Table 4: IPv6 Extension Header Types

<table>
<thead>
<tr>
<th>Header Type</th>
<th>Next Header Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop-by-hop options header</td>
<td>0</td>
<td>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.</td>
</tr>
<tr>
<td>Header Type</td>
<td>Next Header Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination options header</td>
<td>60</td>
<td>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.</td>
</tr>
<tr>
<td>Routing header</td>
<td>43</td>
<td>The routing header is used for source routing.</td>
</tr>
<tr>
<td>Fragment header</td>
<td>44</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication header and ESP header</td>
<td>51, 50</td>
<td>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.</td>
</tr>
<tr>
<td>Upper-layer header</td>
<td>6 (TCP), 17 (UDP)</td>
<td>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.</td>
</tr>
<tr>
<td>Mobility header</td>
<td>To be done by IANA</td>
<td>Extension headers used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings.</td>
</tr>
</tbody>
</table>
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 12: IPv6 Neighbor Discovery—Neighbor Solicitation Message, on page 190.) 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 12: IPv6 Neighbor Discovery—Neighbor Solicitation Message

ICMPv6 Type = 135
Src = A
Dst = solicited-node multicast of B
Data = link-layer address of A
Query = what is your link address?

ICMPv6 Type = 136
Src = B
Dst = A
Data = link-layer address of B

A and B can now exchange packets on this link

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 13: IPv6 Neighbor Discovery—Router Advertisement Message, on page 192.)

**Figure 13: IPv6 Neighbor Discovery—Router Advertisement Message**

![Router advertisement packet definitions: ICMPv6 Type = 134, Src = router link-local address, Dst = all-nodes multicast address, Data = options, prefix, lifetime, autoconfig flag](image)

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 14: IPv6 Neighbor Discovery—Neighbor Redirect Message, on page 193.)

*Figure 14: IPv6 Neighbor Discovery—Neighbor Redirect Message*

---

Neighbor redirect packet definitions:
- IPv6 Type = 137
- Src = link-local address of Device A
- Dst = link-local address of Host H
- Data = target address (link-local address of Device B), options (header of redirected packet)

Note: If the target is a host, the target address is equal to the destination address of the redirect packet and the options include the link-layer address of the target host (if known).
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.

**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. configuration
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface type interface-path-id</td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Do one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ipv4 address ipv4-address mask [secondary]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• ipv4 address ipv4-address mask [secondary]</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code></td>
<td></td>
</tr>
</tbody>
</table>
| 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` | (Optional) Displays the usability status of interfaces configured for IPv4. |
| Step 5 | `show ipv4 interface`  
**Example:**  
RP/0/RSP0/CPU0:router# show ipv4 interface |  |

### 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.

### 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.
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.

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.

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
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>interface type interface-path-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>ipv4 address ip4-address mask [secondary]</td>
<td>Specifies that the configured address is a secondary IPv4 address.</td>
</tr>
<tr>
<td>ipv6 address ipv6-prefix/prefix-length [eui-64]</td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 2**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface type interface-path-id</code></td>
<td>Specifies the interface type and number, and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
```

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4 address ip-address mask [secondary]</code></td>
<td>Specifies a primary or secondary IPv4 address for an interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.99.1 255.255.255.0
```

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 address ipv6-prefix/prefix-length [eui-64]</code></td>
<td>Specifies the IPv6 address assigned to the interface and enables IPv6 processing on the interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:c18:1::3/64
```

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>commit</code></td>
<td>Commit the configuration changes.</td>
</tr>
</tbody>
</table>

---

### 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 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface type interface-path-id</td>
<td>Enables IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3 ipv4 unnumbered interface-type interface-instance</td>
<td>Enables IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5</td>
<td>• 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).</td>
</tr>
<tr>
<td>Step 4 commit</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Limits the rate that IPv4 ICMP destination unreachable messages are generated.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do one of the following:</td>
<td>Limits the rate that IPv4 ICMP destination unreachable messages are generated.</td>
<td></td>
</tr>
<tr>
<td>• <code>icmp ipv4 rate-limit unreachable [DF] milliseconds</code></td>
<td>• The <strong>DF</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>• <code>ipv6 icmp error-interval milliseconds [bucketsize]</code></td>
<td>• The <strong>milliseconds</strong> argument specifies the time period between the sending of ICMP destination unreachable messages.</td>
<td></td>
</tr>
</tbody>
</table>

Example:

RP/0/RSP0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 1000 or
### 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.

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>
PurposeCommand or Action

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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>{ ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>Sets the conflict policy to the highest IP value, that is, the IP address with the highest value gets precedence.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 conflict-policy highest-ip</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# ipv6 conflict-policy highest-ip</td>
</tr>
<tr>
<td>Step 3</td>
<td>commit</td>
</tr>
</tbody>
</table>

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.

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
```
Configuring VRF mode big

Perform this task to configure big mode for a VRF.

**SUMMARY STEPS**

1. configure
2. vrf vrf-name
3. mode big
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 vrf vrf-name</td>
<td>Enters the vrf configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# vrf v1</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrf)#</td>
</tr>
<tr>
<td>Step 3 mode big</td>
<td>Enters the big mode for the corresponding VRF.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrf)# mode big</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrf)#</td>
</tr>
<tr>
<td>Step 4 commit</td>
<td></td>
</tr>
</tbody>
</table>

**Additional References**

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

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address resolution configuration tasks</td>
<td>Configuring ARP module in this publication.</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mapping host names to IP addresses</td>
<td>Host Services and Applications Commands module in the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>Network stack IPv4 and IPv6 commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Network Stack IPv4 and IPv6 Commands section in the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
CHAPTER 9

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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference.

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. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Feature History for Configuring NSR, TCP, UDP, and UDP RAW Transports on the Cisco ASR 9000 Series Router

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

- Prerequisites for Configuring NSR, TCP, UDP, Transports, page 213
- Information About Configuring NSR, TCP, UDP Transports, page 214
- How to Configure Failover as a Recovery Action for NSR, page 215
- Additional References, page 216

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 Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

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.

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 Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide.
For information on how to configure NSR on a per-process level for each OSPF process, refer to the Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> nsr process-failures switchover</td>
<td>Configures failover as a recovery action for active instances to switch over to a standby route processor (RP) to maintain nonstop routing (NSR).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# nsr process-failures switchover</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>
Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>the Cisco ASR 9000 Series Router Transport Stack commands: complete command</td>
<td>Transport Stack Commands in the Cisco ASR 9000 Series Aggregation Services Router</td>
</tr>
<tr>
<td>syntax, command modes, command history, defaults, usage guidelines, and</td>
<td>IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>examples</td>
<td></td>
</tr>
<tr>
<td>the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax,</td>
<td>MPLS Label Distribution Protocol Commands in the Cisco ASR 9000 Series</td>
</tr>
<tr>
<td>command modes, command history, defaults, usage guidelines, and examples</td>
<td>Aggregation Services Router MPLS Command Reference</td>
</tr>
<tr>
<td>the Cisco ASR 9000 Series Router OSPF commands: complete command syntax,</td>
<td>OSPF Commands in the Cisco ASR 9000 Series Aggregation Services Router</td>
</tr>
<tr>
<td>command modes, command history, defaults, usage guidelines, and examples</td>
<td>Routing Command Reference</td>
</tr>
<tr>
<td>MPLS Label Distribution Protocol feature information</td>
<td>Implementing MPLS Label Distribution Protocol in the Cisco ASR 9000 Series</td>
</tr>
<tr>
<td>OSPF feature information</td>
<td>Implementing OSPF in the Cisco ASR 9000 Series Aggregation Services Router</td>
</tr>
<tr>
<td></td>
<td>Routing Configuration Guide</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support</td>
<td>—</td>
</tr>
<tr>
<td>for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
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. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Feature History for Implementing VRRP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>• BFD for VRRP feature was added.</td>
</tr>
<tr>
<td></td>
<td>• MIB support for VRRP feature was added.</td>
</tr>
<tr>
<td>Release 4.1.0</td>
<td>VRRP over IPv6 feature was added.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing VRRP on Cisco IOS XR Software, page 220
- Restrictions for Implementing VRRP on Cisco IOS XR Software, page 220
- Information About Implementing VRRP, page 220
- How to Implement VRRP on Cisco IOS XR Software, page 223
- Configuration Examples for VRRP Implementation on Cisco IOS XR Software, page 229
- MIB support for VRRP, page 237
- Hot Restartability for VRRP, page 238
- Configuration Examples for VRRP Implementation on Cisco IOS XR Software, page 238
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

The following are restrictions for implementing 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 15: Basic VRRP Topology, on page 221 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 15: 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 *master virtual router* and is also known as the *IP address owner*. As the master virtual 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 master virtual router fails, the router configured with the higher priority becomes the master virtual router and provides uninterrupted service for the LAN hosts. When Router A recovers, it becomes the master 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 to 100 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 master 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 master 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 master 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 master or a backup virtual router. By default, the highest priority VRRP router functions as master, and all the others function as backups. Priority also determines the order of ascendancy to becoming a master virtual router if the master 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 master 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 master 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 master virtual router.

By default, a preemptive scheme is enabled whereby a higher-priority backup virtual router that becomes available takes over from the current master 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 master upon the failure of the original higher priority master, remains the master even if the original master virtual router recovers and becomes available again.

**VRRP Advertisements**

The master virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the master 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 master 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.

### How to Implement VRRP on Cisco IOS XR Software

This section contains instructions for the following tasks:

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VRRP virtual router id (vrid) has to be different for different sub-interfaces, for a given physical interface.</td>
</tr>
</tbody>
</table>

### Customizing VRRP

Customizing the behavior of VRRP is optional. Be aware that as soon as you enable a VRRP group, that group is operating. It is possible that if you first enable a VRRP group before customizing VRRP, the router could take over control of the group and become the master virtual router before you have finished customizing the feature. Therefore, if you plan to customize VRRP, it is a good idea to do so before enabling VRRP.

The sections that follow describe how to customize your VRRP configuration.
### SUMMARY STEPS

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family {ipv4 | ipv6}
5. vrrp vrid version { 2 | 3 }
6. text-authentication
7. accept-mode{disable}
8. priority priority
9. preempt [delay seconds] [disable]
10. timer [msec] interval [force]
11. track interface type instance interface-path-id [priority-decrement]
12. delay [minimum seconds] [ reload seconds]
13. commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enables VRRP configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router vrrp</td>
<td>Enables VRRP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type interface-path-id</td>
<td>Enables VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv6</td>
</tr>
<tr>
<td>Step 5</td>
<td>vrrp vrid version { 2</td>
<td>3 }</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp vrid 1 version 3</td>
</tr>
</tbody>
</table>

**Note** The `version` keyword is available only for the ipv4 address family.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# vrrp 3 version 3</td>
<td>(Optional) Configures the simple text authentication used for Virtual Router Redundancy Protocol (VRRP) packets received from other routers running VRRP.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# text-authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6 text-authentication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# text-authentication</td>
<td>(Optional) Configures the simple text authentication used for VRRP packets received from other routers running VRRP.</td>
</tr>
<tr>
<td><strong>Step 7 accept-mode {disable}</strong></td>
<td>Enters the IPv4 or IPv6 address family submode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router)# accept-mode disable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8 priority priority</strong></td>
<td>(Optional) Sets the priority of the virtual router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router)# priority 254</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9 preempt [delay seconds] [disable]</strong></td>
<td>(Optional) Sets the master virtual router and optionally, the time in seconds before the router advertises virtual IP address ownership to be the master router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router)# preempt delay 15</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 10</strong> timer [msec] interval [force]</td>
<td>(Optional) Configures the interval between successive advertisements by the master router in a VRRP virtual router.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router)# timer 4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> track interface type instance interface-path-id [priority-decrement]</td>
<td>(Optional) Configures the VRRP to track an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router)# track interface TenGigE 0/0/CPU0/1 30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> delay [minimum seconds] [reload seconds]</td>
<td>(Optional) 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# (config-vrrp-virtual-router) # delay minimum 2 reload 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling VRRP

Use the *address* command to enable VRRP on an interface, as described in the sections that follow.
SUMMARY STEPS

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family ipv4
5. vrrp vrid version { 2 | 3 }
6. address address
7. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>router vrrp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enables VRRP configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1 RP/0/RSP0/CPU0:router(config-vrrp-if)#</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enables VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enters the IPv4 or IPv6 address family submode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>vrrp vrid version { 2</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# vrrp 3 version 3 RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#</td>
</tr>
<tr>
<td>Note</td>
<td>The version keyword is available only for the ipv4 address family.</td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Step 6 | enable vrrp address

Example:

```
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
address 2001:db8::/32
```

We recommend that you do not remove the VRRP configuration from the IP address owner and leave the IP address of the interface active, because duplicate IP addresses on the LAN will result.

To disable VRRP on the interface and remove the IP address of the virtual router, use the `no vrrp address` command.

Step 7 | commit

Verifying VRRP

Use the `show vrrp` command to display a brief or detailed status of one or all VRRP virtual routers.

**SUMMARY STEPS**

1. `show vrrp [ipv4 | ipv6] [interface type instance interface-path-id [vrid]] [brief | detail | statistics [all]]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>`show vrrp [ipv4</td>
</tr>
</tbody>
</table>

Example:

```
RP/0/RSP0/CPU0:router # show vrrp
```

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>clear vrrp statistics [ ipv4 ] [ ipv6 ] [interface] interface-path-id [vrid]]</strong>&lt;br&gt;Example: RP/O/RSP0/CPU0:router# clear vrrp statistics</td>
</tr>
</tbody>
</table>

### Configuration Examples for VRRP Implementation on Cisco IOS XR Software

This section provides the following VRRP configuration examples:

### Configuring accept-mode

Perform this task to disable the installation of routes for the VRRP virtual addresses.

### SUMMARY STEPS

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family {ipv4 | ipv6}
5. vrrp vrid version { 2 | 3 }
6. accept-mode disable
7. commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>router vrrp</td>
</tr>
<tr>
<td>Example: RP/O/RSP0/CPU0:router(config)# router vrrp</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type interface-path-id</td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv6</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> vrrp vrid version { 2</td>
<td>3 }</td>
</tr>
<tr>
<td><strong>Note</strong> The version keyword is available only for the ipv4 address family.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# vrrp 3 version 3</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> accept-mode disable</td>
<td>Disables the installation of routes for the VRRP virtual addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# accept-mode disable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> commit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Global Virtual IPv6 Address

Perform this task to configure the global virtual IPv6 address for a virtual router.
SUMMARY STEPS

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family ipv6
5. vrrp vrid version 3
6. address global address
7. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router vrrp</td>
<td>Enables the VRRP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
</tr>
<tr>
<td>Step 3 interface type</td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</td>
</tr>
<tr>
<td>Step 4 address-family ipv6</td>
<td>Enters the IPv4 or IPv6 address family submode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv6</td>
</tr>
<tr>
<td>Step 5 vrrp vrid version 3</td>
<td>Enters the virtual router configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note  The version keyword is available only for the ipv4 address family.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3</td>
</tr>
<tr>
<td>Step 6 address global</td>
<td>Configures the global virtual IPv6 address for a virtual router.</td>
</tr>
<tr>
<td>address</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
RP/0/RSP0/CPU0:routerconfig-vrrp-virtual-router)# address global 2001:db8::/32 | VRRP packet sizes are limited by the corresponding interface's Maximum Transmission Unit (MTU). This limits the maximum number of global virtual IPv6 addresses that can be supported in a single VRRP session. For example, the default MTU on gigabitEthernet interfaces would allow for a maximum of 90 VRRP global virtual IPv6 addresses in a single session. In order to have more such addresses, you need to increase the interface's MTU accordingly.

Step 7 commit

---

**Configuring a Primary Virtual IPv4 Address**

Perform this task to configure the primary virtual IPv4 address for a virtual router.

**SUMMARY STEPS**

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family ipv4
5. vrrp vrid version { 2 | 3 }
6. address address
7. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enables the VRRP configuration mode.</td>
</tr>
<tr>
<td>Step 2 router vrrp</td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# router vrrp</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type interface-path-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### COMMANDS AND ACTIONS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</code></td>
<td>Enters the IPv4 address family submode.</td>
</tr>
<tr>
<td><code>address-family ipv4</code></td>
<td>Enters the virtual router configuration submode.</td>
</tr>
<tr>
<td>`vrrp vrid version { 2</td>
<td>3 }`</td>
</tr>
<tr>
<td><code>address address</code></td>
<td>Configures the primary virtual IPv4 address for a virtual router.</td>
</tr>
<tr>
<td><code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Secondary Virtual IPv4 Address

Perform this task to configure the secondary virtual IPv4 address for a virtual router.

#### SUMMARY STEPS

1. `configure`
2. `router vrrp`
3. `interface type interface-path-id`
4. `address-family ipv4`
5. `vrrp vrid version { 2 | 3 }`
6. `address address secondary`
7. `commit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router vrrp</code></td>
<td>Enables the VRRP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface type interface-path-id</code></td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>address-family ipv4</code></td>
<td>Enters the IPv4 address family submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`vrrp vrid version { 2</td>
<td>3 }`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Note: The <code>version</code> keyword is available only for the ipv4 address family.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# vrrp 3 version 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>address address secondary</code></td>
<td>Configures the secondary virtual IPv4 address for a virtual router.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# address 10.20.30.1 secondary</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Virtual Link-Local IPv6 Address

Perform this task to either configure the virtual link-local IPv6 address for a virtual router or to specify that the virtual link-local IPv6 address should be enabled and calculated automatically from the virtual router virtual Media Access Control (MAC) address.

The IPv6 address space is structured differently compared to IPv4. Link-local addresses are used to identify each interface on the local network. These addresses may either be configured or determined automatically in a standard way using the link-layer (hardware) address of the interface (MAC address for Ethernet interfaces). Link-local addresses have a standard format and are valid only on the local network (they cannot be routed to, from multiple hops away).

Global unicast IPv6 addresses occupy a disjoint subset of the IPv6 address space from link-local addresses. They can be routed to, from multiple hops away and have an associated prefix length (between 0 and 128 bits).

Each VRRP virtual router has an associated virtual link-local address. This may be configured or determined automatically from the virtual router's virtual MAC address. The virtual MAC address must be unique on the local network. The virtual link-local address is analogous to an IPv4 virtual router's primary virtual IPv4 address, except that its virtual IP (VIP) state is always considered to be up, since duplicate address detection is not required for addresses whose scope is local.

### SUMMARY STEPS

1. configure
2. router vrrp
3. interface type interface-path-id
4. address-family ipv6
5. vrrp vrid version 3 address linklocal {address | autoconfigure}
6. commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enables the VRRP configuration mode.</td>
</tr>
<tr>
<td>Step 2 router vrrp</td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
</tr>
<tr>
<td>Step 3 interface type interface-path-id</td>
<td>Enables the VRRP interface configuration mode on a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/2/0/1</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>address-family ipv6</th>
</tr>
</thead>
</table>
| **Example:** | RP/0/RSP0/CPU0:routerconfig-vrrp-if)#
| | address-family ipv6 |

| Step 5 | vrrp vrid version 3 address linklocal {address | autoconfigure} |
|--------|-----------------------------------------|
| **Example:** | RP/0/RSP0/CPU0:routerconfig-vrrp-address-family)#
| | vrrp 1 version 3 address linklocal
| | FE80::260:3EFF:FE11:6770
| | RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
| | RP/0/RSP0/CPU0:router(config-vrrp-address-family)#
| | vrrp 1 version 3 address linklocal autoconfigure
| | RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#

| Step 6 | commit |

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters the IPv6 address family submode.</td>
</tr>
</tbody>
</table>

### Purpose Command or Action

#### Step 4
- address-family ipv6
  - **Example:**
    - RP/0/RSP0/CPU0:routerconfig-vrrp-if)#
    - address-family ipv6

#### Step 5
- vrrp vrid version 3 address linklocal {address | autoconfigure}
  - **Example:**
    - RP/0/RSP0/CPU0:routerconfig-vrrp-address-family)#
    - vrrp 1 version 3 address linklocal
    - FE80::260:3EFF:FE11:6770
    - RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
    - RP/0/RSP0/CPU0:router(config-vrrp-address-family)#
    - vrrp 1 version 3 address linklocal autoconfigure
    - RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You must disable IPv6 Duplicate Address Detection (DAD) on an interface when the VRRP router's virtual link-local address is the same as the interface's link-local address. When DAD is disabled, duplicate packets are not flagged as duplicates.</td>
</tr>
<tr>
<td>• The version keyword is available only for the ipv4 address family.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
</tbody>
</table>
### Implementing VRRP

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables the VRRP configuration mode.</td>
</tr>
<tr>
<td>router vrrp</td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# router vrrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables the task of logging the VRRP state change events via syslog.</td>
</tr>
<tr>
<td>message state disable</td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp)# message state disable</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrrp)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

### 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 master, and forwards packets sent to these IP addresses. The election process provides dynamic fail over(standby) in the forwarding responsibility should the master 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 master state or if the standby router is made master.

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>configure</strong></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>snmp-server traps vrrp events</code></td>
<td>Enables the SNMP server notifications for VRRP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config)snmp-server traps vrrp events</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>commit</strong></td>
<td></td>
</tr>
</tbody>
</table>

Hot Restartability for VRRP

In the event of failure of a VRRP process in one group, forced failovers in peer VRRP master 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:

```plaintext
cfg
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:

cfg
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 master 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 master for this group with priority 200.
  • Advertising interval is 30 seconds.
  • Preemption enabled.

• Group 100:
  • Router configured first becomes master 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Quality of Service Commands on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
<tr>
<td>Class-based traffic shaping, traffic policing, low-latency queuing, and Modified Deficit Round Robin (MDRR)</td>
<td>Configuring Modular Quality of Service Congestion Management on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide</td>
</tr>
<tr>
<td>WRED, RED, and tail drop</td>
<td>Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide</td>
</tr>
<tr>
<td>VRRP commands</td>
<td>VRRP Commands on Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</td>
</tr>
<tr>
<td>master command reference</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Commands Master List</td>
</tr>
<tr>
<td>getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Information about user groups and task IDs</td>
<td>Configuring AAA Services on Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>
### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
CHAPTER 11

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, page 243
- Information About Implementing Video Monitoring, page 243
- Implementing Video Monitoring, page 248
- Configuration Examples for Implementing Video Monitoring, page 260
- Additional References, page 265

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 artifact or even a "black screen" at the 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.
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 *Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference* 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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

This task configures a standard IPv4 access list.

Standard access lists use source addresses for matching operations.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong></td>
</tr>
</tbody>
</table>
| **Step 2** | `ipv4 access-list name`  
**Example:**  
RP/0/RSP0/CPU0:router# ipv4 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 |
| **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 |

**Note:** 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 `destination` keyword to specify the network or host number to 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-wildcard` argument to specify the wildcard bits to be applied to the destination.

**Purpose**

- Enters IPv4 access list configuration mode and configures access list acl_1.
- (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.
- Allows you to specify the source and destination ports with these conditions.
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
</tbody>
</table>
| **Step 2** | `class-map type traffic class-map-name`  
  **Example:**  
  RP/0/RSP0/CPU0:router(config)# class-map type traffic class1 |
| **Step 3** | `match access-group ipv4 acl-name`  
  **Example:**  
  RP/0/RSP0/CPU0:router(config-cmap)# match access-group ipv4 acl1 |
| **Step 4** | `end-class-map`  
  **Example:**  
  RP/0/RSP0/CPU0:router(config-cmap)# end-class-map | Completes the class-map configuration. |
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).

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>commit</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
</tbody>
</table>
| **Step 2** | policy-map type *performance-traffic policy-map-name*  
*Example:*  
RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1 |
| **Step 3** | class type *traffic class-name*  
*Example:*  
RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name |
| **Step 4** | monitor metric ip-cbr  
*Note* Currently only ip-cbr metric monitoring is supported for video monitoring.  
*Example:*  
RP/0/RSP0/CPU0:router(config-pmap-c)# monitor metric ip-cbr |
| **Step 5** | rate layer3 packet *packet-rate pps*  
*Example:*  
RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# rate layer3 packet packet-rate 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>policy-map type performance-traffic policy-map-name</td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>class type traffic class-name</td>
<td>Enters the class-map to be matched for this policy. Multiple classes can be specified for a single policy.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>monitor metric ip-cbr</td>
<td>Enters the IP-CBR metric monitor submode.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-pmap-c)# monitor metric ip-cbr</td>
<td>Note: Currently only ip-cbr metric monitoring is supported for video monitoring.</td>
</tr>
<tr>
<td>5</td>
<td>rate media bit-rate {bps</td>
<td>kbps</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# rate media 100 mbps</td>
<td>Note: The default unit of media bit-rate is kbps.</td>
</tr>
<tr>
<td>6</td>
<td>media packet count in-layer3 packet-count</td>
<td>Specifies the number of media packets for each IP payload.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# media packet count in-layer3 10</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>media packet size packet-size</td>
<td>Specifies the size in bytes for each media packet in the IP payload.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# media packet size 198</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 policy-map type performance-traffic policy-map-name</td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
</tbody>
</table>

Example:

RP/0/RSP0/CPU0:router(config) # policy-map type performance-traffic policy1
### Command or Action | Purpose
--- | ---
**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** | {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 default 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 value is 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>policy-map type performance-traffic policy-map-name</td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1</td>
</tr>
<tr>
<td>3.</td>
<td>class type traffic class-name</td>
<td>Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name</td>
</tr>
<tr>
<td>4.</td>
<td>react react-id {mrv</td>
<td>delay-factor</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-pmap-c)# react 1 mrv</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>threshold type immediate</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold type immediate</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>threshold value ( \text{ge}</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config- pmap-c-react)# threshold value ge 50</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>action syslog</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config- pmap-c-react)# action syslog</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>alarm severity {error</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm severity critical</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>alarm type {discrete</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config- pmap-c-react)# alarm type discrete</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface type interface-path-id</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# interface type interface-path-id</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 service-policy type performance-traffic input policy-name</td>
<td>Attaches the policy to the interface in the ingress direction.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-if)# service-policy type performance-traffic input policy1</td>
<td>Attaches the policy to the interface in the ingress direction.</td>
</tr>
<tr>
<td>Step 4 commit</td>
<td></td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>performance traffic clone profile <code>profile_name</code></td>
<td>Enters the performance traffic clone profile mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# performance traffic clone profile profile1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type <code>interface-path-id</code></td>
<td>Configures the egress interface to a clone profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# interface GigabitEthernet 0/0/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>flow ipv4 source <code>&lt;source-ip&gt;</code> destination <code>&lt;destination-ip&gt;</code></td>
<td>Configures the traffic flows that need to be cloned, to the clone profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)#</td>
<td></td>
</tr>
</tbody>
</table>
Multiple flows can be associated with a single clone profile. Similarly, a single flow can be associated with the multiple clone profiles.

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

```plaintext
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
```
**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 GigabitEthernet0/0/0.1
  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
```
### 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

```plaintext
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
```

---

**Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide, Release 4.2.x**

OL-26068-04  263
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
!

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference</td>
</tr>
<tr>
<td>Getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Modular quality of service command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC4445</td>
<td>Proposed Media Delivery Index (MDI)</td>
</tr>
</tbody>
</table>
### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
<tr>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td></td>
</tr>
<tr>
<td>1027</td>
<td>43</td>
</tr>
<tr>
<td>1195, OSI IS-IS usage</td>
<td>202</td>
</tr>
<tr>
<td>2373</td>
<td>199</td>
</tr>
<tr>
<td>826</td>
<td>43</td>
</tr>
<tr>
<td>959</td>
<td>120</td>
</tr>
</tbody>
</table>

**A**

ABF (ACL-based forwarding) 11, 26
  - overview 11
  - security ACL, how to 26
ABF with security ACL 26
ABF-OT 11
accept-mode 229
access 12, 14
  - lists 12, 14
    - applying 14
    - inbound or outbound interfaces, applying on 14
    - IPv4 or IPv6, how to 12
access lists 12, 14
  - applying 14
  - IPv4 or IPv6 12
  - applying 14
access lists, applying 14
Adding Entries with Sequence Numbers 34
  - Example command 34
Adding Entries Without Sequence Numbers 34
  - Example command 34
Additional References 167, 265
Additional References command 38, 53, 86, 114, 133, 177, 209, 216, 240
address argument 199
address command 226
address conflict resolution 195
address formats 181
address repository manager 195
Address Repository Manager 195
address repository manager function 195
address resolution 43
addresses (continued)
  - primary 197
  - secondary 200
advertisement 222
aggregatable global address 183
aggregatable global address format 183
aggregatable global address format, figure 183
applying 14
ARM (Address Repository Manager) 195
ARP (Address Resolution Protocol) 41, 42, 43, 44
  - address resolution 43
  - cache entries 44
  - definition 42
  - MAC (Media Access Control) 41
  - proxy ARP 43
RFC 1027 43
RFC 826 43
Assigning a DHCP Profile to a Bridge Domain 113
  - Example command 113
assigning addresses to individual router interfaces 199
Assigning an Unnumbered Interface 208
  - Example command 208

**B**

basic IPv6 packet header fields 185
benefits 58
BGP Attributes Download 61
BGP policy accounting, classification 59

**C**

cache entries 44
cache entries, definition 44
CEF (Cisco Express Forwarding) 57, 58, 59, 60
  - benefits 58
  - BGP policy accounting, classification 59
description 57
features 58
CEF (Cisco Express Forwarding) (continued)
FIB (Forwarding Information Base) 59
reverse path forwarding 60
Checking Network Connectivity 131
Example command 131
Checking Network Connectivity for Multiple Destinations 121
CIDR format 5
using 5
Cisco IOS XR DHCP Relay on a VRF 104
Example command 104
Cisco IOS XR DHCP Relay on an Interface 103
Example command 103
Cisco IOS XR DHCP Relay Profile 103
Example command 103
Cisco IOS XR Relay Agent Giaddr Policy 104
Example command 104
Cisco IOS XR Relay Agent Information Option Support 104
Example command 104
Class-map 250
configuring 250
Clearing VRRP Statistics 228, 240
Example command 240
commands 120, 214, 226, 228
nsr process-failures switchover 214
rcp copy 120
show vrrp 228
vrrp ipv4 226
components 170
configuration 123
Configuration Examples for ARP Configuration on Cisco IOS XR Software command 52
Configuration Examples for DHCP Snooping command 112
Configuration Examples for HSRP Implementation on Cisco IOS XR Software command 166
Configuration Examples for Implementing Access Lists and Prefix Lists command 32
Configuration Examples for Implementing CEF on RoutersCisco IOS XR Software command 72
Configuration Examples for Implementing Host Services and Applications on command 131
Configuration Examples for Implementing LPTS Policers command 172
Configuration Examples for Implementing Network Stack IPv4 and IPv6 208
Configuration examples for Implementing Video Monitoring 260
Configuration Examples for the Cisco IOS XR DHCP Relay Agent command 103
Configuration Examples for VRRP Implementation on Cisco IOS XR Software command 229, 238
configuring 171, 250, 251, 257, 258
Configuring a DHCP Profile for Trusted Bridge Ports 113
Example command 113
Configuring a Global Virtual IPv6 Address 230
Configuring a Primary Virtual IPv4 Address 152, 232
configuring a router 126
Configuring a Router for Multiple HSRP Groups 166
Example command 166
Configuring a Router to Use rcp, FTP, or TFTP Connections 133
Example command 133
Configuring a Secondary Virtual IPv4 Address 153, 233
Configuring a slave follow 154
Configuring a slave primary virtual IPv4 address 156
Configuring a slave secondary virtual IPv4 address 157
Configuring a slave virtual mac address 158
Configuring a Trusted Bridge Port 113
Example command 113
Configuring a Virtual Link-Local IPv6 Address 235
Configuring a VRRP Group 238
Example command 238
Configuring accept mode 229
configuring activation delay 146
Configuring an HSRP Group 166
Example command 166
Configuring an HSRP Session Name 159
Configuring an Untrusted Profile on a Bridge Domain 113
Example command 113
Configuring BGP Attributes Download 86
Example command 86
Configuring BGP Policy Accounting 72
Example command 72
Configuring DHCPv6 stateful relay agent for prefix delegation 101
Configuring Domain Services 132
Example command 132
configuring failover as recovery 215
configuring group attributes 142
Configuring LPTS Policers 173
Example command 173
Configuring object tracking for HSRP 165
configuring relay agent 95
Configuring the DHCPv6 (Stateless) Relay Agent 92
Configuring the Switching of Modular Services Card to Management Ethernet Interfaces on the Route Processor 86
Example command 86
Configuring Unicast RPF Checking 86
Example command 86
Configuring VRF mode big 129
connections, how to 125, 126
Creating a Static ARP Cache Entry 52
Example command 52
customization 223
customize, how to 223
customizing 223
Customizing HSRP 149
host services and applications (continued)
  prerequisites 117
telnet 120
TFTP server 119
Hot restartability 166
  for HSRP 166
Hot Restartability for VRRP 238
  for VRRP 238
how to configure 171
how to enable 226
HSRP 142, 146, 148
  configuring activation delay 146
  configuring group attributes 142
  enabling ICMP redirect messages 148
HSRP (Hot Standby Router Protocol) 135, 136, 139, 141, 142, 146, 148
  configuring group attributes 142
  configuring activation delay 146
  description 135
  enabling 139, 141
  enabling support for ICMP redirect messages 148
  groups 136
  overview 136
  preemption 139
HSRP (Hot Standby Router Protocol), figure 136

I
  ICMP packet header 194
  ICMP rate limiting 203, 204
  IFIB (Internal Forwarding Information Base) 170
  Implementing 243
  Implementing IPSLA-OT 27
  inbound connection, telnet 120
  inbound or outbound interfaces, applying on 14
  interfaces, IP addresses 197, 200
    primary, IP address 197
  introduction (IPv6 for Cisco IOS XR) 181
  IP 14, 197, 200
    access lists 14
    addresses 197, 200
      multiple, assigning 200
      primary 197
      secondary 200
  IP address conflict resolution 206
  IP protocol number 222
  IPARM conflict resolution 205
  IPSLA support 12
  IPv4 and IPv6 protocol stacks 201
  IPv4 and IPv6 protocol stacks, configuring 201
  IPv4 and IPv6 protocol stacks, how to 201
  IPv4 or IPv6 12
  IPv4 or IPv6 access lists 12
  IPv4 or IPv6, how to 12
  IPv4 packet header format 185
  IPv4 packet header format, figure 185
  IPv4-compatible IPv6 address 185
  IPv4-compatible IPv6 address format 185
  IPv4-compatible IPv6 address format, figure 185
  IPv6 181, 185, 190, 192, 193, 194, 199
  assigning addresses to individual router interfaces 199
  extension header format, figure 185
  neighbor redirect message 193
  packet header 185
  packet header format, figure 185
  address argument 199
  address formats 181
  ICMP packet header 194
  introduction (IPv6 for Cisco IOS XR) 181
  neighbor discovery 190
  neighbor redirect message, figure 193
  neighbor solicitation message, figure 190
  prefix argument 199
  RFC 2460 181
  router advertisement method, figure 192
  IPv6 address 181
    formats 181
  IPv6 addresses to individual router interfaces, assigning 199
  IPv6 extension header 185
  IPv6 extension header format 185
  IPv6 for Cisco IOS XR 181
  IPv6 neighbor discovery 190, 192, 193
    neighbor redirect message, figure 193
    neighbor solicitation message, figure 190
    router advertisement method, figure 192
  IPv6 neighbor discovery-neighbor redirect message 193
  IPv6 neighbor discovery-neighbor solicitation message 190
  IPv6 neighbor discovery-router advertisement method 192
  IPv6 neighbor redirect message 193
  IPv6 packet header format 185
  IPv6 packet header format, figure 185
  ipv6-address argument 199
  ipv6-prefix argument 199

L
  line protocol 28
  link local address format 184
  link local address format, figure 184
  link-local address 184
  list 29
  lists 12, 14
    applying 14
    inbound or outbound interfaces, applying on 14
lists (continued)
   IPv4 or IPv6, how to 12
Local Packet Transport Services (LPTS) 170, 171
   components 170
   policers 170, 171
      configuring 171
      how to configure 171
      overview 170
Longest Prefix Resolution 206

M
MAC (Media Access Control) 41
master virtual router 222
MIB support for VRRP 237
Multiple Group Optimization (MGO) for HSRP 149
multiple, assigning 200

N
neighbor discovery 190
neighbor redirect message 193
neighbor redirect message, figure 193
neighbor solicitation message, figure 190
neighbor, IPv6 190
network connectivity 118, 121
   ping tool 118
   traceroute 118
network stack IPv4 and IPv6 195
Nonstop Routing (NSR) 214, 215
   configuring failover as recovery 215
   failover as recovery, how to 215
   function 214
      nsr process-failures switchover command 214
nsr process-failures switchover 214
nsr process-failures switchover command 214

O
Object Tracking 12
Option 82 information 105
OSPFv2 SPF 61
overview 11, 136, 170
Overview 244

P
packet header 185
packet header fields, IPv6 185
packet header format, figure 185
packet routes 122
packet routes, checking 122
packet routes, how to check 122
ping tool 118
policers 170, 171
   configuring 171
   how to configure 171
   overview 170
Policy-map 251
   configuring 251
   preemption 139
   prefix argument 199
   prefix list 10, 11
   prefix prioritization 61
      OSPFv2 SPF 61
Prefix Prioritization 61
      OSPFv2 SPF 61
prerequisites 117
primary 197
Primary Virtual IPv4 Address 232
primary, IP address 197
proxy ARP 43

R
RAW protocol 214
rcp 125
rcp (remote copy protocol) 120, 125
   connections, how to 125
   definition 120
   rcp copy command 120
   troubleshooting tips 125
rcp connections 125
rcp copy 120
rcp copy command 120
relay agent, how to 95
relay information option (option 82) 106
remote copy protocol (RCP) 119
Resequencing Entries in an Access List 33
   Example command 33
reverse path forwarding 60
RFC 43, 120, 199, 202
   1027 43
   1195, OSI IS-IS usage 202
   2373 199
   826 43
   959 120
RFC 1027 43
RFC 2460 181
RFC 826 43
route 30
tasks (continued)
packet routes 122
cp connections 125
ttr 124
ttftp 128

T

tasks 12, 14, 26, 95, 121, 122, 123, 124, 125, 126, 128, 129, 139, 141, 142, 146, 148, 199, 201, 203, 206, 223, 226, 228

S

secondary 200
secondary addresses, IP 200
Secondary Virtual IPv4 Address 233
security ACL, how to 26
sequence numbering behavior 6
server, router configuration 124
Service policy 257
configuring 257
show vrpr 228
show vrpr command 228
simplified IPv6 packet header 185
single LAN, process 43
solicitation message, IPv6 190
State Change Logging 236
static 205
syslog source-interface 130

U

UDP (User Datagram Protocol) 214
untrusted link 105
uRPF (Unicast IPv4 and IPv6 Reverse Path Forwarding) 60
using 5
using rcp connections 125

V

verification 228
verify, how to 228
Verifying BGP Policy Statistics 75
Example command 75
Video Monitoring 243, 244, 247
Implementing 243
Overview 244
Video Monitoring (continued)
  Terminology 247
  Features 244
Video Monitoring Trap and Clone 244, 258
  configuring 258
Virtual Link-Local IPv6 Address 235
VRRP 223, 226, 228
  customization 223
  how to enable 226
  verification 228
VRRP (Virtual Router Redundancy Protocol) 220, 222, 223, 226, 228
  description 220
  advertisement 222

VRRP (Virtual Router Redundancy Protocol) (continued)
  customize, how to 223
  customizing 223
  enable, how to 226
  enabling 226
  IP protocol number 222
  master virtual router 222
  show vrrp command 228
  verify, how to 228
  vrrp ipv4 command 226
vrrp ipv4 226
vrrp ipv4 command 226
VRRP Statistics, clearing 228